

Глава 1 Теоретические аспекты информационной безопасности экономических систем

1.1 Основные понятия О РУССКОМ ХАКЕРЕ, БЕССМЫСЛЕННОМ И БЕСПОЩАДНОМ

Окончание. Начало на с. 1

ДЕСЯТКИ лет домо-рошенные строители информационных сетей пользуются американским оборудованием. Сам чёрт не знает, что в нём внутри и что произойдёт, если кем-то извне будет дана команда хотя бы по остановке его работы или работе в режиме «глюков и запаздывания», что ещё хуже. В один миг «американские настоящие хакеры» могут остановить наши электростанции, заблокировать подачу тепла и электричества в лютую стужу, остановить работу аэропортов и железной дороги и чёрт-те что ещё! Это вам не взлом сервера Демпартии США, это чистый кирдык, который может случиться в любой момент.

Самое время почесать репу и задуматься — почему они до сих пор этого не сделали? Ответ очевиден — боятся атомной бомбы. Она тоже работает, как хакер. При взрыве на высоте в километр где-нибудь над Нью-Йорком можно одновременно распылить графитную пыль. Всё, что работает на электричестве, почти сразу ломается — от коротких замыканий. Но это будет означать начало «горячей войны», что крайне нежелательно. С другой стороны, американский государственный хакер и его хозяин должны знать, что возмездие может наступить из космоса и без применения атомного оружия. На современном языке это называется Использование Радиоэлектронных Средств (РЭБ). С ними у нас всё не так плохо — научились так искажать электронные по-

можем сделать слепыми и неуправляемыми.

Осталось решить главную задачу — дать понять командам американских хакеров, что их возможные проделки до добра не доведут. Что неотвратимы удар возмездия и удачное завершение Судного дня. Это когда российские межконтинентальные ядерные ракеты уверенно смогут долететь до вражеской территории и их не уничтожат на активном участке полёта с помощью американской ПРО из Аляски и Польши. Только это и может пока остановить настоящих американских хакеров.

И здесь самое время напомнить ещё раз, что вот этого у нас как раз и не хватает. Программа по развёртыванию тяжёлых спутниковых систем закрыта два года назад, а по созданию сверхтяжёлых носителей даже не начата. Именно они могли бы парализовать любую зону над земной поверхностью и сделать американскую ПРО бесполезной. Но идеолог создания этой оборонной системы член-корреспондент РАН и доктор технических наук **Виталий Лопота** так и находится под следствием по чёрному навету, хотя с него и сняли позорный тюремный браслет. Тем временем «Роскосмос» продолжает модернизировать космическую технику 50-х годов прошлого века.

Другой задачи нашим учёным пока не поставлено. «Самому» явно не до фантастических сюжетов будущего — против него сегодня весь «западный» мир. А новая российская знать, в том числе и политическая, в такую ерунду, как «хакерские» атаки, скорее всего, просто не верит.

Современное общество называется информационным. Широкое развитие средств вычислительной техники и связи позволило собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше. Благодаря новым информационным технологиям производственная и непроизводственная деятельность человека, его повседневная сфера общения безгранично расширяются за счет вовлечения опыта, знаний и духовных ценностей, выработанных мировой цивилизацией, и сама экономика все в меньшей степени характеризуется как производство материальных благ и все в большей — как распространение

информационных продуктов и услуг.

Современный этап информатизации связан с использованием персональной электронно-вычислительной техники, систем телекоммуникаций, создания сетей ЭВМ. Возрастает потребность в разработке и применении эффективных решений в сфере информационной индустрии. Она занимается производством технических и программных средств, информационных технологий для получения новых знаний.

На определенном этапе развития информационной индустрии рождается информационное общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество людей.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Именно новые технологии привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности международного информационного обмена. Формирование информационного общества концептуально и практически означает формирование мирового информационного пространства.

Информационное пространство (инфосфера) - сфера человеческой деятельности связанная: с созданием, преобразованием и потреблением информации и включающая в себя:

- индивидуальное и общественное сознание
- информационные ресурсы, то есть информационную инфраструктуру (комплекс организационных структур, технических средств, программного и другого обеспечения для формирования, хранения, обработки и передачи информации), а также собственно информацию и ее потоки.

Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Каждый прорыв человечества в будущее не освобождает его от груза прошлых ошибок и нерешенных проблем. Когда экономические войны из-за интеграции национальных экономик стали слишком опасными и убыточными, а глобальный военный конфликт вообще способен привести к исчезновению жизни на планете, война переходит в иную плоскость - информационную.

Информационная война - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Информационное воздействие - акт применения информационного оружия.

Информационное оружие - комплекс технических и других средств, методов и технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;
- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации;
- распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений;
- воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства,

используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий.

Под **угрозой безопасности информации** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Если исходить из классического рассмотрения кибернетической модели любой управляемой системы, возмущающие воздействия на нее могут носить случайный характер. Поэтому среди угроз безопасности информации следует выделять как один из видов угроз случайные, или непреднамеренные. Их источником могут быть выход из строя аппаратных средств, неправильные действия работников информационных системы (ИС) или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д. Такие угрозы тоже следует держать во внимании, т.к. ущерб от них может быть значительным. Однако в данной работе наибольшее внимание уделяется угрозам умышленным, которые в отличие от случайных преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют "компьютерным пиратом" (хакером).

В своих противоправных действиях, направленных на овладение чужими секретами, взломщики стремятся найти такие источники конфиденциальной информации, которые бы давали им наиболее достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С помощью различного вида уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации понимается материальный объект, обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Информационная безопасность включает:

- ✓ состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;
- ✓ состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;
- ✓ состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;
- ✓ экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);
- ✓ финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов).

Обеспечение информационной безопасности должно начинаться с выявления субъектов отношений, связанных с использованием информационных систем. Спектр их интересов может быть разделен на следующие основные категории: доступность (возможность за приемлемое время получить требуемую информационную услугу), целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения), конфиденциальность (защита от несанкционированного ознакомления).

Исходя из вышеизложенного, в наиболее общем виде информационная безопасность может быть определена как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой (рис. 1).



Рис. 1 Структура понятия «Информационная безопасность»

Понятие информационной безопасности в узком смысле этого слова подразумевает:

- надежность работы компьютера;
- сохранность ценных данных;
- защиту информации от внесения в нее изменений неуполномоченными лицами;
- сохранение тайны переписки в электронной связи.

Безопасность проявляется как невозможность нанесения вреда функционированию и свойствам объекта, либо его структурным составляющим.

Объектом информационной безопасности может быть коммерческое предприятие. Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными. Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или

сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз.

К объектам информационной безопасности на предприятии относят:

- ❖ информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;
- ❖ средства и системы информатизации - средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

При осуществлении коммерческой деятельности возникает информация, известность которой другим участникам рынка может существенно снизить доходность этой деятельности. В деятельности государства порождается информация, раскрытие которой может снизить эффективность проводимой политики. Подобная информация закрывается, и устанавливаемый режим ее использования призван предупредить возможность несанкционированного ознакомления с ней. В этом случае объектом безопасности выступает режим доступа к информации, а информационная безопасность заключается в невозможности нарушения этого режима. Примером могут служить информационно-телекоммуникационные системы и средства связи, предназначенные для обработки и передачи сведений, составляющих государственную тайну. Основным объектом безопасности в них является режим доступа к секретной информации. Информационная безопасность таких систем заключается в защищенности этой информации от несанкционированного доступа, уничтожения, изменения и других действий. Система обеспечения безопасности информации включает подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашений.

Безопасное программное обеспечение представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Политика безопасности включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

Угроза безопасности информации - события или действия, которые могут привести к искажению, неразрешенному использованию или к разрушению информационных ресурсов управления системы, а также программных и аппаратных средств.

Защита информации (ЗИ) - комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности: целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Основные предметные направления ЗИ - охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Система - это совокупность взаимосвязанных элементов, подчиненных единой цели.

Признаками системы являются следующие:

1. Элементы системы взаимосвязаны и взаимодействуют в рамках системы.
2. Каждый элемент системы может в свою очередь рассматриваться как самостоятельная система,

но он выполняет только часть функций системы.

3. Система как целое выполняет определенную функцию, которая не может быть сведена к функциям отдельно взятого элемента.
4. Подсистемы могут взаимодействовать как между собой, так и с внешней средой и изменять при этом свое содержание или внутреннее строение.

Под системой безопасности будем понимать организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз.

Система защиты информации представляет организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз

С позиций системного подхода к защите информации предъявляются определенные требования:

- обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявления ее узких и слабых мест и противоправных действий;
- безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах экономической системы и на всех этапах технологического цикла обработки информации;
- планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции;
- защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам;
- эффективность защиты информации означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз;
- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации; обеспечение степени конфиденциальной информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого система защиты информации может иметь:

правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы действия;

организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба безопасности, служба режима, служба защиты информации техническими средствами и др.

аппаратное обеспечение. Предполагается широкое использование технических средств, как для защиты информации, так и для обеспечения деятельности собственно системы защиты информации;

информационное обеспечение. Оно включает в себя документированные сведения (показатели, файлы), лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

программное обеспечение. К нему относятся антивирусные программы, а также программы (или части программ регулярного применения), реализующие контрольные функции при решении учетных, статистических, финансовых, кредитных и других задач;

математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации;

эргономическое обеспечение. Совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации.

Глоссарий основных понятий информационной безопасности представлен в приложении № 6.

1.2 Экономическая информация как товар и объект безопасности

В буквальном переводе с латинского слово *informatio* означает разъяснение, осведомление, сообщение о каком-то факте, событии и т.п.

В кибернетике информация обычно трактуется как степень устранения неопределенности знания у получателя. Иными словами, информацией является не любое сообщение, а лишь такое, которое содержит неизвестные ранее его получателю факты.

Информацию различают по отраслям знаний: техническая, экономическая, биологическая и т.п.

Экономическая информация относится к области экономических знаний. Она характеризует процессы снабжения, производства, распределения и потребления материальных благ.

Управление экономическими объектами всегда связано с преобразованием экономической информации.

С кибернетических позиций любой процесс управления сводится к взаимодействию управляемого объекта (им может быть станок, цех, отрасль) и системы управления этим объектом. Последняя получает информацию о состоянии управляемого объекта, соотносит ее с определенными критериями (планом производства, например), на основании чего вырабатывает управляющую информацию.

Очевидно, что управляющие воздействия (прямая связь) и текущее состояние управляемого объекта (обратная связь) - не что иное, как информация. Реализация этих процессов и составляет основное содержание работы управленческих служб, включая и экономические.

В деятельности любой фирмы присутствует **информационный ресурс** - это документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и др. информационных системах), т.е. документированные знания. Информационные ресурсы в современном обществе играют не меньшую, а нередко и большую роль, чем ресурсы материальные. Знание - кому, когда и где продать товар может цениться на меньше, чем товар, и в этом плане динамика развития общества свидетельствует о том, что на "весах" материальных и информационных ресурсов последние начинают преобладать. Причем тем сильнее, чем белее общество открыто, чем более развиты в нем средства коммуникации, чем большей информацией оно располагает.

Информационные ресурсы являются исходной для создания **информационных продуктов**. Последние являются результатом интеллектуальной деятельности человека и распространяются с помощью услуг.

Посредством информационных услуг осуществляется получение и предоставление в распоряжение пользователя информационных продуктов.

Юридической основой этой операции должен быть договор между двумя сторонами - поставщиком и потребителем, а источником информационных услуг - **базы данных**. Они могут существовать в компьютерном и некомпьютерном вариантах, в виде библиографических и небиблиографических взаимосвязанных данных, основанных на общих правилах описания, хранения и манипулирования данными.

Если информационные ресурсы, продукты и услуги, представляют ценность для предметной деятельности, то они являются товаром, за исключением случаев, предусмотренных законодательством РФ (прил. № 2).

Информация как всякий товар, имея потребительскую стоимость, обладает рядом особенностей, отличающих ее от товаров, например, продуктов питания, которые при потреблении, как известно, исчезают.

К числу особенностей информации как товара следует отнести:

- **неисчерпаемость** - по мере развития общества и роста потребления ее запасы не убывают, а растут;

- **сохраняемость** - при использовании не исчезает и даже может увеличиваться за счет трансформации полученных сообщений;

- **несамостоятельность** - проявляет свою "движущую силу" только в соединении с другими ресурсами (труд, техника, сырье, энергия).

Следующим важнейшим свойством информации, как товара, является ее цена, формирующаяся на рынке под воздействием, в основном, спроса и предложения. Например, цена на программу "1С-Бухгалтерия" формируется, исходя из затрат на разработку этого информационного продукта, его качества, а также ожидаемого спроса на него. Предложение этого товара может быть обеспечено без каких-либо ограничений в нужном количестве экземпляров в отличие от товарно-материальных ресурсов, которые, как известно, со временем истощаются.

Если информация представляет ценность для организации, то необходимо эту ценность не только использовать, но и защищать.

Цена информации в предпринимательской деятельности может также определяться, как величина ущерба, который может быть нанесен фирме в результате использования коммерческой информации конкурентами. Или наоборот прибыли (дохода), который может быть получен фирмой в результате использования коммерческой информации при принятии управленческих решений.

Информация может использоваться в организации, если удовлетворяет следующим требованиям: конфиденциальность, целостность, оперативность использования (доступность) и достоверность.

Часть информации обращающейся в фирме представляет собой конфиденциальную информацию, чаще она отражает коммерческую тайну (КТ). Перечень сведений конфиденциального характера утвержден президентом РФ, Указом № 188 от 6 марта 1997 года (прил. № 2).

Под КТ предприятия понимаются сведения о производстве, технологии, управлении, финансах, и другой деятельности предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам.

Состав и объем сведений, составляющих КТ, определяются руководством предприятия. Для того, чтобы иметь возможность контролировать деятельность предприятий, Правительство России выпустило 05.12.91 г. Постановление № 35 "О перечне сведений, которые не могут составлять коммерческую тайну" (прил. № 3).

Информация может составлять коммерческую тайну, если она отвечает следующим требованиям (критерии правовой охраны):

- к ней нет свободного доступа на законном основании;
- обладатель информации принимает меры к охране ее конфиденциальности.

К коммерческой тайне не может быть отнесена информация:

- содержащаяся в учредительных документах;
- содержащаяся в документах, дающих право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии и т.д.)
- содержащаяся в годовых отчетах, бухгалтерских балансах, формах государственных статистических наблюдений, аудиторских заключений, а также в иных, связанных с исчислением и уплатой налогов;
- содержащая сведения об оплачиваемой деятельности государственных служащих;
- содержащаяся в годовых отчетах фондов об использовании имущества;
- связанная с соблюдением экологического и антимонопольного законодательства, обеспечением безопасных условий труда, реализацией продукции, причиняющей вред здоровью населения;
- о деятельности благотворительных организаций и некоммерческих организаций, не связанных с предпринимательской деятельностью;
- о наличии свободных рабочих мест;
- о реализации государственной программы приватизации;
- о ликвидации юридического лица;
- для которой определены ограничения по установлению режима коммерческой тайны в соответствии с федеральными законами и принятыми в целях их реализации подзаконными актами.

Основными субъектами права на коммерческую тайну являются обладатели коммерческой тайны,

их правопреемники.

Обладатели коммерческой тайны - физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

Правопреемники - физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайну другого лица.

Перечень сведений, относящихся к КТ и носящий рекомендательный характер, может быть сгруппирован по тематическому принципу. Сведения, включенные в данный перечень, могут быть КТ только с учетом особенностей конкретного предприятия (организации).

1. Сведения о финансовой деятельности – прибыль, кредиты, товарооборот; финансовые отчеты и прогнозы; коммерческие замыслы; фонд заработной платы; стоимость основных и оборотных средств; кредитные условия платежа; банковские счета; плановые и отчетные калькуляции.

2. Информация о рынке - цены, скидки, условия договоров, спецификация продукции, объем, история, тенденции производства и прогноз для конкретного продукта; рыночная политика и планирование; маркетинг и стратегия цен; отношения с потребителем и репутация; численность и размещения торговых агентов; каналы и методы сбыта; политика сбыта; программа рекламы.

3. Сведения о производстве продукции - сведения о техническом уровне, технико-экономических характеристиках разрабатываемых изделий; сведения о планируемых сроках создания разрабатываемых изделий; сведения о применяемых и перспективных технологиях, технологических процессах, приемах и оборудовании; сведения о модификации и модернизации ранее известных технологий, процессов, оборудования; производственные мощности; состояние основных и оборотных фондов; организация производства; размещение и размер производственных помещений и складов; перспективные планы развития производства; технические спецификации существующей и перспективной продукции; схемы и чертежи новых разработок; оценка качества и эффективности.

4. Сведения о научных разработках - новые технологические методы, новые технические, технологические и физические принципы; программы НИР; новые алгоритмы; оригинальные программы.

5. Сведения о материально-техническом обеспечении - сведения о составе торговых клиентов, представителей и посредников; потребности в сырье, материалах, комплектующих узлах и деталях, источники удовлетворения этих потребностей; транспортные и энергетические потребности.

6. Сведения о персонале предприятия - численность персонала предприятия; определение лиц, принимающих решения.

7. Сведения о принципах управления предприятием - сведения о применяемых и перспективных методах управления производством; сведения о фактах ведения переговоров, предметах и целях совещаний и заседаний органов управления; сведения о планах предприятия по расширению производства; условия продажи и слияния фирм.

8. Прочие сведения - важные элементы системы безопасности, кодов и процедур доступа, принципы организации защиты коммерческой тайны.

Законом РФ от 02.12.90 г. "О банках и банковской деятельности" введено понятие "банковской тайны".

Банковская тайна - защищаемые банками и иными кредитными организациями сведения о банковских операциях по счетам и сделкам в интересах клиентов, счетах и вкладах своих клиентов и корреспондентов, а также сведения о клиентах и корреспондентах, разглашение которых может нарушить право последних на неприкосновенность частной жизни.

К основным объектам банковской тайны относятся следующие:

1. Тайна банковского счета - сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации;

2. Тайна операций по банковскому счету - сведения о принятии и зачислении поступающих на счет клиента денежных средств, о выполнении его распоряжений по перечислению и выдаче соответствующих сумм со счета;

3. Тайна банковского вклада - сведения обо всех видах вкладов клиента в кредитной организации.

4. Тайна частной жизни клиента.

Служебная тайна - защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения, их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права. Для осуществления ее правовой охраны и защиты необходим специальный Федеральный закон «О служебной тайне».

Информация может считаться служебной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- ✓ отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);
- ✓ является охраноспособной конфиденциальной информацией ("чужой тайной") другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);

Профессиональная тайна - защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

- доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;
- запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;
- информация не относится к сведениям, составляющим государственную и коммерческую тайну.

В соответствии с этими критериями можно выделить следующие объекты профессиональной тайны:

1. Врачебная тайна
2. Тайна связи.
3. Нотариальная тайна.
4. Адвокатская тайна.
5. Тайна усыновления.
6. Тайна страхования.

ЛИЧНОСТЬ

Кто, как и зачем собирает огромный массив данных о жителях России?

ОБ ИНТЕРНЕТ-ШПИОНАЖЕ, ИНФОРМАЦИОННЫХ ВОЙНАХ И ВИРТУАЛЬНЫХ БИТВАХ С РЕАЛЬНЫМИ ЖЕРТВАМИ ГЛАВНОМУ РЕДАКТОРУ «АИФ» ИГОРЮ ЧЕРНЯКУ РАССКАЗАЛ АЛЕКСАНДР ЖАРОВ, РУКОВОДИТЕЛЬ РОСКОМНАДЗОРА.

ЭКСТРЕМИСТЫ ИЛИ ТЕРРОРИСТЫ?

- Александр Александрович, ваше ведомство считает чем-то вроде цербера, душителя свобод, который так и норовит заблокировать популярный сайт или вынести предупреждение газете.

- В этом нет ничего удивительного, потому что наша служба надзорная. Мы надзираем за тем, что сейчас называют «информационным обществом», в том числе за средствами связи и средствами массовой информации, за интернет-ресурсами.

- Это своего рода цензура?

- Цензура - это проверка содержания статьи или телесюжета, перед тем как они будут напечатаны в газете или показаны в эфире. В нашей стране действует конституционный запрет на цензуру, и то, чем мы занимаемся, принципиально от цензуры отличается. Роскомнадзор реагирует на нарушения закона постфактум. Например, если отсутствует указание на то, что упомянутая в тексте или телесюжете организация относится к категории экстремистских.

- О каких организациях идет речь? Об ИГИЛ нужно писать, что её деятельность запрещена?

- Скажем, украинские «Правый сектор» и «УНА-УНСО» внесены в список экстремистских организаций Минюста. По поводу организаций из этого списка есть прямое требование в ст. 4 закона о СМИ: журналисты должны упоминать об их запрещенном статусе. А ИГИЛ, или ДАИШ, - это террористическая организация, список таких организаций ведёт ФСБ. В этом случае указание обязательно, но, по нашему глубокому убеждению, желательно. Ведь у ИГИЛ есть целые подразделения, занимающиеся пропагандой. Каждую неделю они выпускают новый ролик на русском языке и массированно выбрасывают его в Сеть - на сотни, а то и тысячи площадок, сайтов, форумов, в соцсе-



А. Жаров: «Мне кажется логичным контролировать точки входа Интернета к нам в страну».

Фото Дмитрия ЛЕБЕДЕВА/Коммерсантъ

ти. Благодаря особой методике их выявления за сутки-двое нам удаётся удалить все эти ролики. Поэтому террористы сменили тактику. Раньше они пытались посещать на максимальном количестве площадок один и тот же ролик. Теперь новые фильмы выпускают один за другим в расчёте на то, что кто-то успеет их увидеть. Основная цель террористов в Интернете - рекрутировать новых последователей. Поэтому очень важно указывать, что эта организация террористическая. С нашей стороны это маркер: «Мы знаем, кто вы. Вы - террористы».

- Пропанганда терроризма - это очень серьёзно. Но порой решения Роскомнадзора вызывают недоумение...

- Встречаются в нашей практике и курьёзные нарушения. В основном они связаны с исполнением решений региональных судов. Недавно к нам поступило принятое одним из судов решение о блокировке сайта, который рассказывал о производстве лампама. Но оказалось, что речь идёт о сетевой игре, в ходе которой нужно виртуально делать взрывчатку из ингредиентов, совершенно не соответствующих реальной рецептуре. Мы обратились к прокурору, инициировавшему решение суда, и дело пересмотрели.

КТО МОЖЕТ ОТКЛЮЧИТЬ ИНТЕРНЕТ?

- Не так давно советник президента Герман Клименко поднимал тему ограничения доступа в Интернет, ссылаясь на опыт Китая. Могут ли и в России появиться такие барьеры?

- Китайский проект «Золотой щит» ближе к определению цензуры. Эта система осуществляет предфильтрацию трафика. В том числе фильтрует информацию, поступающую в китайское интернет-пространство извне. Обслуживают её десятки тысяч высококвалифицированных специалистов.

У нас в Госдуме обсуждается законопроект о критической инфраструктуре Интернета. Мне кажется логичным контролировать точки входа Интернета к нам в страну, потому что его отключение может привести к техногенной катастрофе. Такой контроль есть во многих странах: в том же Китае, Турции, Германии и др.

- А кто контролирует Интернет и может его отключить?

- Сложный вопрос. Исторически Интернет был создан Пентагоном для военных коммуникаций. Позднее он превратился в гражданское средство связи. Но долгое время эта система финансировалась из бюджета США. Доменные имена и IP-адреса (это своего рода сетка, на которой держится Интернет, его инфраструктура) распределяет американская корпорация ICANN. В 2016 г. она формально стала международной организацией, но не надо забывать о том, что «кто девушку ужинает, тот её и танцует». Влияние США на эту организацию огромно.

ЧТО О ВАС ЗНАЕТ «ФОНАРИК»?

- Эдвард Сноуден обнародовал информацию о том, что через Интернет следят даже за лидерами государства, например за

кандидатом ФРГ Ангелой Меркель. Значит, даже правительственные информационные системы уязвимы? И кто следит за обычными гражданами?

Значит, даже правительственные информационные системы уязвимы? И кто следит за обычными гражданами?

- Уверен, что специальные службы в нашей стране на должном уровне обеспечивают защищённость правительственных каналов связи. И госслужащий обязан пользоваться именно ими. Все иные способы коммуникаций - только для информации, которая не относится к работе. Вообще нам всем нужно помнить, что мир изменился и мы живём в абсолютно прозрачном обществе. Смартфон - это вовсе не дружественный попутчик, наоборот, он постоянный и внимательный наблюдатель. Не раз уже специалисты рассказывали о функции принудительного фотографирования и других возможностях современных гаджетов. Устанавливая ту или иную программу в телефон или планшет, надо внимательно ознакомиться с пользователь-

ским соглашением. Например, многие скачивают очень простое бесплатное приложение «Фонарик». Но прочитайте условия пользования этой программой и увидите, что она получает из вашего телефона огромный объём информации, которой можно торговать. К примеру, перекачивает записную книжку, данные о вашем местонахождении. Зачем? Чтобы использовать ваши «большие пользовательские данные» в коммерческих целях. Так называемые большие данные - это, по сути, уголь и нефть будущего. Они позволяют прогнозировать, как люди того или иного возраста, пола, проживающие на определённой территории, будут себя вести в некой ситуации. Можно вычислить, какие товары и когда им предлагать. За такую информацию готовы бороться и корпорации, и спецслужбы других стран.

- Посоветуйте нашим читателям, как себя обезопасить.

- Определите, какими данными вы готовы делиться со всем миром - их можно держать в смартфоне, компьютере, отдавая себе отчёт в том, что они в любой момент могут быть отправлены в неизвестном направлении. Второй уровень - конфиденциальная информация, её нужно хранить на защищённых носителях. Наконец, абсолютно личную информацию можно записывать

на бумаге, благо все мы пока ещё умеем писать.

- Персональные данные мы оставляем не только в Интернете, но и в банках, больницах. А потом нам начинают названивать фирмы, купившие эти данные...

- Если вам звонит некий человек и предлагает услуги какой-то конторы, в первую очередь выясните название юрлица, которое он представляет. А затем сообщите, что вы требуете удалить ваши персональные данные из базы контактов. После этого следует написать жалобу в региональное подразделение Роскомнадзора. И тогда в эту фирму придёт наш инспектор.

О том, какой далеко не виртуальной опасности подвергаются в Сети дети, и о борьбе с «группами смерти» читайте в продолжении беседы на с. 17.

ГЕПАТИТ, ЦИРРОЗ - НЕ ПРИГОВОР!

Несколько лет назад мне поставили диагноз «гепатит С». Все говорили, что ничего страшного. Да и сама я прекрасно себя чувствовала. Поэтому не придавала этому значения. Потом стала уставать, пропал аппетит, появились отёки, начались проблемы с желудком, стали беспокоить головные боли. Даже не предполагала, что это - признаки болезни. Но всё же решила обследоваться. И пришла в ужас: цирроз печени. В 55 лет! У меня маленькие внуки. Их нужно вырастить, а значит, бороться за жизнь. Но как? Знаю, что есть разные варианты лечения, но никак не определюсь, какому из них можно доверять...

Светлана К., Тюмень

Есть такая программа «Гепатиту нет». Она защищает клетки печени, препятствует их разрушению. Рекомендуются при гепатитах, циррозах и онкологии и, как говорят специалисты, работает на любой стадии болезни. Они считают, что эта программа необходима всем, кто заботится о здоровье своей печени. Но, конечно, лучше подробно проконсультироваться и все вопросы, которые у вас могут возникнуть, задать самим специалистам программы «Гепатиту нет». Это можно сделать по бесплатному телефону 8-800-333-57-03. На ваш звонок ответят ежедневно с 9.00 до 20.00. Реклама

ДОСЬЕ

Александр ЖАРОВ, руководитель Роскомнадзора. Родился в 1964 г. в Челябинске. Окончил Челябинский государственный медицинский университет, позднее - Российскую академию госслужбы при Президенте РФ. В 2008 г. был назначен заместителем министра связи. Женат, 6 детей.

1 марта 2016 г.

Глава 2. Понятие информационных угроз и их виды.

2.1. Информационные угрозы, их виды, причины.

С конца 80-ых, начале 90-х годов проблемы, связанные с защитой информации беспокоят как специалистов в области компьютерной безопасности, так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями, вносимыми компьютерной технологией в нашу жизнь.

Современные автоматизированные информационные системы (АИС) в экономике — сложные механизмы, состоящие из большого количества компонентов различной степени автономности, связанных между собой и обменивающихся данными. Практически каждый из них может выйти из строя или подвергнуться внешнему воздействию.

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Под угрозой безопасности информации (информационной угрозой) понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения конфиденциальности информации. Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым угроза оперативности использования или доступности информации.

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - злоумышленником (хакер, кречер). Потенциальные злоумышленники называются **источниками угрозы**.

Чаще всего **угроза** является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует **окно опасности**, возможны успешные **атаки** на ИС.

Отметим, что некоторые **угрозы** нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, **угроза** отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных **угрозах**, а также об **уязвимых местах**, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же «Проблему 2000»), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

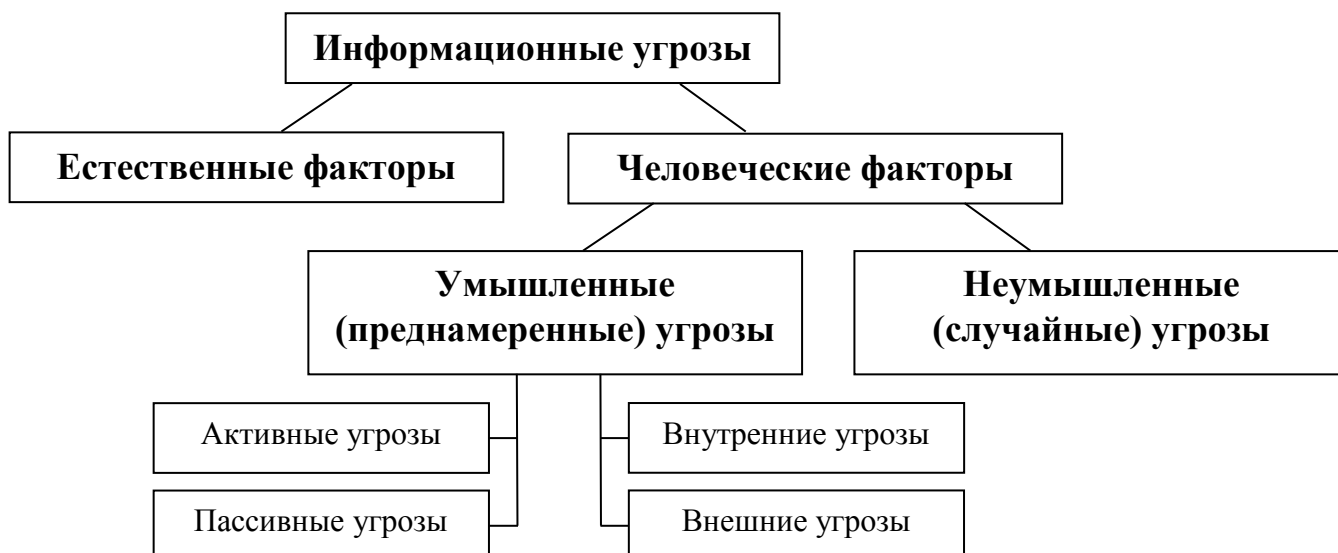
Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнута открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ,

зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Итак, реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или заблокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.





Классификация угроз безопасности информации



Информационные угрозы могут быть обусловлены:

- естественными факторами (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины);

- человеческими факторами. Последние, в свою очередь, подразделяются на:

- угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

- угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение

носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на *внутренние*, возникающие внутри управляемой организации, и *внешние*.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение *промышленный шпионаж* - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование ресурсов; несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания.

Средствами реализации угрозы *раскрытия конфиденциальной информации* могут быть несанкционированный доступ к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.

Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и несанкционированный доступ к защищаемой информации (106). При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом (рис. 2).



Рис. 2. Действия и события, нарушающие информационную безопасность.

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможна *бесконтрольная утечка конфиденциальной информации* по визуально-оптическим, акустическим, электромагнитным и другим каналам.

По физической природе возможны следующие средства переноса информации:

- Световые лучи.
- Звуковые волны.
- Электромагнитные волны.
- Материалы и вещества.

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

- визуально-оптические;
- акустические (включая и акустико-преобразовательные);
- электромагнитные (включая магнитные и электрические);
- материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида - твердые, жидкие, газообразные).

Визуально-оптические каналы - это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источниками конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах.

Акустические каналы. Для человека слух является вторым по информативности после зрения. Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20000 Гц, и содержащихся в человеческой речи - от 100 до 6000 Гц.

В свободном воздушном пространстве акустические каналы образуются в помещениях при ведении переговоров в случае открытых дверей, окон, форточек. Кроме того, такие каналы образуются системой воздушной вентиляции помещений. В этом случае образование каналов существенно зависит от геометрических размеров и формы воздуховодов, акустических характеристик фасонных элементов задвижек, воздухораспределителей и подобных элементов.

Электромагнитные каналы. Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10000 м. (частоты мене 30 Гц) до сублимированных с длиной волны 1 - 0,1 мм. (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения, как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые - наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи

создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне их расположения.

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства бракованные изделия, черновые материалы и др.

Очевидно, что каждый источник конфиденциальной информации может обладать в той или иной степени какой-то совокупностью каналов утечки информации. Причины утечки связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

К факторам утечки могут, например, относиться:

- недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;
- использование неаттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами.

Несанкционированный доступ (НСД)

Это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам.

Есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;
- инициативное сотрудничество;

- склонение к сотрудничеству со стороны взломщика;
- пытки;
- подслушивание;
- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Менеджерам следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- использование неаттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми организационными и инженерно-техническими мерами и др.

Пример №1 (М. Накамото "Япония борется с утечками", "Понедельник" от 02.03.2004г.)

В скандалах и конфликтах, связанных с промышленным шпионажем, японские компании долгое время выступали в роли ответчиков - одним из самых известных примеров этого стало дело 1982 г., когда сотрудников Hitachi обвинили в краже интеллектуальной собственности у корпорации IBM. Однако теперь, по мере обострения международной конкуренции в областях, где японцы традиционно доминировали, они сами все чаще становятся жертвами промышленных шпионов.

Корпорация Sharp, тщательно охраняющая собственные технологические разработки, разместила свой суперсовременный завод по производству жидкокристаллических панелей в местечке Камеяма - в глухой горной местности, вдали от посторонних взоров. Но и здесь гигант электронной промышленности не чувствует себя в полной безопасности: с определенного времени тревогу сотрудников Sharp стал вызывать таинственный автомобиль, примерно раз в месяц объезжавший вокруг секретного объекта корпорации. Подозрительная машина, по мнению представителей Sharp, вполне может принадлежать агенту конкурирующей компании, надеющейся выведать важные детали чужого ноу-хау.

«Утечка технологий из Японии снижает конкурентоспособность страны и приводит к сокращению занятости, - утверждает Йосинори Комия, директор Агентства по защите интеллектуальной собственности при Министерстве экономики, торговли и промышленности (МЭТП). Мы признаем, что некоторые технологии подлежат передаче за границу; но сейчас часто передаются и такие технологии, которые руководители компаний стремятся сохранить в тайне».

Особенно болезненной для японского правительства эта проблема стала сейчас, когда соседи страны восходящего солнца добились серьезных успехов на рынке высоких технологий. Даже самым крупным и сильным в рыночном отношении японским компаниям приходится теперь занимать оборонительную позицию и тщательно оберегать свою интеллектуальную собственность.

По данным МЭТП, многие компании, становящиеся жертвами промышленного шпионажа, стремятся не раздувать скандал, поскольку виновными в кражах оказываются их собственные сотрудники, а не агенты извне. Как признает Йокио Сотоку, вице-президент Matsushita, в японском бизнесе по-прежнему нередки нарушения со стороны "пятой колонны", например со стороны сотрудников, работающих в конкурирующих фирмах по выходным.

Исследования МЭТП показывают также, что одним из каналов утечки коммерческой информации становятся бывшие сотрудники японских компаний, устраивающиеся на работу в других азиатских странах и уносящие с собой ноу-хау своих прежних работодателей. МЭТП выделила основные пути, по которым конфиденциальная информация утекает к конкурентам японских компаний, среди которых - копирование данных сотрудниками в нерабочее время; работа сотрудников по совместительству в конкурирующих компаниях (например, в выходные); создание совместного предприятия с зарубежной компанией при недостаточно проработанной политике информационной безопасности; нарушение партнером-поставщиком оборудования соглашения о сохранении конфиденциальности и т.п.

МЭТП отмечает, что многие компании, не осознавшие вовремя риска, связанного с утечкой ноу-хау, несут из-за этого значительные убытки, но суды в таких случаях относятся к ним без сочувствия, поскольку речь идет о халатности и беспечности. Из 48 судебных дел, в ходе которых японские компании требовали компенсации за ущерб от кражи интеллектуальной собственности, только в 16 случаях эти требования были признаны обоснованными.

Пример №2 (Б. Госсидж "Болтун - находка для конкурента" "Понедельник" от 16.02.2004г.)

Фил Сипович, основатель и глава американской компании Everynetwork, специализирующейся на ИТ-консалтинге, никогда не считал себя болтливым или склонным к неосмотрительным высказываниям. Ведя переговоры о возможном партнерстве с одним из конкурентов, Сипович старался не открывать карты, говоря лишь о том, что считал действительно необходимым для продвижения сделки.

После переговоров исполненный оптимизма Сипович вместе со своим юристом составил проект договора о неразглашении и послал его партнеру по факсу. Ответ пришел только через несколько недель и оказался неожиданным - партнер заявил, что не заинтересован ни в слиянии, ни в альянсе, ни в чем-либо другом... А еще через месяц один из клиентов Сиповича позвонил и сообщил, что к нему обратился с предложением другой консультант. Как оказалось, тот самый несостоявшийся партнер! Только тут Сипович вспомнил, что в ходе переговоров случайно упомянул трех своих ключевых клиентов. Его подозрения оправдались: скоро два других клиента тоже получили предложения от альтернативного консультанта. «Это не было масштабной маркетинговой кампанией, они искали подход лишь к тем клиентам, которых я сам упомянул,- констатирует Сипович. - Сделать я уже ничего не мог, поскольку сам проболтался».

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы, представленные на рис.3.



Рис. 3. Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.)

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;

- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо-и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые **"обиженные" сотрудники** - нынешние и бывшие. Как правило, они стремятся нанести вред организации- "обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Типы и субъекты угроз

	Тип угроз	Оператор	Руководитель	Программист	Инженер (техник)	Пользователь	Конкурент
1.	Изменение кодов	+		+			
2.	Копирование файлов	+		+			
3.	Уничтожение файлов	+	+	+		+	+
4.	Присвоение программ			+	+		+
5.	Шпионаж	+	+	+			+
6.	Установка подслушивания			+	+		+
7.	Саботаж	+		+	+		+
8.	Продажа данных	+	+	+		+	
9.	Воровство		+	+		+	+

И даже если сотрудник не является злоумышленником, он может ошибаться не намеренно вследствие усталости, болезненного состояния и пр.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию. или компрометации указанных ресурсов. Данная угроза, чаще всего, является следствием ошибок в программном обеспечении АИС.

Уничтожение компьютерной информации - это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации - это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо

отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Модификация компьютерной информации - это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных - «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя» (ч. 1 ст. 1 Закона РФ от 23 сентября 1992 года "О правовой охране программ для электронных вычислительных машин и баз данных"). Другими словами это означает изменение ее содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Копирование компьютерной информации - изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий.

Основными типовыми путями несанкционированного доступа к информации, являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- хищение носителей информации и документальных отходов;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- включение в библиотеки программ специальных блоков типа "Троянский конь";
- незаконное подключение к аппаратуре и линиям связи;
- злоумышленный вывод из строя механизмов защиты;
- внедрение и использование компьютерных вирусов.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов, ибо эффективной защиты против них разработать не удалось. Остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности

Ниже перечисляются наиболее распространенные технические угрозы и причины, в результате которых они реализуются:

- несанкционированный доступ к информационной системе - происходит в результате получения нелегальным пользователем доступа к информационной системе;

- раскрытие данных - наступает в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или намеренным образом;
- несанкционированная модификация данных и программ - возможна в результате модификации, удаления или разрушения человеком данных и программного обеспечения локальных вычислительных сетей случайным или намеренным образом;
- раскрытие трафика локальных вычислительных сетей - произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом тогда, когда информация передается через локальные вычислительные сети;
- подмена трафика локальных вычислительных сетей - это его использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а на самом деле это не так;
- неработоспособность локальных вычислительных сетей - это следствие осуществления угроз, которые не позволяют ресурсам локальных вычислительных сетей быть своевременно доступными.

Способы воздействия угроз на информационные объекты подразделяются на:

- информационные;
- программно-математические;
- физические;
- радиоэлектронные;
- организационно-правовые.

К информационным способам относятся:

- нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;
- несанкционированный доступ к информационным ресурсам;
- манипулирование информацией (дезинформация, сокрытие или сжатие информации);
- нарушение технологии обработки информации.

Программно-математические способы включают:

- внедрение компьютерных вирусов;
- установка программных и аппаратных закладных устройств;
- уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

- уничтожение или разрушение средств обработки информации и связи;
- уничтожение, разрушение или хищение машинных или других носителей информации;
- хищение программных или аппаратных ключей и средств криптографической защиты информации;

- воздействие на персонал;
- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления. Радиоэлектронными способами являются:

- перехват информации в технических каналах ее возможной утечки;
- внедрение электронных устройств перехвата информации в технические средства и помещения;

- перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

- воздействие на парольно-ключевые системы;
- радиоэлектронное подавление линий связи и систем управления. Организационно-правовые способы включают:

- невыполнение требований законодательства о задержке в принятии необходимых нормативно-правовых положений в информационной сфере;
- неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Суть подобных угроз сводится, как правило, к нанесению того или иного ущерба предприятию.

Проявления возможного ущерба могут быть самыми различными:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации в работе всего предприятия.

Непосредственный вред от реализованной угрозы, называется воздействием угрозы.

Идентификация угроз предполагает рассмотрение воздействий и последствий от реализации угроз. Обычно воздействие угроз приводит к раскрытию, модификации, разрушению информации или отказу в информационном обслуживании. Более значительные долговременные последствия реализации угрозы приводят к потере бизнеса, нарушению тайны, гражданских прав, потере адекватности данных, потере человеческой жизни и иным долговременным эффектам.

Знание возможных угроз, а также уязвимых мест защиты, необходимо, чтобы выбрать наиболее экономичные средства обеспечения безопасности. Самыми частыми и опасными, с точки зрения размеров ущерба, являются не угрозы даже, а непреднамеренные ошибки пользователей, операторов, системных администраторов и других, обслуживающих информационные системы лиц. Иногда такие ошибки являются угрозами (неправильно преднамеренно введенные данные, ошибки в программе), а иногда это просто следствие человеческих слабостей, которыми, однако, могут воспользоваться злоумышленники - таковы обычно ошибки администрирования, 65% потерь - следствие непреднамеренных ошибок.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль за правильностью совершаемых действий.

Угрозы, исходящие от окружающей среды, весьма разнообразны. В первую очередь следует выделить нарушение инфраструктуры - аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т. п. На долю огня, воды и аналогичных "врагов", среди которых самый опасный - низкое качество электропитания, приходится 13% потерь, которые обычно несут информационные системы.

Внешние субъекты могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков услуг;
- представители надзорных организаций и аварийных служб;
- представители силовых структур.

Внутренние субъекты, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программноаппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- представители службы защиты информации;
- вспомогательный персонал (уборщики, охрана);
- технический персонал (жизнеобеспечение, эксплуатация).

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

- средства связи;
- сети инженерных коммуникаций (водоснабжения, канализации);

- транспорт.

Внутренними источниками потенциальных угроз безопасности информации могут быть:

- аппаратно- программные средства;
- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные технические средства (охраны, сигнализации, телефонии);
- другие технические средства, применяемые в учреждении.

Взаимодействие автоматизированной информационной системы (АИС)

предприятия через Internet со смежными АИС банков, страховых компаний, налоговых органов и пр. может сделать организацию более уязвимой с точки зрения информационной безопасности.

При взаимодействии интегрированной информационной системы управления предприятием с Internet основные угрозы для информационной безопасности организации представляют:

- несанкционированные внешние воздействия из Internet на информационную систему для получения доступа к ее ресурсам и (или) нарушения ее работоспособности;
- отказы аппаратного и программного обеспечения подсистемы взаимодействия (нарушение работы каналов связи с Internet, телекоммуникационного оборудования локальной вычислительной сети, межсетевых экранов);
- непреднамеренные действия сотрудников организации, приводящие к непроизводительным затратам времени и ресурсов, разглашение сведений ограниченного пользования через Internet или нарушению работоспособности подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet;
- преднамеренные действия сотрудников организации, приводящие к разглашению сведений ограниченного пользования через Internet, а также нарушению работоспособности подсистемы взаимодействия информационной системы с Internet или же недоступность предоставляемых услуг через Internet;
- непреднамеренные действия лиц, осуществляющих администрирование подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, приводящие к разглашению сведений ограниченного пользования или нарушению взаимодействия с Internet;
- преднамеренные действия (в корыстных целях, по принуждению третьих лиц, со злым умыслом и т.п.) сотрудников организации, отвечающих за установку, сопровождение, администрирование системного, сетевого или прикладного программного обеспечения, технических средств защиты и обеспечения информационной безопасности подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, которые (действия) приводят к разглашению сведений ограниченного пользования или нарушения взаимодействия с Internet.

Приводимая ниже классификация охватывает только умышленные угрозы безопасности автоматизированных информационных систем экономических объектов (АИСЭО), оставляя в стороне такие воздействия как стихийные бедствия, сбои и отказы оборудования и др. Реализацию угроз в дальнейшем будем называть атакой.

Угрозы безопасности можно классифицировать по следующим признакам:

1. По цели реализации угрозы. Реализация той или иной угрозы безопасности может преследовать следующие цели:

- нарушение конфиденциальной информации;
- нарушение целостности информации;
- нарушение (частичное или полное) работоспособности.

2. По принципу воздействия на объект:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлам данных, каналу связи и т.д.);
- с использованием скрытых каналов.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.

3. По характеру воздействия на объект.

По этому критерию различают активное и пассивное воздействие.

Активное воздействие всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. На основе такого рода анализа можно иногда получить довольно интересную информацию. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

4. По причине появления используемой ошибки защиты.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью политики безопасности реальной системе. Это означает, что разработанная политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий;

- ошибками административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной организации. Например, согласно политике безопасности должен быть запрещен доступ пользователей к определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям.

- ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации. Примером такой ошибки может служить ошибка в программе аутентификации пользователя, когда при помощи определенных действий пользователь имеет возможность войти в систему без пароля.

- ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств.

5. По способу воздействия на объект атаки (при активном воздействии):

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа.

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом. Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных и программе, в частности «маскарад», при котором пользователь присваивает себе каким-либо образом полномочия другого пользователя выдавая себя за него.

6. По объекту атаки. Одной из самых главных составляющих нарушения функционирования АИС является объект атаки, т.е. компонент системы, который подвергается воздействию со стороны злоумышленника. Определение объекта атаки позволяет принять меры по ликвидации последствий нарушения, восстановлению этого компонента, установке контроля по предупреждению повторных нарушений и т.д.

Воздействию могут подвергаться следующие компоненты:

- АИС в целом - злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого обычно используются метод «маскарада», перехват или подделка пароля, взлом или доступ к системе через сеть;

- объекты системы - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности, например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности);

- субъекты системы - процессы и подпроцессы с участием пользователей. Целью таких атак является либо прямое воздействие на работу процесса - его приостановка, изменение привилегий или характеристик (приоритета, например), либо обратное воздействие - использование злоумышленником привилегий, характеристик и т.д. другого процесса в своих целях. Частным случаем такого воздействия является внедрение злоумышленником вируса в среду другого процесса и его выполнение от имени этого процесса. Воздействие может осуществляться на процессы пользователей, системы, сети;

- каналы передачи данных - пакеты данных, передаваемые по каналу связи и сами каналы. Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на каналы - специфический род атак, характерный для сети. К нему относятся: прослушивание канала и анализ трафика (потока сообщений) - нарушение конфиденциальности передаваемой информации; подмена или модификация сообщений в каналах связи и на узлах ретрансляторах - нарушение целостности передаваемой информации; изменение топологии и характеристик сети, правил коммутации и адресации - нарушение доступности сети.

7. По используемым средствам атаки.

Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ системы хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АИСЭО без разрешения администратора безопасности системы.

8. По состоянию объекта атаки. Состояние объекта в момент атаки может оказать существенное влияние на результаты атаки и на работу по ликвидации ее последствий.

Объект атаки может находиться в одном из трех состояний:

- хранения - на диске, магнитной ленте, в оперативной памяти или любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;
- передачи - по линии связи между узлами сети или внутри узла. Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;
- обработки - в тех ситуациях, когда объектом атаки является процесс пользователя.

Подобная классификация показывает сложность определения возможных угроз и способов их реализации. Это еще раз подтверждает тезис, что определить все множество угроз для АИСЭО и способов их реализации не представляется возможным.

Угрозы и уязвимости информационной системы ОАО «ВМЗ»

Угроза	Уязвимости
1. Автоматизированное рабочее место сотрудника	
1. Физический доступ нарушителя к рабочему месту.	1. Отсутствие системы контроля доступа сотрудников к чужим рабочим местам.
	2. Отсутствие системы видеонаблюдения на предприятии.
2. Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации.	1. Отсутствие соглашения о неразглашении между работником и работодателем.
	2. Нечеткая регламентация ответственности сотрудника предприятия.
3. Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов.	1. Отсутствие ограничения доступа пользователей к сети интернет и к внутренней корпоративной сети.
2. Конфиденциальная информация	
1. Физический доступ нарушителя к носителям.	1. Неорганизованность контрольно-пропускного режима в организации.
	2. Отсутствие видеонаблюдения в организации.
2. Разглашение конфиденциальной информации, используемой в документах, вынос носителей за пределы контролируемой зоны.	1. Отсутствие соглашения о неразглашении конфиденциальной информации.
	2. Нечеткое распределение ответственности за документы (носители конфиденциальной информации) между сотрудниками организации.
3. Несанкционированное копирование, печать и размножение носителей конфиденциальной информации.	1. Нечеткая организация конфиденциального документооборота в организации.
	2. Неконтролируемый доступ сотрудников к копировальной и множительной технике.

Информационная безопасность

Защита информации

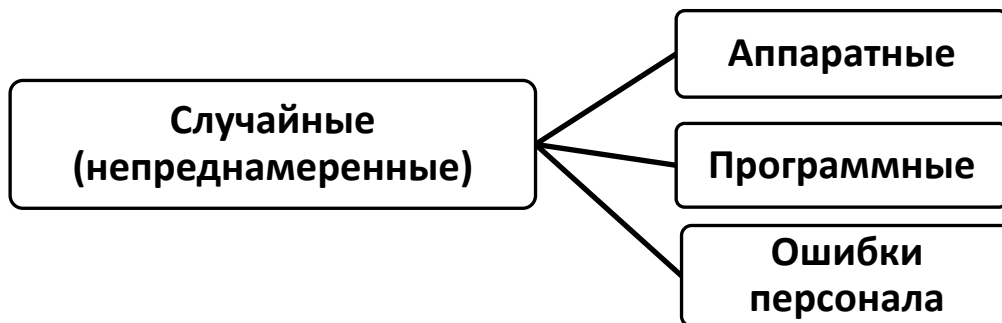
Угрозы безопасности информации

совокупность условий и факторов, создающих потенциальную или реальную опасность утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на нее.

Угрозы воздействия на информацию

- Случайные
- Преднамеренные

Случайные угрозы безопасности информации



Умышленные угрозы безопасности информации

связаны с различными действиями человека, которые преследуют цель нанесения ущерба управляемой системе или пользователям



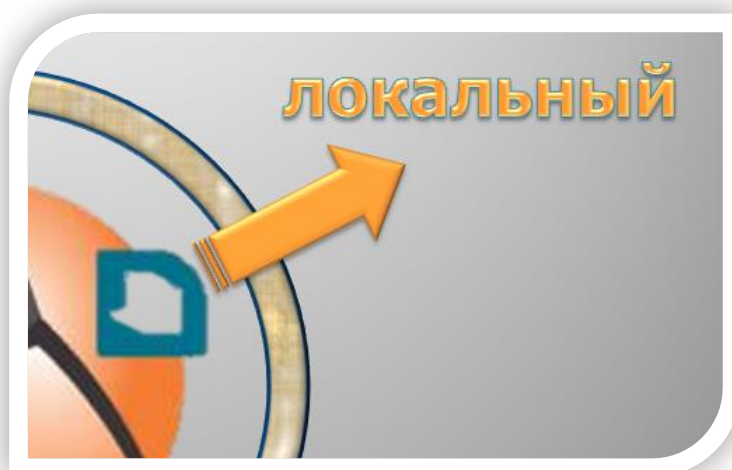
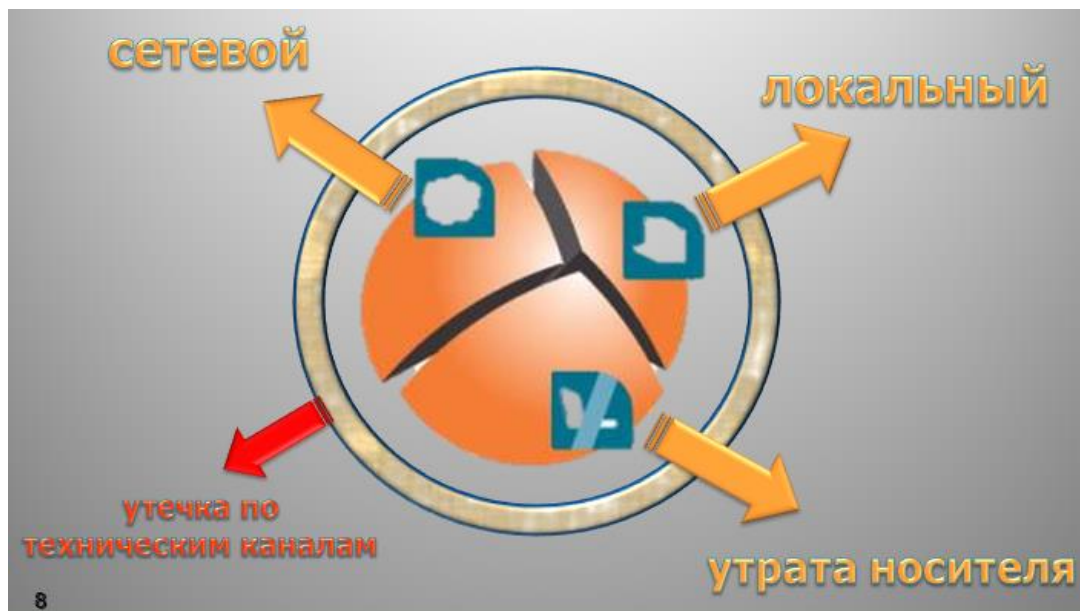
Угрозы безопасности информации (согласно Концепции ИБ ФНС)

- угрозы нарушения конфиденциальности
- угрозы нарушения целостности информации
- угрозы нарушения доступности информации

Утечка конфиденциальной информации

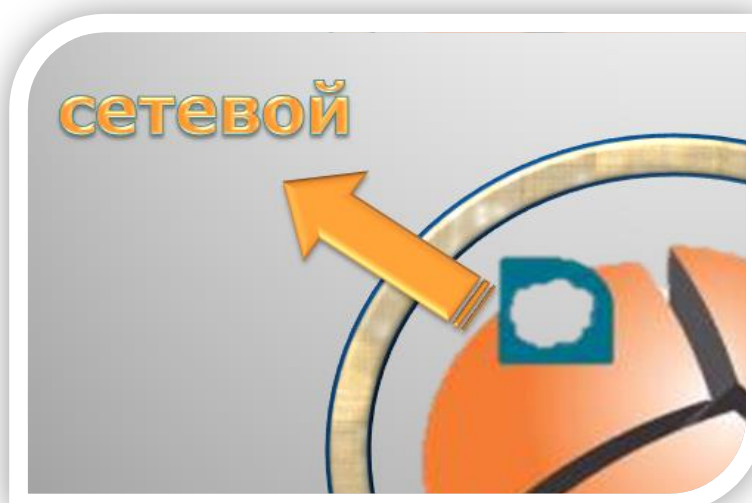
бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы

Основные пути утечки информации

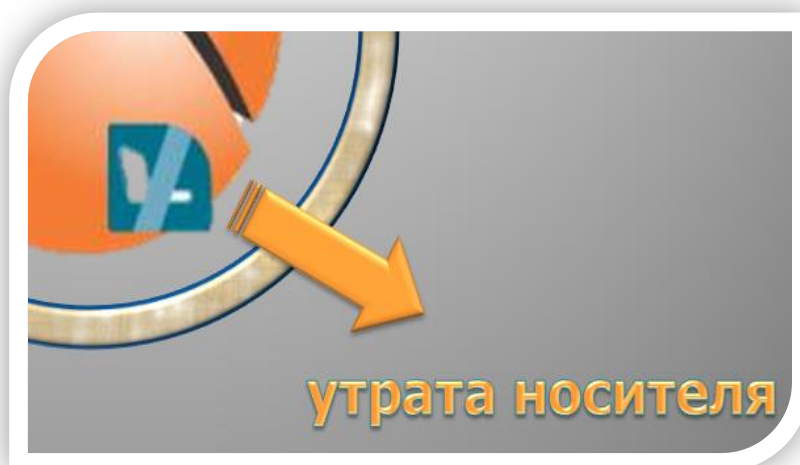


Копирование данных:

- дискеты
- USB-накопители
- CD/DVD-накопители
- локальная печать («твердые копии»)



- почта (e-mail, web mail)
- передача файлов (локальная сеть, ftp, Wi-Fi)
- сетевая печать
- удаленное администрирование



- кража носителя
- потеря носителя
 - локальный носитель (дискета, USB-накопитель, CD/DVD-накопитель)
 - ноутбук
 - смартфон, КПК



- виброакустический
- побочные электромагнитные излучения
- активный перехват по проводным линиям
- радио и видеозакладки
- иные

2.2. Вредоносные программы.

Вирусы и антивирусы

Антон Благовещенский

Если раньше вредоносные программы для компьютера были просто результатом шалостей ленивых программистов, то теперь это серьезный криминальный бизнес, в котором может быть замешан любой пользователь ПК.

Сравнительно недавно, в середине и конце 90-х годов, так называемые компьютерные вирусы в большинстве своем создавали студенты или изнывающие от безделья программисты, решившие попробовать свои силы. В те времена вирус представлял собой программу, которая уничтожала файлы на компьютере, тормозила его работу и вообще мешала жить.

Но времена изменились. Компьютеры стали значительно «умнее» и многократно увеличили свои вычислительные способности. Доступом в Интернет обзавелись не только «избранные», но и вполне обычные люди - выходить в Сеть на приемлемой скорости могут примерно 50 млн человек в России. Появились электронные деньги, многие интернет-магазины начали принимать к оплате банковские карты.

Так что нет ничего удивительного в том, что и вредоносные программы претерпели серьезные изменения. Теперь они занимаются тем, что крадут конфиденциальную информацию (имена, пароли, данные о пластиковых картах) и «заражают» пользовательский компьютер, превращая его в инструмент для совершения киберпреступлений. Одни внедряются на компьютер и воруют персональные данные, другие превращают ПК в «компьютер-зомби», который незаметно для владельца веером рассылает рекламные письма (спам). Причем «жертва» обычно ни о чем не догадывается.

Как вирус проникнет на компьютер?

В прошлом веке вирусы чаще всего «приносили на дискете». Вставив гибкий диск в дисковод и запустив зараженную компьютерную игру, пользователь ПК мог получить целый букет проблем: нужные файлы пропали, компьютер пищит и не загружается. Затем, когда дискеты морально устарели, вирусы поселились на компакт-дисках с пиратскими версиями популярных программ - операционных систем, офисных пакетов, графических редакторов.

Но с повсеместным распространением Интернета вредоносные программы стали распространяться именно с его помощью. Обычно они проникают в компьютер посредством электронной почты, ISQ, через зараженные сайты или вместе с загруженными из Сети программами. Кроме того, недоработки («дыры») в установленных на компьютер программах также могут использоваться для того, чтобы поселить злонамеренную утилиту в недрах ПК. Наконец, не стоит забывать и о том, что USB-накопители, или флэшки, пришедшие на смену компакт-дискам, также могут быть заражены.

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Ниже рассмотрим некоторые (самые распространенные) виды подобных программ:

«Троянский конь» - программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия с древнегреческим «троянским конем» таким образом, вполне оправдана - в не вызывающей подозрений оболочке таится угроза.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователем. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне).

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий - это не мешает выполнению несанкционированных действий.

Вирус - это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.

Своим названием компьютерные вирусы обязаны определенному сходству с вирусами биологическими:

- способностями к саморазмножению;
- высокой скорости распространения;
- избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем);
- наличие в большинстве случаев определенного инкубационного периода;
- способности «заражать» еще незараженные системы;
- трудности борьбы с вирусами и т.д.

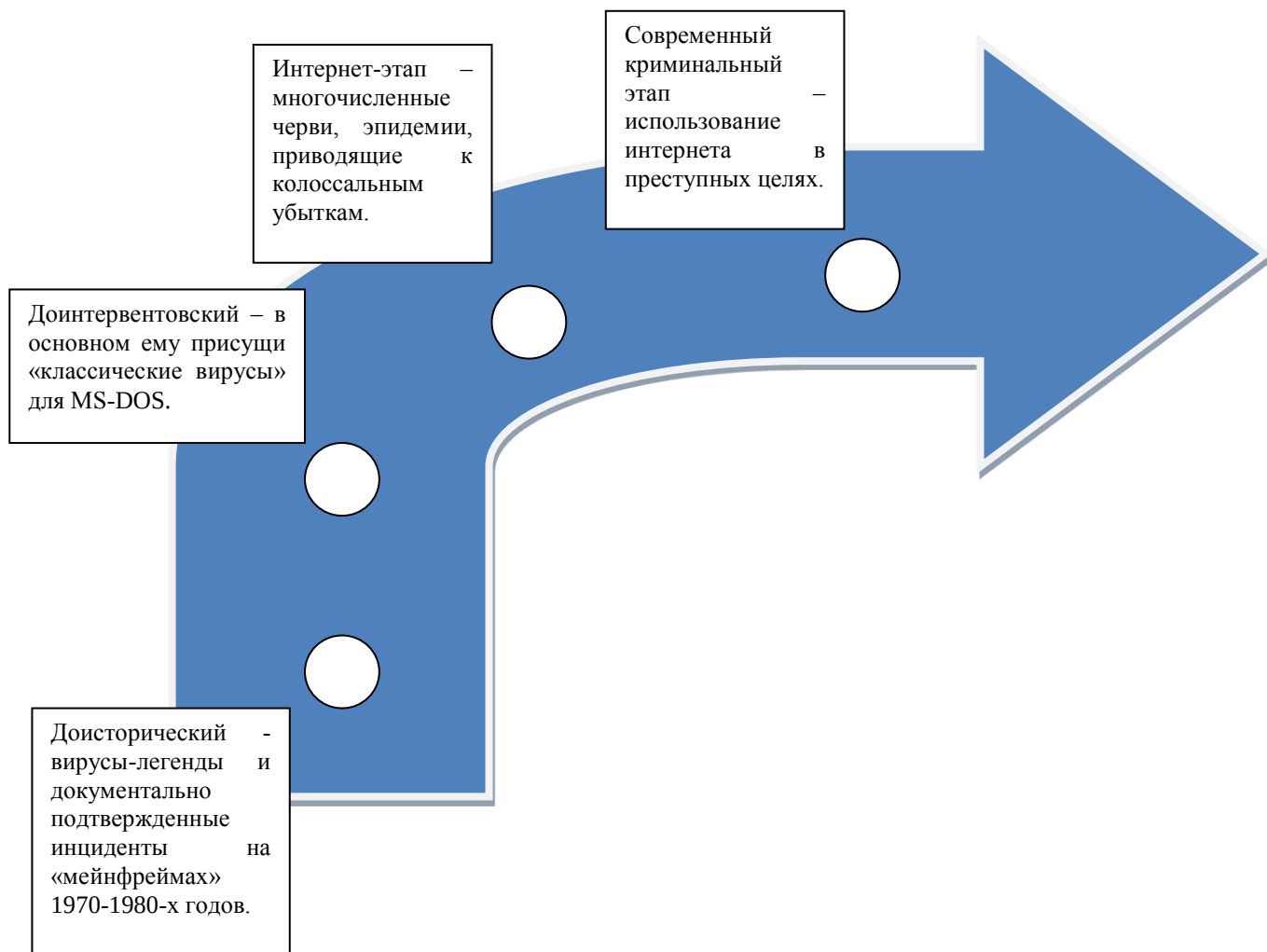


Рис. 1. История компьютерных вирусов.

Среда обитания	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Рис. 2. Основные классы вирусов.

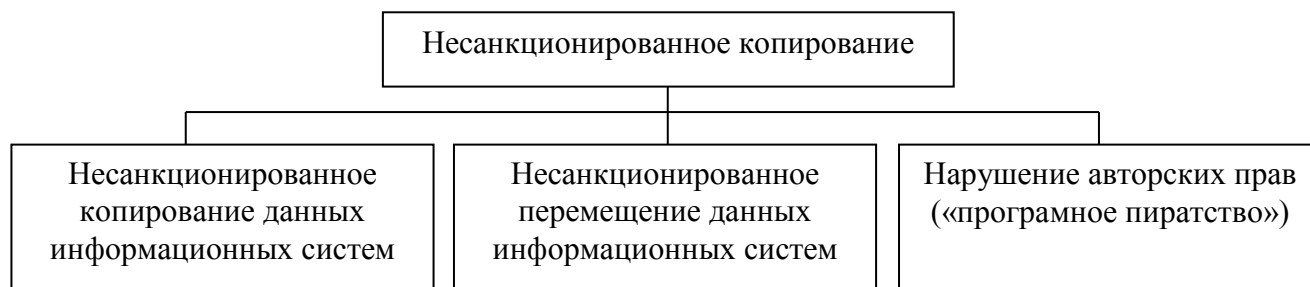


Рис. 3. Копирование информации.

В последнее время к этим особенностям, характерным для вирусов компьютерных и биологических, можно добавить еще и постоянно увеличивающуюся быстроту появления модификаций и новых поколений вирусов, что можно объяснить идеями злоумышленников определенного склада ума.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия.

Процесс заражения вирусом программных файлов можно представить следующим образом. В зараженной программе код последней изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы-вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы. Если вирус записывается в конец программы, то он корректирует код программы с тем, чтобы получить управление первым. После этого управление передается программе-вирусоносителю, и та нормально выполняет свои функции. Более изощренные вирусы могут для получения управления изменять системные области накопителя (например, сектор каталога), оставляя длину и содержимое заражаемого файла без изменений.

Загрузочные вирусы. От файловых вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). На включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно поражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус. Так, например, при попытке загрузить компьютер с гибкого диска происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд.

В частности, к таким документам относятся документы текстового процессора MicrosoftWord. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.

«Червь» - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот

узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса - вирус Морриса (или, вернее, «червь Морриса»), поразивший сеть Internet в 1988 г. Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой считаются дружественными и доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

«Жадные» программы - это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая сообщение о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы.

Другой пример «жадной» программы - программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Что такое шпионские программы?

Как следует из названия, эти программы предназначены для сбора данных и отправки их третьей стороне без вашего ведома и согласия. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера.

Захватчики паролей. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Методика воздействия вредоносных программ в значительной мере зависит от организации обработки информации в системе, разработанной политики безопасности, возможностей установленных средств защиты, а также добросовестности администратора и оператора. Для реализации НСД существует два способа:

- во-первых, можно преодолеть систему защиты, то есть путем различных воздействий на нее прекратить ее действия в отношении себя или своих программ. Это сложно, трудоемко и не всегда возможно, зато эффективно;

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов и пр.

В подавляющем большинстве случаев НСД становится возможным из-за непродуманного выбора средств защиты, их некорректной установки и настройки, плохого контроля работы, а также при небрежном отношении к защите своих собственных данных.

Незаконное использование привилегий

Злоумышленники, применяющие данный способ атаки, обычно используют штатное

программное обеспечение (системное или прикладное), функционирующее в нештатном режиме. Практически любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, при сбоях оборудования или средства, которые способны функционировать с нарушением существующей политики безопасности. В некоторых случаях пользователь должен иметь возможность доступа ко всем наборам системы (например, при внезапной проверке).

Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Для того чтобы уменьшить риск от применения таких средств большинство систем защиты реализует такие функции с помощью набора привилегий - для выполнения определенной функции требуется определенная привилегия. В этом случае каждый пользователь получает свой набор привилегий, обычные пользователи - минимальный, администраторы - максимальный (в соответствии с принципом минимума привилегий).

Естественно, при таких условиях расширенный набор привилегий - заветная мечта любого злоумышленника. Он позволит ему совершать практически любые действия, причем, возможно, даже в обход всех мер контроля. Нарушения, совершаемые с помощью незаконного использования привилегий, являются активным воздействием, совершаемым с целью доступа к какому-либо объекту или системе в целом.

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий операционной системы UNIX), либо в случае халатности при управлении системой и привилегиями в частности (например, при назначении расширенного набора привилегий всем подряд).

Атаки «салями»

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Например, 6,5% годовых от \$102,87 за 31 день составит \$0,5495726. Банковская система может округлить эту сумму до \$0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону - до \$0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день. Его прибыль таким образом составит \$1000, т.е. около \$300 000 в год.

Отсюда и происходит название таких атак - как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков. Естественно, такие атаки имеют смысл лишь в тех организациях, где осуществляется не менее 5000 - 10000 транзакций в день, иначе не имеет смысла рисковать, поскольку в случае обнаружения преступника просто определить. Таким образом, атаки «салями» опасны в основном для крупных банков.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете миллионы.

«Скрытые каналы»

«Скрытые каналы» - пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным.

«Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («тройных коней»).

Например, программист банка не всегда имеет доступ к именам и балансам депозитных счетов. Программист системы, предназначенной для обработки ценных бумаг, может не иметь доступ к предложениям о покупке или продаже. Однако при создании таких систем он может предусмотреть способ получения интересующих его сведений. В этом случае программа скрытым способом устанавливает канал связи с этим программистом и сообщает ему требуемые сведения.

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации, по характеру воздействия являются пассивными, нарушение состоит только в передаче информации. Для организации «скрытых каналов» может использоваться как штатное программное обеспечение, так и специально разработанные «тройные» или вирусные программы. Атака обычно производится программным способом.

«Скрытым каналом» может явиться передача информации о наличии или отсутствии какого-либо набора данных, его размере, дате создания или модификации и т.д.

Также существует большое количество способов организации связи между двумя процессами системы. Более того, многие операционные системы имеют в своем распоряжении такие средства, так как они очень облегчают работу программистов и пользователей. Проблема заключается в том, что очень трудно отделить неразрешенные «скрытые каналы» от разрешенных, то есть тех, которые не запрещаются системной политикой безопасности. В конечном счете все определяется ущербом, который может принести организация «скрытых каналов».

Отличительными особенностями «скрытых каналов» является их малая пропускная способность (по ним обычно можно передавать только небольшое количество информации), большие трудности их организации и обычно небольшой наносимый ими ущерб.

«Маскарад»

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. При этом такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Цель «маскарада» - сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий.

«Маскарад» - это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» - присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций.

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Сборка мусора»

После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитывать такие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Взлом системы»

Под «взломом системы» понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями).

«Взлом системы» - умышленное, активное воздействие на систему в целом. «Взлом системы» обычно происходит в интерактивном режиме.

Поскольку имя пользователя не является секретом, объектом «охоты» обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор

возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа.

«Люки»

Люком называется не описанная в документации на программный продукт возможность работы с этим программным продуктом. Сущность использования люков состоит в том, что при выполнении пользователем некоторых не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности - выход в привилегированный режим).

«Люки» чаще всего являются результатом забывчивости разработчиков. В частности, отладка программы ведется за счет прямого доступа к отдельным частям продукта или наборе определенного сочетания клавиш.

Одним из наиболее показательных примеров использования «забытых» люков является, пожалуй, широко известный в компьютерном мире вирус Морриса. Одной из причин, обусловивших возможность распространения этого вируса, была ошибка разработчика программы электронной почты. По оценкам американских специалистов, ущерб нанесенный в результате этого инцидента, составил более чем 100 миллионов долларов.

Вообще люк (или люки) могут присутствовать в программе в виду того, что программист:

- забыл удалить его;
- умышленно оставил его в программе для обеспечения тестирования или выполнения оставшейся части отладки;
- умышленно оставил его в программе в интересах облегчения окончательной сборки конечного программного продукта;
- умышленно оставил его в программе с тем, чтобы иметь скрытое средство доступа к программе уже после того, как она вошла в состав конечного продукта.

В первом случае «люк» - неумышленная, но серьезная брешь в безопасности системы. Во втором и третьем случаях «люк» - серьезная экспозиция безопасности системы. Наконец, в последнем случае «люк» - первый шаг к атаке системы.

В любом случае «люк» - это возможность получить управление системой в обход защиты.

Отметим, что программная ошибка «люком» не является. «Люк» - это достаточно широко используемый механизм отладки, корректировки и поддержки программ, который создается преднамеренно, хотя чаще всего и без злого умысла. Люк становится опасным, если он не замечен, оставлен и не предпринималось никаких мер по контролю за ним.

«Логической бомбой» называют участок программы, который реализует некоторые действия при наступлении определенных условий в дате или имени файла.

Мировая компьютерная общественность достаточно хорошо знакома с «логическими бомбами». Логическая бомба является одним из излюбленных способов мести программистов Компаниям, которые их уволили или чем-либо обидели. При этом чаще всего срабатывание бомбы становится в зависимость от установки в системе даты - так называемые «часовые» бомбы. Это очень удобно: допустим, программист знает, что его уволят 1 февраля. В таком случае он может установить «часовую» бомбу на взрыв, допустим 6 мая, когда сам он будет уже вне пределов досягаемости для

пострадавшей компании.

После ее запуска на экране дисплея можно увидеть мультипликационные картинки с американской певицей Мадонной, причем показ завершается выдачей сообщения следующего содержания «Только идиот использует свой компьютер для того, чтобы рассматривать видеозвезд!». Во время демонстрации бомба удаляет себя, но заодно удаляет и все файлы на доступных для нее дисках.

Эксперты считают, что на сегодняшний день число существующих вирусов перевалило за 50 тысяч, причем ежедневно появляется от 6 до 9 новых. Реально циркулирующих вирусов в настоящее время насчитывается около более 200.

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Более подробная классификация внутри этих групп представлена на рис. 4.

Среда обитания	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

**Рис.
4.
Основные
классы
вирусов.**

Способы заражения

Резидентные	Находятся в памяти, активны до выключения компьютера
Нерезидентные	Не заражают память, являются активными ограниченное время
Безвредные	Практически не влияют на работу; уменьшают свободную память на диске в результате своего размножения
Неопасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты
Опасные	Могут привести к потере программ или системных данных
Очень опасные	Уменьшают свободную память, создают звуковые, графические и прочие эффекты

Особенности алгоритма вируса

Вирусы-«спутники»	Вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением .com
Вирусы-«черви»	Распространяются по сети, рассылают свои копии, вычисляя сетевые адреса
«паразитические»	Изменяют содержимое дисковых секторов или файлов
«стелс»-вирусы («невидимки»)	Перехватывают обращения операционной системы к пораженным файлам или секторам и подставляют вместо себя незараженные участки
Вирусы-призраки	Не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
Макровирусы	Пишутся не в машинных кодах, а на WordBasic, живут в документах Word, переписывают себя в Normal.dot

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. При заражении компьютера вирусом важно его обнаружить по характерным признакам.

Признаками воздействия вирусов на компьютерную систему служат следующие:

- изменение даты создания и длины файла;
- пропажа файла;
- слишком частые обращения к диску;

- непонятные ошибки;
- «зависание» компьютера;
- самопроизвольная перезагрузка операционной системы;
- замедление работы процессора;
- появление неожиданных графических и звуковых эффектов;
- сообщения антивирусных программ.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Большинство вирусов не выполняет каких-либо действий, кроме своего распространения (заражения других программ, дисков и т.д.) и, иногда, выдачи каких-либо сообщений или иных эффектов, придуманных автором вируса: игры, музыки, перезагрузки компьютера, выдачи на экран разных рисунков, блокировки или изменения функций клавиш клавиатуры, замедления работы компьютера и т.д. Однако сознательной порчи информации эти вирусы не осуществляют. Такие вирусы условно называются **неопасными**. Впрочем, и эти вирусы способны причинить большие неприятности (например, перезагрузки каждые несколько минут вообще не дадут вам работать).

Однако около трети всех видов вирусов портят данные на дисках - или сознательно, или из-за содержащихся в вирусах ошибок, скажем, из-за не вполне корректного выполнения некоторых действий. Если порча данных происходит лишь эпизодически и не приводит к тяжелым последствиям, то вирусы называются **опасными**. Если же порча данных происходит часто или вирусы причиняют значительные разрушения (форматирование жесткого диска, систематическое изменение данных на диске и т.д.), то вирусы называются **очень опасными**.

История компьютерной вирусологии представляется сегодня постоянной «гонкой за лидером», причем, не смотря на всю мощь современных антивирусных программ, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиально новые идеи. Все остальные - «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, догонять вирусную технологию.

Первые исследования саморазмножающихся искусственных конструкций проводились в середине прошлого столетия. Термин «компьютерный вирус» появился позднее - официально его автором считается сотрудник Лехайского университета США Ф.Коэн, который ввел его в 1984 году на 7-й конференции по безопасности информации.

В 1989 г. американский студент сумел создать вирус, который вывел из строя около 6 000 компьютеров Министерства обороны США. Или эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счет несовершенства традиционных антивирусных средств.

Кристоферу Пайну удалось создать вирусы Pathogen и Queen, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса и из-за этого после

каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры, зараженные программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними боролась. Запустив ее, пользователи вместо уничтожения вирусов получали еще один. В результате действий этого вируса были уничтожены файлы множества фирм, убытки составили миллионы фунтов стерлингов.

Широкую известность получил американский программист Моррис. Он известен как создатель вируса, который в ноябре 1988 года заразил порядка 7 тысяч персональных компьютеров, подключенных к Internet.

Убытки от разрушительных последствий вирусных эпидемий, с завидной постоянностью вспыхивающих на просторах Всемирной сети, несут многие крупные интернет-компании, для которых даже несколько часов простоя оборачиваются многомиллионными потерями.

Ведь в результате воздействия некоторых, самых агрессивных из них, может быть не только полностью или частично потеряна информация на жестких или сетевых дисках, но даже могут выйти из строя отдельные микросхемы! Впрочем, существуют и такие, на первый взгляд, вполне безобидные вирусы, которые ничем другим не занимаются, кроме как своим размножением. Однако спустя какое-то время, когда все свободное дисковое пространство будет ими «засорено», производительность системы резко уменьшится.

В последнее время многие из вирусописателей «перепрофилировались». Если раньше подавляющее большинство вирусов создавались исключительно с хулиганскими целями, то сегодня производство вирусов уже превратилось в целую индустрию, приносящую, кстати, ее хозяевам немалый доход. Поэтому «отсталые» вирусы, только и умеющие, что наносить вред операционной системе или приложениям, нынче активно замещают «тройанские кони» - программы, предназначенные для хищения конфиденциальной информации, в первую очередь финансового характера.

При этом пользователь зачастую даже и не подозревает, что стал жертвой. В одно мгновение все пароли и данные кредитных карточек, введенные при совершении покупок через Интернет, могут стать добычей третьих лиц.

Вирусописатели демонстрируют готовность не только к изобретению новых технологий, но и к дальнейшему освоению старых.

Мобильные вирусы

Как и предсказывалось, все большие обороты набирает развитие червей и троянцев для мобильных телефонов. В настоящий момент количество вредоносных программ увеличивается примерно на 1 новую программу в неделю.

Примечателен тот факт, что в антивирусные базы были добавлены представители нового класса червей для мобильных телефонов под управлением операционной системы Symbian. Речь идет о «почтовых мобильных червях», использующих для самораспространения MMS (сервис передачи мультимедийных сообщений). В обнаруженные экземпляры встроено два способа распространения. Первый, уже ставший традиционным для мобильных червей, через протокол Bluetooth; червь распространяется, рассылая себя на все доступные устройства в радиусе 10-15 метров. Второй - при помощи MMS - сообщений.

В настоящий момент известно два семейства MMS-червей:

- Comwar, который рассылает себя по всей адресной книге мобильного телефона;
- Cabir.k, который ведет себя более оригинально, а именно - ждет прихода на телефон SMS-или MMS-сообщения и отправляет себя в ответ на него.

Начавшись с одного единственного Bluetooth-червя, вредоносные программы для мобильных устройств сейчас представлены сразу 3-мя классами: Worm (причем, здесь теперь есть как «сетевые» черви, так и «почтовые»), Virus, Trojan.

Если традиционным вирусам потребовались годы, чтобы прийти к такому количеству поведений, то мобильные вирусы проделали этот путь менее чем за год.

Можно с уверенностью прогнозировать, что в ближайший год появятся мобильные представители других классов компьютерных вирусов.

Справочник угроз при работе в интернет

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих

программ было самораспространение; некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы - типичные проявления кибервандализма.

В чем разница между вирусом и червем?

Вирус - это саморазмножающаяся программа, она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Вирус заражает тем большее количество файлов, чем дольше он находится на компьютере необнаруженным. Червь создает единственную копию своего кода. В отличие от вируса, код червя самостоятелен. Другими словами, червь - это отдельный файл, в то время как вирус - это код, который внедряется в существующие файлы.

Что такое рекламные системы (adware)?

Понятие «adware» включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.

Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер.

Заплатить за свое

Включив компьютер, наш читатель Александр Б. вместо привычной заставки увидел надпись, требующую для нормальной загрузки послать **СМС-сообщение стоимостью 300 руб.**

Он позвонил знакомым программистам с просьбой о помощи. Приехавший компьютерщик переустановил на компьютере программу. Но теперь в машине **вся имеющаяся информация превратилась в страшную абракадабру**. А вирус, который был причиной катастрофы, опять требовал СМС за 300 руб. Время и силы, требуемые для расшифровки необходимых для работы данных, не шли ни в какое сравнение с ценой, названной виртуальными вымогателями. Однако вместо одного сообщения Александру пришлось отправить почти десяток СМС. **Общая сумма снятых с мобильного счета средств составила 2 620 руб.** И только после этого компьютер «заговорил» нормальным языком. При этом тот самый программист выразил сомнение, что проблема не повторится вновь через какое-то время. И рассказал, что ходят слухи о том, что вскоре подобные ситуации начнут происходить не только с компьютерами. Но и со смартфонами и коммуникаторами. Причем в этом случае вирус будет автоматически рассылать сам себя по записной книжке трубки, что приведет к глобальной эпидемии в мире сотовой связи. Чтобы этого не случилось, всем пользователям мобильных телефонов стоит заранее установить на свои трубки **специальные антивирусные программы**.

2.3. Компьютерные преступления и наказания

Для понимания масштабов объёма информатизации общества приведём такие цифры: в настоящий момент в мире насчитывается около 3,5 млрд людей, имеющих доступ к Интернету. Это половина всего населения Земли.

Сетью Интернет в совокупности со своими внутренними информационными сетями пользуются все банки и корпорации, аккумулирующие на своих счетах крупные денежные средства, лакомый кусок для разного рода компьютерных мошенников. Число преступных посягательств на имущество, совершаемых путём злоупотребления доверием или обманом, продолжает расти. В качестве статистических данных приведём отчёт Центра статистической информации Главного информационно-аналитического центра МВД России: в Российской Федерации за 2015 год было зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159 - 159.6 УК РФ (по сравнению с прошедшим годом, это больше на 25 процентов, в 2014 году было зарегистрировано 160214 подобных преступлений). При этом небывалыми темпами растёт число мошенничеств в сфере компьютерной информации (995 зарегистрированных преступлений в 2014 году против 5443 в 2015 году). Раскрываемость же подобных деяний оставляет желать лучшего: в 2015 году она находилась на уровне 7,4 %. По итогам четырёх месяцев 2016 года негативная тенденция остаётся: зарегистрировано 1789 мошенничеств в сфере компьютерной информации (на 143,7% больше). В числе лидеров по количеству данных преступлений: Тюменская область (333 зарегистрированных преступления), Удмуртия (298), Республика Коми (223). Раскрыто всего 72 преступления (на 5,3% меньше по сравнению с аналогичным периодом 2015 года). Низкая раскрываемость данного вида преступлений обусловлена достаточно высоким уровнем подготовки злоумышленников. Обычно они имеют как профессиональное образование, так и необходимую техническую аппаратуру, существенно облегчающую сокрытие следов при совершении компьютерных мошенничеств.

В последнее время все больше внимания в прессе уделяется так называемым «компьютерным преступлениям». Такое внимание не беспочвенно. Дело в том, что сегодня практически ничего не делается без участия компьютеров в сфере коммуникаций, торговли, банковских и биржевых операций и многого другого. Все важнейшие информационные функции современного общества, так или иначе «завязаны» на компьютерах, компьютерных сетях и компьютерной информации.

С появлением современных средств вычислительной техники и телекоммуникаций традиционные преступления - воровство, мошенничество, шпионаж, вымогательство трансформировались в новые формы. Кроме того, появились специфические для компьютерных систем и сетей преступления. Намечается тенденция к использованию информационных технологий организованными преступными группами и распространение их деятельности на межгосударственный уровень. Сотрудники правоохранительных органов при раскрытии и расследовании компьютерных преступлений неизбежно сталкиваются с большими трудностями, так как преступления в сфере компьютерной обработки информации характеризуются высокой скрытностью, трудностями сбора улик по установлению фактов их совершения, сложностью доказывания в суде. Субъекты преступлений - это, как правило, высококвалифицированные программисты, инженеры, специалисты в области телекоммуникационных систем, банковские работники, бывшие сотрудники спецслужб (101).

Понятие *"компьютерная преступность"* охватывает преступления, совершаемые с помощью компьютеров, информационно вычислительных систем и средств телекоммуникаций, или направленные против них с корыстными либо некоторыми другими целями.

Компьютерное преступление как уголовно-правовое понятие - это предусмотренное уголовным законом умышленное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Понятие информационных преступлений

Отечественные и зарубежные издания и средства массовой информации последних лет наводнены различными понятиями, обозначающими те или иные новые проявления криминального характера в информационной области. Встречаются наименования и «компьютерные преступления», «коммуникационные преступления», и «кибербандитизм». Преступников именуют «хакеры», «кракеры», «киберпанки», «бандиты на информационных супермагистральных». Различие в терминологии указывает не только на обеспокоенность общества новой угрозой, но и на отсутствие

полного понимания сути этой угрозы.

* Селиванов Н.А. Советская криминалистика: система понятий. М., 1982. С. 3.

Для компьютерных преступлений характерны следующие особенности ():

- высокая латентность компьютерных преступлений, раскрывается лишь 1-3% из их числа;
- сложность сбора доказательств и процесса доказывания в суде;
- отсутствие четкой программы борьбы с компьютерными преступлениями (одна из причин того, что примерно 90% преступлений данной категории выявляется благодаря случайностям;
- сложность самого процесса раскрытия (в узком смысле слова) компьютерных преступлений;
- отсутствие достаточной следственной практики по расследованию компьютерных преступлений в Российской Федерации.

В.В.Крылов приводит описание возможных способов нарушения конфиденциальности и целостности компьютерной информации без их классификации (116):

- хищение машинных носителей информации в виде блоков и элементов ЭВМ (например, флоппи-дисков);
- копирование машинных носителей информации;
- копирование документов с исходными данными;
- копирование с устройств отображения информации (устройств вывода) выходных документов;
- использование визуальных оптических и акустических средств наблюдения за ЭВМ;
- считывание и расшифровка различных электромагнитных излучений и «паразитных наводок» в ЭВМ и обеспечивающих системах;
- запоминание информации;
- фотографирование информации в процессе ее обработки;
- изготовление дубликатов входных и выходных документов;
- копирование распечаток;
- использование программных «ловушек»;
- маскировка под зарегистрированного пользователя;
- использование недостатков программного обеспечения и операционных систем;
- использование поражения программного обеспечения вирусами;
- подмена и хищение машинных носителей информации и документов;
- подмена элементов программ и баз данных;
- включение в программы блоков типа «троянский конь», «логическая бомба» и т.п.;
- чтение информации из ОЗУ;
- несанкционированное подключение к основной и вспомогательной аппаратуре ЭВМ, внешним запоминающим устройствам, периферийным устройствам, линиям связи и др.

В более общем виде способы совершения КП можно классифицировать на (101):

- несанкционированный доступ;
- вирусная модификация;
- перехват информации;
- комбинированное использование.

Несанкционированный доступ включает:

- несанкционированное подключение;
- несанкционированную модификацию;
- несанкционированное блокирование;
- несанкционированное уничтожение.

К несанкционированному подключению относятся - несанкционированный доступ к вычислительным ресурсам, воздействие на парольно-ключевые системы, установка программных и закладных устройств.

При совершении криминальных действий, связанных с несанкционированным копированием информации, преступники, как правило, копируют:

- документы, содержащие интересующую их информацию;
- технические носители;

- информацию, обрабатываемую в информационных системах.

Под модификацией информации понимается внесение в нее любых изменений, обуславливающих ее отличие от той, которую собственник информационного ресурса включил в систему и которой владеет.

Несанкционированное блокирование информации заключается в невозможности доступа к ней со стороны законного пользователя.

Уничтожение информации включает и полную или частичную ликвидацию, как самой информации, так и ее носителей.

Под *перехватом* понимают получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации () (рис.6).

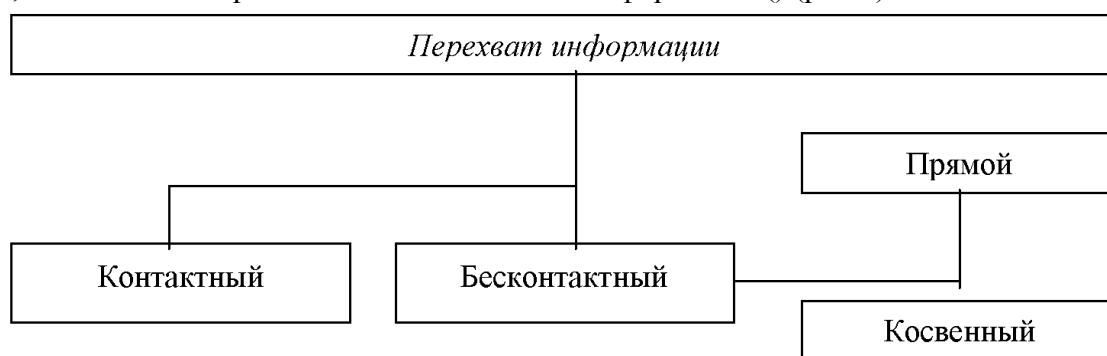


Рис. 6

Пример 1.

Дистанционный перехват компьютерной информации с монитора был впервые продемонстрирован на Каннском международном конгрессе по вопросам компьютерной безопасности в марте 1985 г. Перехват производился из автомобиля, находящегося на улице, в отношении монитора, установленного на восьмом этаже здания, расположенного в 100 м от автомобиля сотрудником голландской телекоммуникационной компании РТТ ().

Для анализа собранной информации в стационарных условиях возможно использование преступниками видеомэгнитофонов. Перехвату подвержены передачи данных и переговоры с радиомодемов и радиотелефонов.

С криминалистической точки зрения под *злонамеренной вирусной модификацией* мы понимаем разработку, использование либо распространение таких программ, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесению несанкционированных собственником изменений в компьютерную информацию.

Факты появления и развития в России компьютерных преступлений, ранее неизвестные отечественной юридической науке и практике, вызывают особую тревогу.

Первое преступление подобного рода в бывшем СССР было зарегистрировано в 1979 г. в г. Вильнюсе. Оно было совершено способом манипуляции ценными данными при совершении хищения денежных средств. А второе подобное преступление было совершено уже в 1982 г. в г. Горьком (нынешний Н.Новгород). Совершению подобных преступлений с использованием одинаковых методик, по мнению специалистов, способствовало то обстоятельство, что в этот период времени все отделения связи бывшего СССР переводились на новую централизованную автоматическую систему обработки (получение и отправки денежных переводов клиентов, функционирующую на базе компьютерного комплекса «Онега»).

Еще одно из нашумевших первых компьютерных преступлений относит нас к 1981 г. Экономистом Брестского областного производственного объединения К. были совершены хищения денежных средств. Как свидетельствуют материалы уголовного дела, будучи экономистом по учету заработной платы и отвечая за достоверность документов и сдачу их в ОАСУ, К. на протяжении ряда лет (начиная с 1981 г.) вносила в компьютерные бухгалтерские документы на начисление заработной платы подложные данные. В результате чего заработная плата начислялась на счета вымышленных лиц и переводилась в сберкассы г. Бреста на специально открытые ею счета родственников.

Средства компьютерной техники, в частности компьютерная система, иногда используются

преступником и как инструмент посягательства на другие объекты, например как воздействие на администрацию с целью повышения по службе. Так, в августе 1983г. на волжском автомобильном заводе в г. Тольятти следственной бригадой Прокуратуры РСФСР был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу электронно-вычислительной машины, обеспечивающей заданное технологическое функционирование автоматической системы подачи механических узлов на главный сборочный конвейер завода. В результате произошел сбой в работе данного конвейера и заводу был причинен существенный материальный ущерб: 200 легковых автомобилей марки «ВАЗ» не сошло с конвейера, пока программисты не выявили и не устранили источник сбоев. Программист был привлечен к уголовной ответственности: приговор суда - три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика главного конвейера.

1985 год. На Л-ом судостроительном заводе была разоблачена преступная группа численностью свыше 70 человек, в которую входили работники расчетного бюро центральной бухгалтерии завода, должностные и материально-ответственные лица почти всех структурных подразделений предприятия во главе с начальником бюро расчетов Б., ранее судимой за хищение. Расследование показало, что преступники путем внесения данных в машиннограммы незаконно завышали фактический размер средств к выплате, числящихся на субсчете балансового счета 70 («Расчеты по оплате труда»), на котором учитывались все внеплановые выплаты, выдаваемые рабочим и служащим завода в установленном порядке (внеплановые авансы, пособия по временной нетрудоспособности, премии и т.д.). Излишки начисленных средств относились на затраты производства. Параллельно осуществлялся ввод в ЭВМ фиктивных (свободных на данный момент) табельных номеров с указанием вымышленных фамилий их владельцев. В результате из вычислительного центра, обслуживающего бухгалтерию, в подразделения завода поступали распечатки о начислениях заработной платы, служившие основанием для выплаты денег через кассу. Начисленные на подставных лиц деньги изымались по подложным доверенностям либо по сговору с кассиром-раздатчиком.

До 1988 г. были разоблачены преступные группы, действовавшие аналогичными способами и совершившие хищения в крупных и особо крупных размерах на заводах Петровского и «Красное Сормово» г. Горький (Н.Новгород), одного из предприятий г.Ленинграда (Санкт-Петербург) и ряда других городов.

Наибольшую опасность представляет компьютерная преступность в финансовой сфере, так как, во-первых, остро встала проблема безопасности, а банковская информация представляет собой реальные деньги, во-вторых, затрагивает конфиденциальные интересы большого количества клиентов банка.

Так, например, начиная с 1991 года, российские банки неоднократно подвергались нападению со стороны "электронных грабителей". В 1991 году сотрудниками подразделений по борьбе с экономическими преступлениями в системе Внешэкономбанка была разоблачена преступная группа, которая путем манипуляций с валютными счетами физических лиц присвоила 125 тыс. долларов США.

Ущерб от преступлений с банковскими авизо оценивали в 1993 году более чем в 2 млрд. долларов. В Московском РКЦ Центробанка было предотвращено электронное хищение на сумму свыше 300 млн. долларов, во Внешэкономбанке около 1 млн. долларов США. В 1995 году в Мытищинском банке г. Москвы было похищено с помощью ЭВМ более 150 тыс. долларов.

О масштабах этого явления говорит и тот факт, что только за 1993-1994 гг. было совершено более 300 попыток проникновения в компьютерные сети ЦБ России. В целом в 1995 году по России выявлено 185 хищений с использованием электронных средств доступа, ущерб по которым составил 250 млрд. рублей. За их совершение к уголовной ответственности привлечено более 60 человек. Эти преступления имели место в гг. Москве, С.-Петербурге, Волгоградской, Калининской, Мурманской, Ростовской областях и ряде других регионов.

Особое беспокойство вызывает усиление организованности и интернационализации этого вида преступлений. Например, согласованными действиями сотрудников МВД России, полиции Великобритании, Германии, Израиля, Нидерландов была пресечена деятельность международной преступной группы, специализирующейся на хищениях валютных средств путем незаконного проникновения в компьютерные сети иностранных банков. Активным участником и организатором этой преступной группы был В.Левин, по официальной версии укравший вместе с сообщниками 3,5

млн. долл. со счетов клиентов "Сити-банка" - крупнейшего банка США,

По данному уголовному делу Левин проходит как технический исполнитель преступной международной группировки "кибергангстеров", которые взламывали электронную защиту американского "Сити-банка", изымали крупные суммы со счетов клиентов из Аргентины, Колумбии, Мексики, Новой Зеландии, Индонезии, Уругвая, Гонконга, Канады, США и переводили их методом электронного трансферта на счета, заблаговременно открытые в банках Западной Европы, Америки, России и Израиля. Все операции со счетами "Сити-банка" производились из офиса АО "Сатурн". Эта фирма, торгующая компьютерами, принадлежала другу Левина и его сообщнику по ограблению американского банка.

1 марта 1995 года Левин был арестован английскими властями в аэропорту под Лондоном по пути следования на компьютерную выставку В Голландию. По одной из существующих версий, преступник проник в "компьютерные сейфы" "Сити-банка" по коммуникационным сетям Интернет.

К наиболее типичным способам совершения компьютерных преступлений специалисты относят следующие:

- подделка отчетов и платежных ведомостей;
- приписка сверхурочных часов работы;
- фальсификация платежных документов;
- хищение из денежных фондов;
- добывание запасных частей и редких материалов;
- кража машинного времени;
- вторичное получение уже произведенных выплат;
- фиктивное продвижение по службе;
- получение фальшивых документов;
- внесение изменений в программы и машинную информацию;
- перечисление денег на фиктивные счета;
- совершение покупок с фиктивной оплатой и др.

В своих преступных деяниях компьютерные преступники руководствуются следующими основными мотивами (101):

- а) выйти из финансовых затруднений;
- б) получить, пока не поздно, от общества то, что оно якобы задолжало преступнику;
- в) отомстить фирме и работодателю;
- г) выразить себя, проявить свое "я";
- д) доказать свое превосходство над компьютерами.

Отличительными особенностями данных преступлений являются высокая латентность, сложность сбора доказательств, транснациональный характер (как правило, с использованием телекоммуникационных систем), значительность материального ущерба, а также специфичность самих преступников. Как правило, ими являются высококвалифицированные программисты, банковские служащие.

Высокая латентность компьютерных преступлений обусловлена тем, что многие организации разрешают конфликт своими силами, поскольку убытки от расследования могут оказаться выше суммы причиненного ущерба (изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что неприемлемо ни для одной организации). Их руководители опасаются подрыва своего авторитета в деловых кругах и в результате - потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности.

Непосредственным предметом преступного посягательства по делам о КП являются следующие:

- компьютерная система (ЭВМ, сервер, рабочая станция);
- процесс обработки и хранения информации;
- компьютерные сети (сети ЭВМ).

Нарушение целостности информации без непосредственного участия человека включает:

- выход из строя серверов, рабочих станций;
- сбои в сети электропитания;
- выход из строя магнитных носителей информации;
- неполадки в кабельной системе, сетевом оборудовании;

- прочие аппаратные и программные сбои.

Российские исследователи отмечают следующие особенности совершения компьютерных преступлений в финансовой сфере:

- большинство злоумышленников - клерки, хотя высший персонал банка также может совершить преступление и нанести банку гораздо больший ущерб, однако такого рода случаи происходят намного реже;
- как правило, злоумышленники используют свои собственные счета, на которые переводятся похищенные суммы;
- большинство преступников не знает, как "отмыть" украденные деньги; умение совершить преступление и умение получить деньги - это не одно и то же;
- компьютерные преступления не всегда высоко технологичны, ряд злоумышленных действий достаточно просто может быть совершен обслуживающим персоналом;
- многие злоумышленники объясняют свои действия тем, что они всего лишь берут в долг у банка с последующим возвратом; как правило, этого не происходит.

Классификация компьютерных преступлений

В зависимости от способа воздействия на компьютерную систему специалисты выделяют четыре вида компьютерных преступлений:

- *Физические злоупотребления*, которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
- *Операционные злоупотребления*, представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.
- *Программные злоупотребления*, которые включают в себя: различные способы изменения системы математического обеспечения ("логическая бомба" - введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; "тройанский конь" - включение в обычную программу своего задания).
- *Электронные злоупотребления*, которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Все способы совершения компьютерных преступлений можно объединить в три основные группы: методы перехвата, методы несанкционированного доступа и методы манипуляции.

- *Методы перехвата.*

Непосредственный перехват - осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

- *Методы несанкционированного доступа.*

Классификация этих методов предложена Ю.М.Батуриным (15). Поэтому считаем возможным далее по тексту настоящей работы использовать его лексический перевод оригиналов названий способов с английского языка, которые наиболее часто применяются в международной юридической практике.

"Компьютерный абордаж". Данный способ совершения компьютерного преступления осуществляется преступником путем случайного подбора (или заранее добытого) абонентского номера компьютерной системы потерпевшей стороны. Преступником производится подбор кода доступа к компьютерной системе жертвы (если таковой вообще имеется) или используется заранее добытый код. Иногда для этих целей преступником используется специально созданная самодельная либо заводская (в основном, зарубежного производства) программа автоматического поиска пароля, добываемая преступником различными путями.

Стоит обратить внимание на то, что существует множество программ- "взломщиков",

называемых на профессиональном языке HACK-TOOLS (инструмент взлома). Эти программы работают по принципу простого перебора символов. Но они становятся малоэффективными в компьютерных системах, обладающих программой- "сторожем" компьютерных портов, ведущей автоматический протокол обращений к компьютеру и отключающей абонента, если пароль не верен. Поэтому в последнее время преступниками стал активно использоваться метод "интеллектуального перебора", основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. Интересны результаты экспериментов, представленные специалистами в форме таблицы (табл. 1)

Таблица 1

Тематические группы паролей	% частоты выбора пароля человеком	% раскрываемости пароля
Имена, фамилии и производные	22,2	54,5
Интересы (хобби, спорт, музыка)	9,5	29,2
Даты рождения, знаки зодиака свои и близких; их комбинация с первой группой	11,8	54,5
Адрес жительства, место рождения	4,7	55,0
Номера телефонов	3,5	66,6
Последовательность клавиш ПК, повтор символа	16,1	72,3
Номера документов (паспорт, пропуск, удостоверение и т.д.)	3,5	100,0
Прочие	30,7	5,7

"Неспешный выбор". Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может, не спеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства. Обычно такой способ используется преступником в отношении тех, кто не уделяет должного внимания регламенту проверки своей системы, предусмотренной методикой защиты компьютерной системы.

"Бреши". В отличие от "неспешного выбора", при данном способе преступником осуществляется конкретизация уязвимых мест в защите: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом "бреши" могут использоваться преступником многократно, пока не будут обнаружены. Появление этого способа обусловлено тем, что программисты иногда допускают ошибки при разработке программных средств, которые не всегда удается обнаружить в процессе отладки программного продукта. Например, методика качественного программирования предполагает: когда программа X требует использования программы V - должна выдаваться только информация, необходимая для вызова V, а не она сама. Для этих целей применяются программы группировки данных. Составление последних является довольно скучным и утомительным, поэтому программисты иногда сознательно нарушают методику программирования и делают различные упрощения, указывая, например, индекс места нахождения нужных данных в рамках более общего списка команд программы. Именно это и создаст возможности для последующего нахождения подобных "брешей".

"Люк". Данный способ является логическим продолжением предыдущего. В этом случае в найденной "бреши" программа разрывается и туда дополнительно преступник вводит одну или несколько команд. Такой "люк" открывается по мере необходимости, а включенные команды автоматически выполняются.

Следует обратить внимание на то, что при этом всегда преступником осуществляется

преднамеренная модификация (изменение) определенной компьютерной информации.

"Маскарад". Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Система защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации пользователя (например, по биометрическим параметрам: отпечаткам пальцев, рисунку сетчатки глаза, голосу и т.п.) оказываются не защищенными от этого способа. Самый простейший путь к проникновению в такие системы - получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путем подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу; обнаружения такого документа в организациях, где не налажен должный контроль за их хранением; отбора информации из канала связи и т.д. Так, например, задержанный в декабре 1995 года сотрудниками московского РУОПа преступник похищал наличные денежные средства из банкоматов банка "Столичный" с использованием обычной электронной кредитной карточки путем подбора цифровой комбинации кода доступа в компьютерную систему управления счетами клиентов банка. Общая сумма хищения составила 400 млн. руб.

"Аварийный". В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы данной программы заключается в том, что она позволяет достаточно быстро обойти все имеющиеся средства защиты информации и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным. Такие программы являются универсальным "ключом" в руках преступника.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств.

Методики несанкционированного доступа сводится к двум разновидностям:

"Взлом" изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

"Взлом" извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем "взлома" защитных систем организаций.

Хищение информации. Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторским правом;
- глобальная информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государств.

Похищаются сведения о новейших научно-технических разработках, планах компании по маркетингу своей продукции и заключаемых сделках.

Типичным злоупотреблением, посягающим на объекты авторских прав, являются преступления, связанные с несанкционированным размножением компьютерных программ.

Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации

причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы.

Повреждение системы. Данная группа объединяет преступления, совершаемые с целью разрушить или изменить данные, являющиеся важными для владельца или многих пользователей системы - объекта несанкционированного доступа.

Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающим лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания.

Особую опасность представляют злоупотребления, связанные с распространением вирусов через Интернет.

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

"Троянский конь"- способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе, либо оказать воздействие на администрацию предприятия с корыстной целью.

"Логическая бомба" - тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

"Временная бомба" - разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

"Асинхронная атака" - состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.

"Моделирование" используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления.

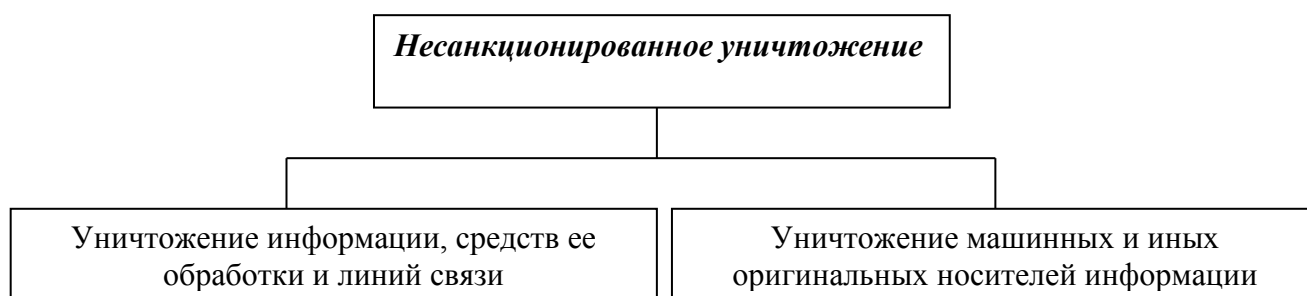


Рис. 2.3.6.



Рис. 2.5.1.

Субъекты компьютерных преступлений

Лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

- лица, не связанные трудовыми отношениями с организацией жертвой, но имеющие некоторые связи с ней;
- сотрудники организации, занимающие ответственные посты;
- сотрудники-пользователи ЭВМ, злоупотребляющие своим положением.

Западные специалисты подразделяют представляющий опасность персонал на категории в соответствии со сферами деятельности.

Операционные преступления - совершаются операторами ЭВМ, периферийных устройств ввода информации в ЭВМ и обслуживающими линии телекоммуникации.

Преступления, основанные на использовании программного обеспечения, обычно совершаются лицами, в чьем ведении находятся библиотеки программ; системными программистами; прикладными программистами; хорошо подготовленными пользователями.

Для аппаратурной части компьютерных систем опасность совершения преступлений представляют: инженеры-системщики, инженеры по терминальным устройствам, инженеры-электронщики.

Определенную угрозу совершения компьютерных преступлений представляют и *сотрудники, занимающиеся организационной работой*: управлением базами данных, руководством работой по программному обеспечению.

Определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование ЭВМ.

Особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры и связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Например, *около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков*. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих - системные администраторы и другие сотрудники служб автоматизации банков.

По сведениям Национального центра данных о преступности, связанной с ЭВМ (Лос-Анджелес, США), компьютерные правонарушения наиболее часто совершаются программистами, студентами и операторами ввода исходных данных. В табл. 3 указаны основные типы и субъекты угроз для компьютерных систем.

Таблица 3

Типы и субъекты угроз

Тип угроз	Оператор	Руководитель	Программист	Инженер (техник)	Пользователь	Конкурент
Изменение кодов	+		+			
Копирование файлов	+		+			
Уничтожение файлов	+	+	+		+	+
Присвоение программ			+	+		+
Шпионаж	+	+	+			+
Установка			+	+		+
Саботаж	+		+	+		+
Продажа данных	+	+	+		+	
Воровство		+	+		+	+

Субъектов компьютерных преступлений с точки зрения профессиональной подготовленности принято подразделять на лиц, совершающих преступления: а) "нетехнические";

б) "технические", требующие минимума специальных знаний;

в) "высокотехнические", возможные при условии основательного владения вычислительной техникой.

Практика показывает, что большинство преступлений категории "а" совершают малознакомые с вычислительной техникой служащие со средним образованием. Однако этих людей отличают два качества: они имеют доступ к компьютеру и знают, какие функции выполняет он в их организации. "Нетехнические" преступления совершаются главным образом путем кражи пароля доступа к файлам информации, хранящейся в машинной памяти. Владея паролем и определенными навыками, можно войти в засекреченные файлы, изменить их содержание и т.п. Эти преступления довольно просты для расследования, и, усилив защиту системы, их легко предупредить.

"Технические" преступления связаны с манипуляциями программами, которые составлены специалистами. Изменить их могут лишь лица, имеющие соответствующую квалификацию. Наибольшую трудность для правоохранительных органов представляют "высокотехнические" преступления.

Анализируя компьютерные преступления, можно установить общность "почерка" злоумышленника (или организованной группы):

- реализуется несанкционированный доступ к автоматизированной информационной системе, к ее аппаратно-программным средствам, модифицируются важные записи;
- вносятся изменения в существующее программное обеспечение для создания специальных счетов физических и юридических лиц, рассылки фальшивых платежных документов и пр.
- параллельно уничтожаются следы компьютерного преступления путем модернизации бухгалтерских документов аналитического и синтетического учета;
- осуществляется получение наличных средств.

Опасность, как правило, таится внутри организации, а не вне ее. Компьютерному преступлению способствуют такие предпосылки, как отсутствие надлежащей системы бухгалтерского учета, комплексной защиты информации и ее контроля, слабая готовность персонала, отсутствие или слабая организация системы разделения доступа и т.п.

Причинами, побуждающими недобросовестных сотрудников к совершению компьютерных преступлений, являются:

- корысть;
- ошибка пользователей и программистов неумышленного характера;
- безответственность в организации системы информационной безопасности;
- самоутверждение путем демонстрации своего превосходства;
- месть за какие-либо действия администрации;
- недостатки созданных информационных систем и технологий.

Полагается, что преступления в сфере компьютерной информации являются

"беловоротничковыми преступлениями" ("БП" - это такие правонарушения, при совершении которых имеет место нанесение ущерба торговле, нарушение страховых и валютных правил, взяточничество и т.п.). В отличие от многих других "беловоротничковых преступлений", которые в большинстве случаев совершаются, несмотря на существующую систему учета и контроля, компьютерные преступления обычно являются следствием отсутствия надлежащего контроля. Ранее компьютер считали защищенным от всякого рода "злоумышленников", и поэтому различные предосторожности рассматривались излишними.

Общей причиной существования преступности является несовершенство человека, его предрасположенность, как к добру, так и злу.

По мнению специалистов, большинство серьезных компьютерных преступлений, связанных с неправомерным доступом к компьютерной информации, совершаются группой лиц. Это подтверждается и статистикой. Так, 38% преступников действовали без соучастников, тогда как 62% - в составе преступных групп.

Прежде всего, это связано с тем, что на современном этапе развития компьютерных технологий одному человеку практически невозможно одновременно нейтрализовать системы защиты, выполнить какие-либо манипуляции с информацией, а затем еще запутать за собой следы преступления.

Уголовный кодекс Российской Федерации, вступивший в действие в 1997 г., установил нормы, объявляющие общественно опасными деяниями конкретные действия **в сфере компьютерной информации** и устанавливающие ответственность за их совершение. Такие нормы появились в

российском законодательстве впервые.

К уголовно наказуемым отнесены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В тех случаях, когда общественно опасные действия в области информационных отношений совершаются без применения компьютерных средств, законодатель нередко относит их к другим, соответствующим родовым объектам.

Так, клевета или оскорбление (ст. 129, 130 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных (подчеркнуто мной. — В. К.) сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140 УК РФ), нарушение авторских, смежных, изобретательских и патентных прав (ст. 146, 147 УК РФ) находятся в разделе “Преступления против личности”. Кража, мошенничество, хищение предметов, имеющих особую ценность, умышленные уничтожение или повреждение имущества, заведомо ложная реклама, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. 158, 159, 164, 167, 182, 187, 189 УК РФ) в разделе “Преступления в сфере экономики” и т.д.

Статья 159. Мошенничество

(в ред. Федерального [закона](#) от 08.12.2003 N 162-ФЗ)

1. Мошенничество, то есть [хищение](#) чужого имущества или приобретение права на чужое имущество путем [обмана](#) или [злоупотребления доверием](#), -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

(в ред. Федерального [закона](#) от 07.12.2011 N 420-ФЗ)

2. Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением [значительного ущерба](#) гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

(в ред. Федерального [закона](#) от 07.12.2011 N 420-ФЗ)

3. Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в [крупном размере](#), -

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

(в ред. Федеральных законов от 27.12.2009 N 377-ФЗ, от 07.03.2011 N 26-ФЗ, от 07.12.2011 N 420-ФЗ, от 29.11.2012 N 207-ФЗ)

4. Мошенничество, совершенное организованной группой либо в [особо крупном размере](#) или повлекшее лишение права гражданина на жилое помещение, -

(в ред. Федерального [закона](#) от 29.11.2012 N 207-ФЗ)

наказывается лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

(в ред. Федеральных законов от 27.12.2009 N 377-ФЗ, от 07.03.2011 N 26-ФЗ)

Статья 159.1. Мошенничество в сфере кредитования
(введена Федеральным [законом](#) от 29.11.2012 N 207-ФЗ)

1. Мошенничество в сфере кредитования, то есть хищение денежных средств заемщиком путем представления банку или иному кредитору заведомо ложных и (или) недостоверных сведений, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные [частями первой](#) или [второй](#) настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные [частями первой](#) или [третьей](#) настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Примечание. Крупным размером в настоящей статье, а также в [статьях 159.3, 159.4, 159.5, 159.6](#) настоящей главы признается стоимость имущества, превышающая один миллион пятьсот тысяч рублей, а особо крупным - шесть миллионов рублей.

Статья 159.2. Мошенничество при получении выплат
(введена Федеральным [законом](#) от 29.11.2012 N 207-ФЗ)

1. Мошенничество при получении выплат, то есть хищение денежных средств или иного имущества при получении пособий, компенсаций, субсидий и иных социальных выплат, установленных законами и иными нормативными правовыми актами, путем представления заведомо ложных и (или) недостоверных сведений, а равно путем умолчания о фактах, влекущих прекращение указанных выплат, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные *частями первой* или *второй* настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в *крупном размере*, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные *частями первой* или *третьей* настоящей статьи, совершенные организованной группой либо в *особо крупном размере*, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 159.3. Мошенничество с использованием платежных карт

(введена Федеральным *законом* от 29.11.2012 N 207-ФЗ)

1. Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением *значительного ущерба* гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные *частями первой* или *второй* настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в *крупном размере*, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные *частями первой, второй* или *третьей* настоящей статьи, совершенные организованной группой либо в *особо крупном размере*, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

КонсультантПлюс: примечание.

Статья 159.4 утратила силу в соответствии *Постановлением* Конституционного Суда РФ от 11.12.2014 N 32-П.

Статья 159.4. Мошенничество в сфере предпринимательской деятельности

(введена Федеральным [законом](#) от 29.11.2012 N 207-ФЗ)

1. Мошенничество, сопряженное с преднамеренным неисполнением договорных обязательств в [сфере](#) предпринимательской деятельности, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до двухсот сорока часов, либо ограничением свободы на срок до одного года, либо принудительными работами на срок до одного года, либо лишением свободы на тот же срок.

2. То же деяние, совершенное в [крупном размере](#), -

наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок с ограничением свободы на срок до одного года или без такового.

3. То же деяние, совершенное в [особо крупном размере](#), -

наказывается штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок с ограничением свободы на срок до двух лет или без такового.

Статья 159.5. Мошенничество в сфере страхования

(введена Федеральным [законом](#) от 29.11.2012 N 207-ФЗ)

1. Мошенничество в сфере страхования, то есть хищение чужого имущества путем обмана относительно наступления страхового случая, а равно размера страхового возмещения, подлежащего выплате в соответствии с законом либо договором страхователю или иному лицу, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением [значительного ущерба](#) гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные [частями первой](#) или [второй](#) настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в [крупном размере](#), -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные [частями первой](#), [второй](#) или [третьей](#) настоящей статьи, совершенные организованной группой либо в [особо крупном размере](#), -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья 159.6. Мошенничество в сфере компьютерной информации
(введена Федеральным [законом](#) от 29.11.2012 N 207-ФЗ)

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные [частями первой](#) или [второй](#) настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в [крупном размере](#), -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные [частями первой](#), [второй](#) или [третьей](#) настоящей статьи, совершенные организованной группой либо в [особо крупном размере](#), -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

[гл. 21, "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ \(ред. от 03.07.2016\)](#)
[{КонсультантПлюс}](#)

2.3. Данные о способе и механизме совершения преступления

Элементами криминалистической характеристики преступления любого вида являются данные о механизме совершения преступления, данные о способе совершения преступления, данные об обстановке совершения преступления, данные о свойствах личности лица, совершившего преступление.

В криминалистике под способом совершения преступления понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющую различного рода характерные следы вовне, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личности данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления.¹

Механизм совершения преступления понимается как система данных, описывающих временной и динамический порядок связи отдельных этапов, обстоятельств, факторов подготовки, совершения и сокрытия следов преступления, позволяющих воссоздать картину процесса его совершения.²

Из приведенных определений следует, что у каждого способа совершения преступления существует свой механизм: Именно обобщенные данные о механизме совершения преступления содержат сведения о наиболее характерных следах преступления. Рассмотрим существующие на сегодняшний день криминалистические знания о компьютерных преступлениях с этих точек зрения.

Уголовно-правовой контроль над компьютерной преступностью в России

В целях борьбы с компьютерной преступностью российским законодательством (глава 28 УК РФ) предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ).

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

(в ред. Федерального [закона](#) от 07.12.2011 N 420-ФЗ)

1. [Неправомерный доступ](#) к охраняемой законом компьютерной информации, если это деяние повлекло [уничтожение](#), [блокирование](#), [модификацию](#) либо [копирование](#) компьютерной информации, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального [закона](#) от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные [частями первой](#) или [второй](#) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего [служебного положения](#), -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные [частями первой](#), [второй](#) или [третьей](#) настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

(в ред. Федерального [закона](#) от 07.12.2011 N 420-ФЗ)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные [частью первой](#) настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие [крупный ущерб](#) или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на

срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные **частями первой** или **второй** настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

(в ред. Федерального **закона** от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование **компьютерной информации**, причинившее **крупный ущерб**, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное **частью первой** настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

гл. 28, "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 03.07.2016) {КонсультантПлюс}

Для начала вспомним, что собой представляет мошенничество в сфере компьютерной информации. Как сказано в диспозиции статьи 159.6 УК РФ мошенничество в сфере компьютерной информации это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Следовательно, преступное посягательство происходит сразу на два предмета: имущество и компьютерную информацию. Компьютерная информация представляет собой сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, как указано в примечании к статье 272 УК РФ. Объективная сторона преступления выражается в действиях, кои перечислены в статье 159.6 УК РФ: ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Компьютерные хищения, как показало изучение уголовных дел, можно разделить на три основные группы:

1) с помощью сотовой связи через использование услуги «Мобильный банк»:

- владелец телефона утрачивает его по различным причинам (потеря или хищение), при этом потерпевший не отключает услугу «Мобильный банк» от сим-карты, таким образом, злоумышленник имеет возможность переводить денежные средства, хранящиеся на пластиковой карте собственника телефона на подконтрольные ему счета

- лицо меняет номер телефона, оставляя старую сим-карту, либо сим-карта с подключенной услугой «Мобильный банк» не используется в течении продолжительного времени, после чего компания

мобильной связи перепродаёт данный номер другому лицу, которое, получив смс-сообщение от банка, переводит денежные средства со счёта потерпевшего на свой счёт

- через смс-сообщения о имеющемся долге, блокировке карты или об отсутствии средств на счёте
- с помощью программы-вируса

2) преступления, связанные с приобретением и оплатой товара через мошеннические сайты. В таком случае потерпевшие, думая, что приобретают товар или услугу, перечисляют деньги мошенникам, взамен не получая ничего

3) преступления, связанные с возвратом потерянного имущества за вознаграждение или приобретением товаров и услуг посредством сети Интернет за вознаграждение, когда потерпевшие перечисляют денежные средства на банковские счета или номера телефонов злоумышленников

Особенной чертой данных видов преступлений является то, что преступники активно используют компьютерную информацию. Компьютерная информация часто не является предметом посягательства, но представляет обязательный элемент способа совершения мошенничества в сфере компьютерной информации.

Согласно примечанию к статье 272 УК РФ, под компьютерной информацией следует понимать сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Поэтому мнение, что квалифицировать по ст. 159.6 УК РФ необходимо только те деяния, которые совершаются с помощью сети Интернет, является ошибочным. Телефонные мошенничества также следует относить к преступлениям, совершаемым в сфере компьютерной информации. Однако, помимо компьютерной информации необходимо обратить внимание на прочие особенности, для определения, будет являться деяние мошенничеством или иным видом хищения.

Способами компьютерного мошенничества являются: ввод, модификация, блокирование, удаление компьютерной информации и иное вмешательство в функционирование средств хранения, обработки и передачи информации, а также информационно-телекоммуникационных сетей. Наиболее распространёнными способами являются:

- 1) Кража конфиденциальной информации о банковских картах (фишинг)
- 2) взлом паролей
- 3) Интернет-аукционы, где продавцы самостоятельно повышают ставки, дабы поднять цену выставленного на аукцион товара

Схема мошенничества в сфере компьютерной информации заключается в том, что злоумышленник, похищая имущество потерпевшего, осуществляет неправомерный доступ к компьютерной информации.

Каспийским городским судом Республики Дагестан по ч. 2 ст. 159.6 УК РФ привлечен к уголовной ответственности И. Используя компьютер, подключенный к сети Интернет, перечислил с электронного счёта, принадлежащего Р. на счет системы «Киви-кошелек» денежные средства в сумме 5560 рублей 60 копеек, после чего перечислил эту сумму на принадлежащий себе банковский счёт в ОАО «Экспресс-банк» и позднее через банкомат обналичил полученные незаконным путём денежные средства, причинив, таким образом, ущерб потерпевшему Р.¹

Нижегородским районным судом г. Нижнего Новгорода Л. была привлечена к уголовной ответственности по ч. 3 ст. 159.6 УК РФ. Л. работала в филиале коммерческого банка старшим специалистом отдела по работе с корпоративными клиентами. В июне 2012 года Л. начала переводить денежные средства со счетов клиентов банка на подконтрольные ей счета, оформленные по вымышленным данным. Л. провела финансовую корректировку с использованием автоматизированной системы расчетов Marti, после чего перевела денежные средства на имеющиеся у неё пластиковые карты, используя банковский сервис «Лёгкий платёж». После чего Л. создала несколько счетов на вымышленные имена Б. и Ж.

Согласно условиям работы банковского сервиса «Лёгкий платёж» для перевода денежных средств с абонентом, т.е. с физическим лицом, должен быть заключен договор, согласно которому максимальная сумма одной операции по абонентскому номеру составляет не более 14999 рублей, максимальная общая сумма платежей в сутки не более 30000 рублей. Для преодоления данных ограничений Л. неоднократно меняла абонентский номер на лицевых счетах, тем самым получая возможность проводить большее количество операций. В целом Л. по лицевому счету 1 на имя Б.

¹ Приговор Каспийского городского суда Республики Дагестан по делу Р. // <http://www.sudrf.ru> (дата обращения: 02.01.2017)

произвела 24 операции по замене абонентского номера, по лицевому счету 1 на имя Ж. – 31 операцию, по лицевому счету 2 на имя Б. – 14, по лицевому счету 2 на имя Ж. – 21.²

Таким образом, в период с июня по ноябрь 2012 года Л. со счетов клиентов банка похитила путем перевода на счета Б. и Ж. денежные средства на общую сумму 2613581 рублей 73 копейки. Продолжая реализацию своего преступного умысла, направленного на хищение денежных средств, Л. совершила финансовые корректировки на счетах клиентов банка, обосновав это тем, что тариф, применённый изначально, был неверен, хотя это и не соответствовало действительности, таким образом, Л. модифицировала компьютерную информацию. Похищенные денежные средства Л. перевела на имеющиеся у нее пластиковые карты и использовала их по собственному усмотрению.

На практике, ст. 159.6 УК РФ не редко применяется по совокупности со ст. 272 УК РФ, которая предусматривает ответственность за неправомерное завладение компьютерной информацией.

Иногда правоприменитель квалифицирует сообщение ложных сведений через телефонную сеть как мошенничество, а действия, не сопровождающиеся обманом, как кражу. Разберём на конкретном примере, как необходимо разграничивать указанные деяния.

В 2013 году Грачевским районным судом Ставропольского края был вынесен приговор в отношении Н., которая умышленно совершила мошенничество в сфере компьютерной информации. Н. получила на сотовый телефон смс-сообщение посредством услуги «Мобильный банк» о наличии на не принадлежащем ей банковском счёте, открытого на имя Ш., остатка денежных средств. Н., используя принадлежащий ей сотовый телефон марки «Самсунг» и номер телефона, зарегистрированного на имя Д., к которому ошибочно подключена услуга «Мобильный банк» Сбербанк России, путём ввода компьютерной информации, перечислила денежные средства со счёта Ш. на счёт, привязанный к сим-карте телефона «Самсунг».

Далее Н. путём ввода компьютерной информации в форме электрических сигналов с помощью сервиса «смс-сообщения» на номер «7878», воспользовавшись услугой денежных переводов, с учётом снятия комиссии за пользование услугой, перевела денежные средства со счёта сим-карты, зарегистрированного на Д. на счёт сим-карты, зарегистрированной на своё имя, тем самым распорядилась ими по своему усмотрению, причинив Ш. имущественный ущерб.³

В рассмотренном примере судом подчёркивается способ совершения преступления: путем ввода компьютерной информации в форме электрических сигналов, этим указывая на то, что преступное деяние было совершено именно с использованием компьютерной информации. Это следует выделить, так как в судебной практике достаточно распространена ошибка, при которой подобные деяния первоначально квалифицируются по ст. 159 УК РФ.

Кроме того, следует отграничивать мошенничество в сфере компьютерной информации от кражи. Например, обналичивание через банкомат денег с помощью похищенной банковской карты право применителем в настоящее время квалифицируется как кража. В то же время доктрина уголовного права отвергает возможность квалифицировать как кражу хищение имущества, не имеющего признаков вещи (в том числе права на имущество). Завладение банковской картой позволяет злоумышленнику получить право на имущество, а затем, осуществляя незаконный ввод компьютерной информации, получить доступ к денежным средствам. Указанные деяния квалифицируются по ст. 158 УК РФ, поскольку Пленум Верховного Суда РФ в п. 13 Постановления от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее - Постановление Пленума ВС РФ № 51) указывает на обязательный признак мошенничества - наличие обманутого физического лица.⁴ В то же время в пояснительной записке к законопроекту от 11.04.2012 «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (о выделении самостоятельных составов мошенничества) ВС РФ разъясняет, что подобное преступление совершается не путем обмана или злоупотребления доверием конкретного субъекта, а посредством

² Приговор Нижегородского районного суда г. Нижнего Новгорода по делу Л. // <http://www.sudrf.ru> (дата обращения: 02.01.2017)

³ Приговор Грачевского районного суда Ставропольского края по делу Н. // URL: <http://www.sudrf.ru> (дата обращения: 02.01.2017)

⁴ Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51 г. Москва «О судебной практике по делам о мошенничестве, присвоении и растрате» // Официальный сайт Российской газеты. URL: <https://rg.ru/2008/01/12/sud-voprosy-dok.html> (дата обращения: 28.12.2016)

получения доступа к компьютерной системе и совершения любого действия, прописанного в ст. 159.6 УК РФ.⁵ Следовательно, согласно выше изложенному, незаконное завладение денежными средствами лица посредством пластиковой карты необходимо квалифицировать как мошенничество в сфере компьютерной информации. Нужно отметить, что квалификация подобного деяния меняется на ст. 159.3 УК РФ «Мошенничество с использованием платежных карт», если оно совершено путем обмана уполномоченного работника кредитной, торговой или иной организации.

Впрочем, в ряде случаев судебной практики хищение денежных средств через использование услуги «Мобильный банк» квалифицируется как кража. В качестве примера приведём решение Пермского районного суда по делу Ш. Действия злоумышленника были квалифицированы по п. «в» ч. 2 ст. 158 УК РФ. Преступник, используя телефонный номер с подключённой услугой «Мобильный банк» тайно перевёл денежные средства на сумму 9611 рублей, принадлежащие потерпевшей М. на счёт другого телефонного номера, после чего распорядился похищенными средствами по своему усмотрению.⁶

В данном случае судом не были в должной мере проанализированы нормы закона и разъяснения, а так же не было обращено внимание на судебную практику по данному вопросу, что привело к ошибочной квалификации.

Одной из наиболее часто возникающих проблем является отсутствие в диспозиции ст. 159.6 УК РФ таких способов совершения мошенничества, как обман или злоупотребление доверием. Так как ст. 159.6 УК РФ является специальной нормой, предполагается, что указанный способ был заложен законодателем в смысл ст. 159.6 УК РФ по умолчанию, исходя из определения термина «мошенничество», предлагаемого в диспозиции ст. 159 УК РФ.

Много вопросов возникает при определении термина «иное вмешательство в функционирование средства хранения компьютерной информации», так как в законе трактовка данного термина нигде не даётся. Можно предположить, что под иным вмешательством следует понимать осуществление незаконных действий, изменяющих установленный процесс обращения с компьютерной информацией, в том числе ее обработки, хранения, использования и передачи.

Помимо этого, применение в законе термина «удаление информации» не совсем корректно с технической точки зрения. Затирание компьютерной информации не является удалением. По сути, информация остаётся, но становится скрытой. Данный факт не освобождает преступника от уголовной ответственности, так как затирание подпадает под иное вмешательство, moreover, следует отметить, что понятие «уничтожение», используемое в ст. 272 УК РФ, более точно отражает особенности рассматриваемого деяния.

Целый ряд правовых норм, касающихся ответственности за правонарушения в области СМИ, включая защиту прав журналистов, содержится в Законе «О средствах массовой информации» № 2124-І от 27.12.1991 г. Так, в ст. 58 данного закона закреплено, что ущемление свободы массовой информации, т.е. воспрепятствование в какой бы то ни было форме со стороны граждан, должностных лиц государственных органов и организаций, общественных объединений, законной деятельности учредителей, редакций, издателей и распространителей продукции СМИ, а также журналистов, в том числе посредством осуществления цензуры, влечет ответственность в соответствии с законодательством РФ. Обнаружение органов, организаций, учреждений или должностей, в задачи либо функции которых входит осуществление цензуры массовой информации, влечет немедленное прекращение их финансирования и ликвидацию и т.д.

За совершение преступлений в сфере компьютерных и информационных технологий предусматривается уголовная ответственность. Стоит отметить, что эти преступления можно считать абсолютно новой разновидностью, так как их не существовало в уголовном законодательстве до 1996 года⁷. В Уголовном кодексе Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.07.2016) (далее

⁵ Пояснительная записка к проекту Федерального закона от 11.04.2012 N 53700-6 "О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации" // СПС «КонсультантПлюс»

⁶ Приговор Пермского городского суда по делу Ш. // <http://www.sudrf.ru> (дата обращения: 03.01.2017).

⁷ Кудрявцев В.Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического

– УК РФ) данная разновидность преступлений регулируется положениями Главы 28 «Преступления в сфере компьютерной информации». Данная глава является наименьшей по количеству статей всего Раздела IX УК РФ, в ней всего три статьи – 272-274: неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Следует подчеркнуть, что ни одна из этих статей не предусматривает возможности привлечения к ответственности лиц с 14 лет, в соответствии с ч. 2 ст. 20 УК РФ.

Практические примеры анализируемой категории преступления находим в судебной практике. Рассмотрим пример: *гражданином Ш. было совершено незаконное использование объектов авторского права, приобретение, хранение контрафактных экземпляров произведений в целях сбыта, совершенные в крупном размере, а также распространение компьютерных программ, заведомо предназначенных для несанкционированной модификации компьютерной информации. Вина подсудимого была доказана, в том числе и результатами проведённого обыска по месту жительства Ш., где были изъяты системный блок компьютера и диск DVD-R. Изъятые объекты были переданы на компьютерно-техническую экспертизу. Согласно заключению компьютерно-технической экспертизы, на представленном компакт диске содержалась коммерческая версия программного продукта «...», имеющая существенные признаки отличия от лицензионных вариантов. В файловых структурах установочного комплекта программных продуктов содержалось вредоносное программное обеспечение, позволяющее осуществить несанкционированное уничтожение, блокирование, модификацию, копирование, внесение изменений в существующие программы или производящие нейтрализацию средств защиты компьютерной информации, что позволяло использовать программу неограниченное время – в директории папки D:\K.g.\...\Crack\, содержащей вредоносный программный продукт – программу «Компас_3D_V12_antiHASp_vl.0.exe», предназначенную для эмуляции ключа аппаратной защиты HASp, путём модификации системного реестра ОС. Данная программа позволяла осуществить несанкционированное уничтожение, блокирование, модификацию, копирование, внесение изменений в существующие программы или производит нейтрализацию средств защиты компьютерной информации. Данный программный продукт являлся вредоносным⁸. Суд квалифицировал действия Ш по ч.2 ст. 146 УК РФ, как незаконное использование объектов авторского права, приобретение, хранение, контрафактных экземпляров произведений в целях сбыта, совершенные в крупном размере и по ч.1 ст. 273 УК РФ как распространение компьютерных программ, заведомо предназначенных для несанкционированной модификации компьютерной информации. Судья прекратил уголовное дело в связи с наличие оснований для признания раскаяния подсудимого Ш деятельным и свидетельствующим об утрате им общественной опасности.*

правопорядка. Материалы международной научно-практической конференции (Нижний Новгород, 1 марта 2012 года) / Под ред.: Козлов А.В., Панченко П.Н. - Нижний Новгород: НИУ ВШЭ - Нижний Новгород, 2012. С. 69-76.

⁸ Архив Первомайского районного суда г. Ижевска Удмуртской Республики, постановление о прекращении уголовного дела №1-316/12 от 29 июня 2012 г. – [Электронный ресурс]. Режим доступа: <http://sudact.ru/regular/doc/jggEQVTdCdG> (дата обращения 04.08.2016).

Глава 3 Принципы построения системы информационной безопасности

• **Государственное регулирование информационной безопасности**

Новые информационные технологии, органически встраиваясь в информационные системы экономических объектов и повышая эффективность и качество их работы, породили и проблемы обеспечения информационной безопасности. Возникли мало изученные информационные угрозы, реализация которых может приводить к непредсказуемым и даже катастрофическим последствиям, сводя на нет все усилия по повышению эффективности управления экономическим объектом. Ежегодный ущерб от компьютерных злоупотреблений только в США составляет от 100 млн. до 7.5 млрд. долларов. Утечка только 20 процентов коммерческой информации в 60 случаях из 100 приводит к банкротству фирм.

Законодательный, административный и процедурный уровни

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Необходимо всячески подчеркивать важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ - все это функции законодательного уровня.

На законодательном уровне особого внимания заслуживают **правовые акты и стандарты**.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Но то, что для Уголовного или Гражданского кодекса естественно, по отношению к Закону об информации, информатизации и защите информации является принципиальным недостатком. Сами по себе **лицензирование и сертификация** не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ. Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится.

На этом фоне поучительным является знакомство с законодательством США в области ИБ, которое гораздо обширнее и многограннее российского.

Среди стандартов выделяются "**Оранжевая книга**", рекомендации **X.800** и "Критерии оценки безопасности информационных технологий".

"Оранжевая книга" заложила понятийный базис; в ней определяются важнейшие **сервисы безопасности** и предлагается метод **классификации** информационных систем по требованиям безопасности.

Рекомендации X.800 весьма глубоко трактуют вопросы защиты **сетевых конфигураций** и предлагают развитый набор сервисов и **механизмов безопасности**.

Международный стандарт ISO 15408, известный как "**Общие критерии**", реализует более современный подход, в нем зафиксирован чрезвычайно широкий спектр сервисов безопасности (представленных как **функциональные требования**). Его принятие в качестве национального стандарта важно не только из абстрактных соображений интеграции в мировое сообщество; оно, как можно надеяться, облегчит жизнь владельцам информационных систем, существенно расширив спектр доступных сертифицированных решений.

Главная задача мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции начали борьбу с ней при помощи традиционных норм о краже, присвоении, мошенничестве, злоупотреблении доверием и др. Однако такой подход оказался не вполне удачным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений.

Несоответствие криминологической реальности и уголовно-правовых норм потребовало развития последних. Развитие это происходит в двух направлениях:

- более широкое толкование традиционных норм;
- разработка специализированных норм о компьютерных преступлениях.

В передовых странах Запада процесс этот идет уже не один десяток лет: в США - с конца 70-х гг., в Великобритании - с конца 80-х.

Впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона уже в 1978 г. Принятый закон назывался "Computer crime act of 1978" и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные

преступления. В частности, в соответствии с ним противоправные действия, связанные с модификацией, уничтожением, несанкционированным доступом или изъятием компьютерных данных, программ или сопутствующей документации признавались преступлениями и наказывались пятью годами лишения свободы либо штрафом в размере 5000 долл. или тем и другим одновременно в зависимости от тяжести причиненного жертве ущерба.

Те же действия, совершенные с целью хищения какой-либо собственности, наказывались 15 годами лишения свободы либо штрафом в размере 10 000 долл., или тем и другим одновременно. (...)

Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства. Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений. На их правовой базе в первой половине 80-х гг. было разработано федеральное законодательство США, посвященное регулированию правовых вопросов этой проблемы. Данное законодательство было принято Федеральным собранием США в 1984 г. и называлось "Comprehensive crime control act of 1984". В него, в частности, входил первый федеральный закон США по борьбе с компьютерной преступностью, который получил название "Закон об использовании электронных устройств, обеспечивающих несанкционированный доступ к ЭВМ, злоупотреблениях и мошенничестве с помощью компьютеров".

В итоге уже в начале 90-х гг. в США действовали следующие законы: Федеральный закон об ответственности за преступления, связанные с компьютерами; Закон о поддельных средствах доступа, компьютерном мошенничестве и злоупотреблении; Федеральный закон о частной тайне.

Одним из важных шагов в законотворческой деятельности являются принятый сенатом США законопроект о "Об экономическом шпионаже", в соответствии с которым тюремное заключение сроком до 25 лет и штраф до 250 тысяч долларов грозит тем, кто запускает вирусы в компьютерные сети, используемые правительством и финансовыми институтами Америки, а также Акт об экономическом шпионаже, в котором кража информации, представленная в электронном виде, официально признается преступлением.

Преступления, совершаемые с помощью компьютера в финансово-кредитной системе, в особенности отмывание денег, нажитых преступным путем, приняли мировой масштаб. Законодатели, стараясь обезопасить свои страны от его проникновения, издали ряд законов, направленных на организацию контроля государственными органами и банками вкладов и денежных переводов граждан. Что же предусматривается в этой связи в США:

- каждое финансовое учреждение должно предоставлять службе казначейства (агентству внутренних дел) декларацию для совершения различных банковских операций на сумму более 10 тыс. долларов;
- игорные дома с общим годовым доходом свыше одного миллиона долларов вносятся в список финансовых организаций, которые обязаны регистрировать денежные операции на сумму свыше 10 тыс. долларов;
- министр финансов уполномочен выплачивать вознаграждение лицам, которые предоставляют ему сведения (из первых рук) о нарушении финансовой дисциплины при совершении операций на сумму свыше 50 тыс. долларов. Вознаграждение ограничивается либо 25% конфискованной суммы, либо 150 тыс. долл.

Попытки регулирования отношений в сфере компьютерной информации уже не один десяток лет предпринимаются не только в США, но и в других развитых странах.

Примером такого регулирования может стать соответствующее законодательство ФРГ. В 1986 г. Бундестагом был принят второй закон о борьбе с экономической преступностью, которым в Уголовный кодекс было введено семь новых параграфов, содержащих описание компьютерных преступлений. В частности, § 202а УК ФРГ предусматривает уголовную ответственность лиц, незаконно приобретающих для себя или иного лица непосредственно не воспринимаемые, записанные в устройства памяти либо переданные данные, специально защищенные от несанкционированного доступа. Состав так называемого компьютерного мошенничества изложен в § 263 а, в соответствии с которым уголовной ответственности подлежат лица, оказавшие влияние на результаты процесса обработки информации путем неправильного оформления программ (манипуляцией с программным обеспечением).

Российская действительность не является исключением и каждодневно приносит новые примеры преступлений в сфере информатизации и компьютеризации. Последние потребовали от

российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности.

* Лазарев А. Статья для хакера // весь компьютерный мир, 1997, №1. С.9.

** Фемида США не успевает // Компьютера, 1996, № 49. С.8.

Обзор российского законодательства в области информационной безопасности Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - *право на знание достоверной информации о состоянии окружающей среды*.

В принципе, **право на информацию** может реализовываться средствами бумажных технологий, но в современных условиях *наиболее* практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и *судебными* органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение **их** (серверов) информационной безопасности.

Нормативные документы в области информационной безопасности

В РФ к нормативно-правовым актам в области информационной безопасности относятся:

➤ Акты федерального законодательства:

- Международные договоры РФ;
- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления Правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т.д.

К нормативно-методическим документам можно отнести

- Методические документы государственных органов России:

- Доктрина информационной безопасности РФ (Утверждена указом Президента Российской Федерации от 5 декабря 2016 г. №646);
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ.

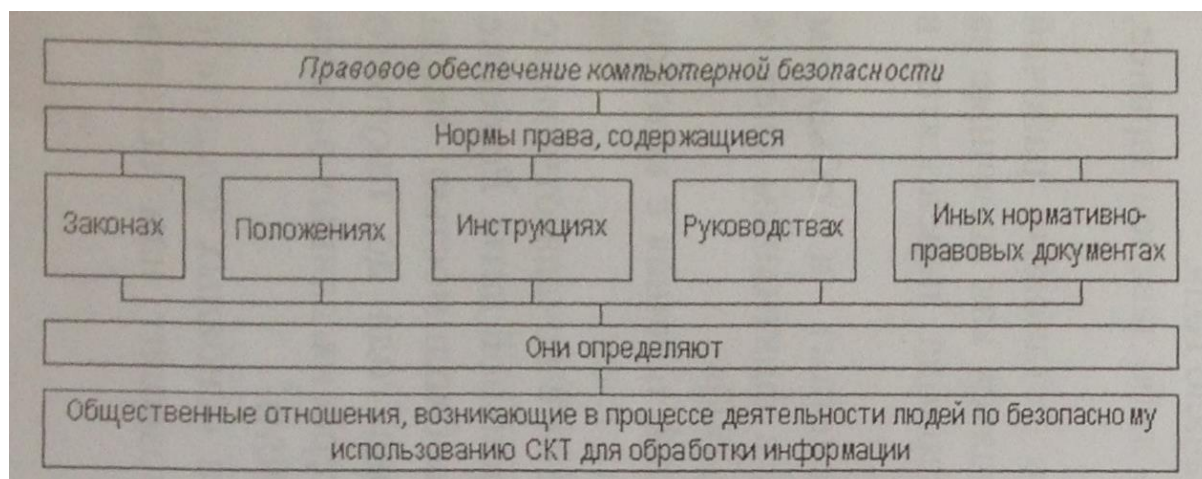


Рис. 1.2.1.

- документы и стандарты, регламентирующие защиту объектов информатизации от несанкционированного доступа к информации;
- документы и стандарты, регламентирующие требования к подсистеме криптографической защиты;
- документы, регламентирующие защиту объектов информатизации от воздействий вредоносных программ;
- документы и стандарты, регламентирующие особенности защиты сетей передачи данных;
- документы и стандарты, регламентирующие защиту объектов информатизации от утечки информации по техническим каналам;
- документы и стандарты, регламентирующие защиту зданий, помещений и контролируемых зон объекта информатизации;
- документы и стандарты, регламентирующие защиту объекта информатизации от внешних воздействующих факторов;
- стандарты, регламентирующие требования к оформлению документации и документов на объект информатизации;
- документы и стандарты, регламентирующие оценку качества объекта информатизации, виды испытаний этих объектов;
- стандарты в области терминов и определений.

По В.И. Ярочкину, *предметами правового регулирования* в области обеспечения информационной, в том числе компьютерной, безопасности являются [78, с. 214]:

- правовой режим информации, средств информатики, индустрии информатизации и систем информационных услуг в условиях риска, средства и формы защиты информации;
- правовой статус участников правоотношений в процессах информатизации;
- порядок отношений субъектов с учетом их правового статуса на различных стадиях и уровнях процесса функционирования информационных структур и систем.

По Э. П. Крюковой [110, с. 116], правовое обеспечение информационной безопасности означает:

- *защиту интересов физических лиц* - путем введения норм, устанавливающих пределы сбора и использования сведений об этих лицах со стороны государства и иных субъектов;
- *защиту интересов государства и общества* - путем установления приоритетов защиты информации, охраняемой как собственность государства¹;
- *защиту интересов юридических и физических лиц* - путем установления норм, регулирующих обращение с охраняемой информацией, обеспечивающей деятельность этих лиц, и установления механизмов защиты этих субъектов.

Правовое обеспечение компьютерной безопасности включает в себя виды деятельности, представленные на рис. 1.2.2.

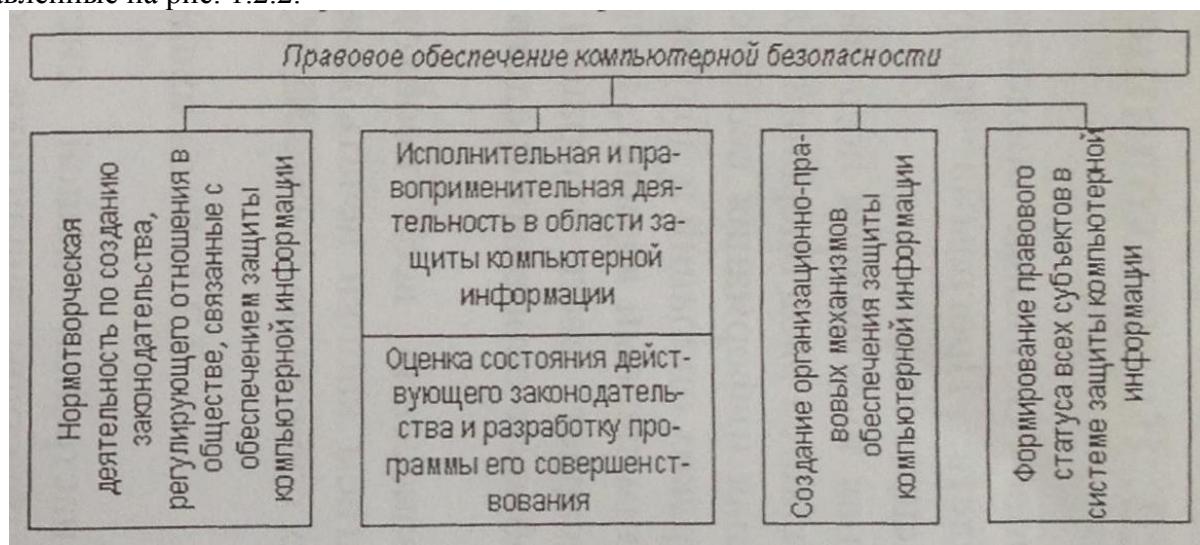
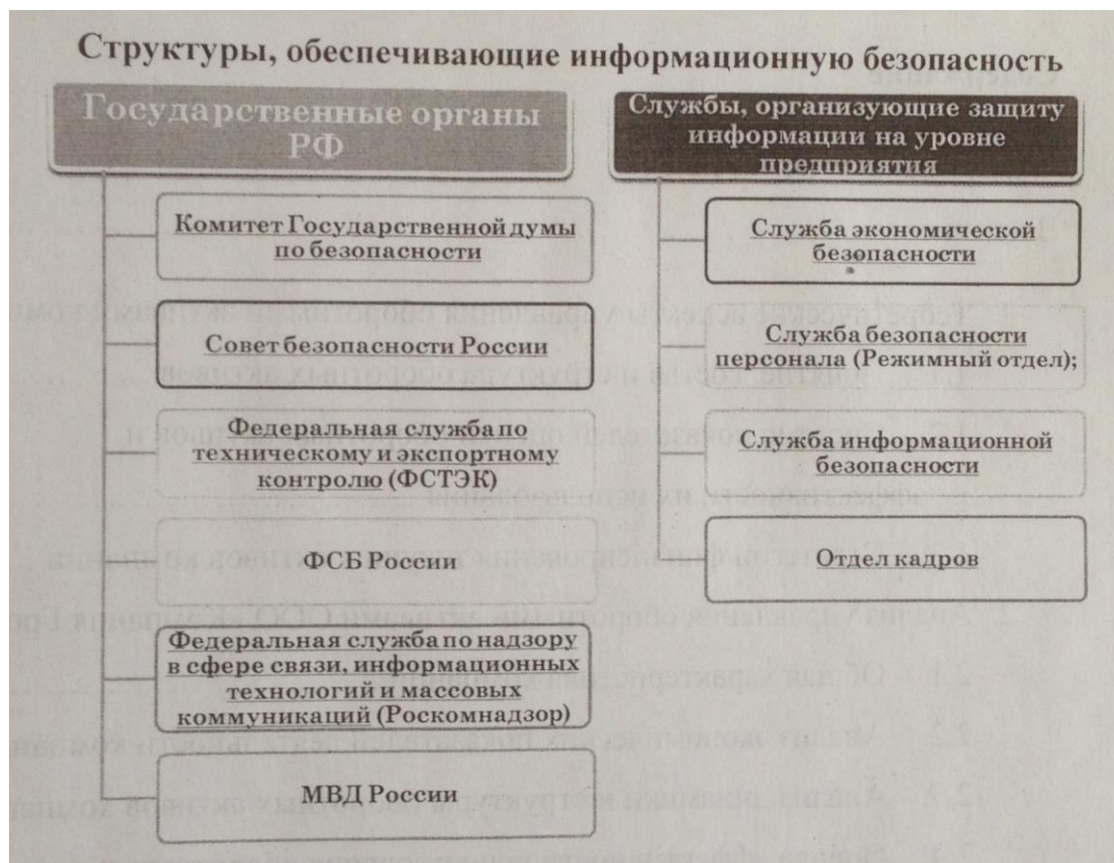


Рис. 1.2.2.

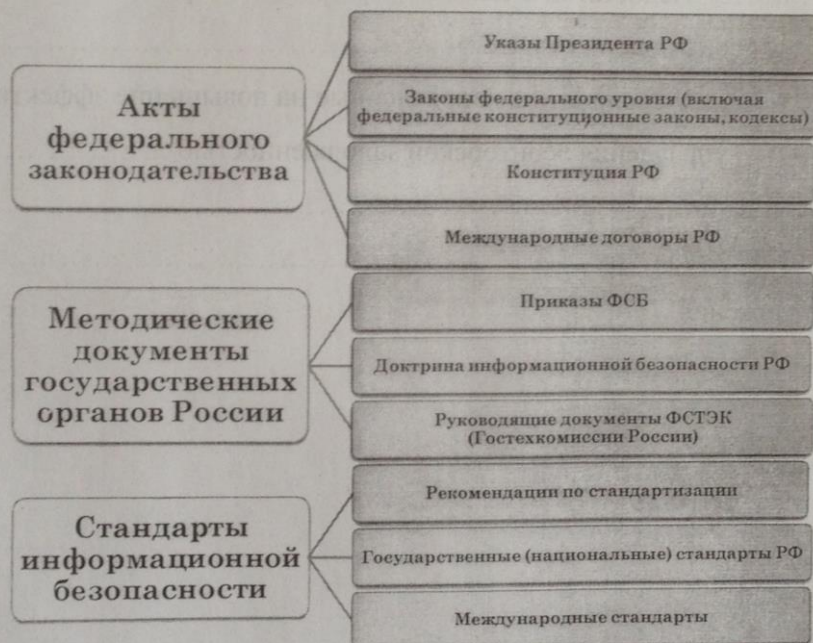
С учетом того, что в современных условиях все большая часть информации обрабатывается с использованием СКТ, данные направления можно отнести и к правовому обеспечению компьютерной

безопасности.

¹ Собственник информации - субъект, в полном объеме реализующий права владения пользования, распоряжения информацией в соответствии с законодательством.



Нормативно-правовые аспекты информационной безопасности



Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается или наказывается

обществом, что так поступать не принято. В рамках обеспечения информационной безопасности следует рассмотреть на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

К первой группе следует отнести основные законодательные акты по информационной безопасности, являющиеся частью правовой системы Российской Федерации.

В Конституции РФ содержится ряд правовых норм, определяющих основные права и свободы граждан России в области информатизации, в том числе ст. 23 определяет право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; ст. 42 обеспечивает право на получение достоверной информации о состоянии окружающей среды и др.

В Уголовном кодексе РФ имеются нормы, затрагивающие вопросы информационной безопасности граждан, организаций и государства. В числе таких статей ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых и телеграфных или иных сообщений», ст. 140 «Отказ в предоставлении гражданину информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование или распространение вредоносных программ для ЭВМ», ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» и др.

В Налоговом кодексе РФ имеется ст. 102 «налоговая тайна».

В Гражданском кодексе РФ вопросам обеспечения информационной безопасности посвящены ст. 139 «Служебная и коммерческая тайна», ст. 946 «Тайна страхования» и др.

Специальное законодательство в области информатизации и информационной безопасности включает ряд законов, и их представим в календарной последовательности.

С принятием в 1992 г. Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» впервые в России программное обеспечение компьютеров было законодательно защищено от незаконных действий. В том же году был принят Закон РФ «О правовой охране топологий интегральных микросхем».

Кодекс РФ об административных правонарушениях устанавливает ответственность за нарушение законодательства в области защиты информации.

Статья 13.12 предусматривает ответственность за нарушение правил защиты информации:

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от 3 до 5 МРОТ; на должностных лиц - от 5 до 10 МРОТ; на юридических лиц - от 50 до 100 МРОТ.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от 5 до 10 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от 10 до 20 МРОТ; на юридических лиц - от 100 до 200 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от 20 до 30 МРОТ; на юридических лиц - от 150 до 200 МРОТ.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на

должностных лиц в размере от 30 до 40 МРОТ; на юридических лиц - от 200 до 300 МРОТ с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.13 предусматривает ответственность за незаконную деятельность в области защиты информации.

1. Занятие видами деятельности в области защиты информации без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от 5 до 10 МРОТ с конфискацией средств защиты информации или без таковой; на должностных лиц - от 20 до 30 МРОТ с конфискацией средств защиты информации или без таковой; на юридических лиц - от 100 до 200 МРОТ с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от 40 до 50 МРОТ; на юридических лиц - от 300 до 400 МРОТ с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

В 1993 г. принят Закон РФ «Об авторском праве и смежных правах», регулирующий отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства, фонограмм, исполнений и пр.

В 1993 г. был также принят Закон РФ «О государственной тайне», регулирующий отношения, возникающие в связи с отнесением сведений к государственной тайне.

В 1995 г. принят закон «О связи», регламентирующий на правовом уровне деятельности в области связи.

Федеральный закон 1995 г. «Об информации, информатизации и защите информации» определяет ряд важных понятий таких, как информация, документ, информационные процессы, ресурсы и пр., а также регулирует отношения, возникающие при формировании и использовании информационных ресурсов, информационных технологий, защите информации и др. Правда, положения этого закона носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно (прил. №1).

К группе направляющих и координирующих законов и нормативных актов относится целая группа документов, регламентирующих процессы лицензирования и сертификации в области информационной безопасности. Главная роль здесь отводилась Федеральному агентству правительственной связи и информации (ФАПСИ) и Государственной технической комиссии (Гостехкомиссии) при Президенте РФ.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами.

Самое важное на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями информационных технологий. Конечно, законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Неуклонный рост компьютерной преступности заставил законодателей России принять адекватные меры по борьбе с этим видом противоправных деяний, в т.ч. и уголовно-правовых. Главным является вступление в законную силу с 1 января 1997 г. нового Уголовного кодекса РФ, в который впервые включена глава «преступления в сфере компьютерной информации». Но начавшаяся работа нового УК РФ сразу же поставила ряд сложных вопросов перед наукой уголовного права и практикой ее применения. Нерешенные противоречия возникают при юридическом анализе преступлений в сфере компьютерной информации, а также во время проведения квалификации указанного вида преступлений.

Преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК); нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (274

УК). Ст.159 «Мошенничество».

Доктрина информационной безопасности Российской Федерации (далее - Доктрина) утверждена Президентом РФ в декабре 2016 г.

В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

В 2006 г. принят Закон «Об электронной подписи» (с изм. и доп. от 2015 г.), необходимый для развития системы электронных платежей.

В целях защиты информационных ресурсов РФ необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными экономически важными производствами;
- интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечить защиту сведений, составляющих государственную тайну;
- расширять международное сотрудничество РФ в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.
- осуществлять мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов РФ, на предприятиях, в учреждениях и организациях независимо от формы собственности;
- развернуть работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Обеспечение информационной безопасности РФ в сфере экономики играет ключевую роль в обеспечении национальной безопасности РФ.

Воздействию угроз информационной безопасности РФ в сфере экономики наиболее подвержены:

- 1) система государственной статистики;
- 2) кредитно-финансовая система;
- 3) информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;
- 4) системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;
- 5) системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Основными мерами по обеспечению информационной безопасности в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;
- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;
- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;
- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;
- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

Статья 23 Конституции гарантирует **право на личную и семейную тайну**, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к **средствам защиты информации**.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как **банковская, коммерческая и служебная тайна**. Согласно статье 139, информация составляет **служебную или коммерческую тайну** в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие у доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе **"О государственной тайне"** (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

Закон "Об информации, информационных технологиях и защите информации" № 149-ФЗ от 27.03.2006 г. с изм. от 21.07.2014 г.

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

* **информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

* **документированная информация** (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

* **информационные процессы** - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

К подзаконным нормативным актам в области информатизации относятся соответствующие Указы Президента РФ, Постановления Правительства РФ, Приказы и другие документы, издаваемые федеральными министерствами и ведомствами. Например, Указ Президента РФ об утверждении перечня сведений конфиденциального характера от 6 марта 1997 г. № 188 (прил. №2).

Для создания и поддержания необходимого уровня информационной безопасности в фирме разрабатывается система соответствующих правовых норм, представленная в следующих документах:

- Уставе и/или учредительном договоре;
- коллективном договоре;
- правилах внутреннего трудового распорядка;
- должностных обязанностях сотрудников;
- специальных нормативных документах по информационной безопасности (приказах, положениях, инструкциях);
- договорах со сторонними организациями;
- трудовых договорах с сотрудниками;
- иных индивидуальных актах.

Подробнее см. 3.3.

ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Дата актуализации: 21.05.2015



Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Обозначение:   [ГОСТ Р ИСО/МЭК 27005-2010](#)

Обозначение
англ:   [GOST R ISO/IEC 27005-2010](#)

Статус: [действует](#)

Название рус.: Информационная технология. Методы и средства обеспечения безопасности.
Менеджмент риска информационной безопасности

Название англ.: Information technology. Security techniques. Information security risk management

Дата
добавления в 01.09.2013
базу:

Дата
актуализации: 21.05.2015

Дата введения: 01.12.2011

Область применения: Стандарт представляет руководство по менеджменту риска информационной безопасности. Стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска. Знание концепций, моделей, процессов и терминологии, изложенных в ИСО/МЭК 27001 и ИСО/МЭК 27002, важно для полного понимания стандарта. Стандарт применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации.

Оглавление:

- 1 Область применения
- 2 Нормативные ссылки
- 3 Термины и определения
- 4 Структура национального стандарта
- 5 Предпосылки создания стандарта
- 6 Обзор процесса менеджмента риска информационной безопасности

7	Установление контекста
7.1	Общие положения
7.2	Основные критерии
7.3	Область применения и границы
7.4	Организационная структура менеджмента риска информационной безопасности
8	Оценка риска информационной безопасности
8.1	Общее описание оценки риска информационной безопасности
8.2	Анализ риска
8.3	Оценка риска
9	Обработка риска информационной безопасности
9.1	Общее описание обработки риска
9.2	Снижение риска
9.3	Сохранение риска
9.4	Предотвращение риска
9.5	Перенос риска
10	Принятие риска информационной безопасности
11	Коммуникация риска информационной безопасности
12	Мониторинг и переоценка риска информационной безопасности
12.1	Мониторинг и переоценка факторов риска
12.2	Мониторинг, анализ и улучшение менеджмента риска
	Приложение А (справочное) Определение области применения и границ процесса менеджмента риска информационной безопасности
	Приложение В (справочное) Определение и установление ценности активов и оценка влияния . . .
	Приложение С (справочное) Примеры типичных угроз
	Приложение D (справочное) Уязвимости и методы оценки уязвимости
	Приложение Е (справочное) Подходы к оценке риска информационной безопасности
	Приложение F (справочное) Ограничения, относящиеся к снижению риска
	Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации
	Библиография

Разработан: ООО НПФ Кристалл
ФГУ ГНИИИ ПТЗИ ФСТЭК России

Утверждён: 30.11.2010 Федеральное агентство по техническому регулированию и метрологии (632-ст)

Издан: Стандартиформ (2011 г.)

Заменяет собой:

-   ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»
 -   ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»
-

без делопроизводства не обойтись



Рис. В. Ушаков

Международное признание как документ, определяющий общие направления в управлении информационной безопасностью, получил стандарт ISO/IEC 17799:2000. Он сумел завоевать авторитет и признание у организаций различных отраслей экономики многих стран мира. И в нашей стране он также активно используется.

Международная организация по стандартизации ISO опубликовала 20 июня 2005 года новую версию стандарта ISO 17799. В нее внесено значительное количество изменений и дополнений. Основные усилия разработчиков были направлены на придание ему большей универсальности. Многие положения, формулировавшиеся ранее как **требования только к программному обеспечению**, изменены таким образом, чтобы **распространить их действие и на другие сферы деятельности и виды ресурсов**.

Нововведения и изменения

Разработчики стандарта постарались отследить из-

менения в законодательных актах, постановлениях правительства, защите персональных данных и прав интеллектуальной собственности) и соответствующее усиление требований к обеспечению информационной безопасности.

Изменился стиль и формат подачи информации. Теперь четко выделяются **мера обеспечения информационной безопасности и указания по ее практической реализации**, основной упор делается на меры по обеспечению соответствия законодательно-нормативным требованиям.

Хотя первая версия стандарта и говорила о необходимости оценки рисков, чтобы определить, какие требования стандарта применимы в конкретной организации, но ничего не говорила о том, как ее проводить. В новой версии даны

стандарты ISO по оценке рисков.

В специальной главе говорится о порядке обновления об инцидентах и выявленных слабых местах в системе информационной безопасности, организации работы для их предотвращения и эффективного реагирования при их возникновении (включая вопросы распределения ответственности, разработки процедур, извлечения уроков из накопленного опыта и сбора доказательств).

Стала подробнее указана по классификации ресурсов и более подробно рассматриваются меры обеспечения информационной безопасности: инвентаризация, определение ответственных, классификация, маркировка и правильное использование информационных ресурсов. Это особенно важно для организаций, желающих **защитить информацию, подпадающую под законодательно-нормативные требования или являющуюся интеллектуальной собственностью**.

Глава «Безопасность, связанная с персоналом» была переименована в «Кадровую безопасность» и значительно расширена. В нее включены указания по мерам безопасности, которые необходимо выполнять до приема сотрудников на работу (проверка сотрудников, определение прав и обязанностей, условия найма, управление обязанностями, обучение безопасности, дисциплинарные меры, увольнение или пе-

реходные требования к обеспечению соответствия деятельности организации законодательно-нормативным и иным требованиям, а также **растущая популярность стандарта по управлению документами ISO 15489** и накопленный опыт работы с определенными видами электронных документов.

За подробными указаниями по управлению документами новая версия отсылает к стандарту ISO 15489-1, который, надо полагать, теперь уже официально будет использоваться при сертификации по стандартам информационной безопасности. Ссылка на то, что организация должна обеспечивать свою информационную безопасность в области управления документами, основываясь на положениях первого в мире международного стандарта по делопроизводству, очень важна, поскольку **фактически обязывает специалистов в области информационных технологий и информационной безопасности использовать его требования в своей работе**.

Изменились требования к хранению зашифрованных документов и документов, подписанных ЭЦП. В прежней версии стандарта говорилось о необходимости сохранять криптографические ключи и предоставлять их по мере необходимости авторизованным сотрудникам. Теперь предлагается **обеспечить сохранность и целостность, относящихся к использо-**

вать, аутентичность ЭЦП и расшифровать документы в течение всего срока их хранения.

Все разделы стандарта содержат **требования к документированию деятельности организации по обеспечению информационной безопасности**. Правильно организованное управление документами необходимо для решения поставленных задач и для успешного прохождения международной сертификации.

Система везде и всюду

Сам стандарт ISO 17799 является сводом правил «хорошей деловой практики» и не предназначен для сертификации. Комитет — разработчик стандарта в начале июля выпустил финальный проект «шарного» стандарта ISO 27001 «Требования к системам управления информационной безопасностью» (на основе известного британского стандарта BS799-2) и собирается в конце 2005 года опубликовать его окончательный вариант. **ISO 27001 описывает систему управления информационной безопасностью**, в рамках которой можно выбирать и использовать отдельные меры, содержащиеся в ISO 17799, и именно по требованиям ISO 27001 планируется организовать **проведение международной сертификации**. Кроме того, в нем проведена дальнейшая «гармонизация» подходов с другими стандартами менеджмента ка-

«планируй — выполняй — проверяй — исправляй»).

Новая серия

Стандарты ISO, относящиеся к одной теме, обычно группируются в серии. Примерами служат IS 9000 по управлению качеством и ISO 14000 по управлению окружающей средой. Теперь формируется новая серия **ISO 27000 информационной безопасности**. Стандарт ISO 27001 — первый в ней. Предполагается, что в конечном итоге стандарт ISO 17799 будет «переименован» в ISO 27000. Разрабатывается еще один документ — по метрике оценки безопасности, который предполагается впоследствии опубликовать как ISO 27004.

В России планируется утвердить ISO 17799 как национальный стандарт в конце 2005 года, но пока не ясно, будут ли соответствовать версии 2005 года или старой версии 2000 года.

Обновленный стандарт ISO 17799 будет полезен при создании современной системы информационной безопасности как в государственных, так и в коммерческих организациях. Не малое внимание уделено вопросам безопасности, связанным с персоналом организации, и говорится о защите таких важных информационных ресурсов, как бумажная документация и сведения, хранящиеся в головах сотрудников. Стандарт и его положения можно использовать при разработке внутренних нормативных документов организации. Знание его положений повышает квалификацию персонала.

Н. Храмцовская

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
9 июня 2012 г. N 382-П

ПОЛОЖЕНИЕ
О ТРЕБОВАНИЯХ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ И О ПОРЯДКЕ
ОСУЩЕСТВЛЕНИЯ БАНКОМ РОССИИ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ
ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ
ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ

Глава 1. Общие положения

1.1. На основании Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" (Собрание законодательства Российской Федерации, 2011, N 27, ст. 3872) (далее - Федеральный закон N 161-ФЗ) настоящее Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств (далее - требования к обеспечению защиты информации при осуществлении переводов денежных средств), а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

1.2. Оператор по переводу денежных средств обеспечивает выполнение банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к обеспечению защиты информации при осуществлении переводов денежных средств, с учетом перечня операций, выполняемых банковскими платежными агентами (субагентами), и используемых автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается банковскими платежными агентами (субагентами). Оператор по переводу денежных средств обеспечивает контроль соблюдения банковскими платежными агентами (субагентами), привлекаемыми к деятельности по оказанию услуг по переводу денежных средств, требований к защите информации при осуществлении переводов денежных средств.

1.3. Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры могут привлекать организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

Глава 2. Требования к обеспечению защиты информации при осуществлении переводов денежных средств

Год назад вступил в силу федеральный закон «О персональных данных» № 152, направленный на защиту личной информации. Что изменилось?

- Инициатива законодателей была своевременна: участились случаи мошенничества, связанные с использованием персональных данных, в том числе для изъятия крупных сумм денег, - говорит Олег Тимофеев, член совета Нижегородского регионального отделения Ассоциации юристов РФ. - Но, на мой взгляд, и год спустя не

решена проблема обеспечения должного уровня безопасности хранения информации, защиты от утечек из баз данных крупных организаций: государственных структур, страховых компаний, банков, it-компаний и других. Дело не только в техническом обеспечении, но и в формировании правильного отношения к персональным данным. Люди должны понимать: даже паспорт, оставленный на пару минут на стойке администрации, - это бесценная информация.

К персональным данным могут быть отнесены сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, - иным нематериальным благам и имущественным интересам:

- биграфические и опознавательные данные (в том числе об обстоятельствах рождения, усыновления, развода);
- яичные характеристики (в том числе о личных привычках и наклонностях);
- сведения о семейном положении (в том числе о семейных отношениях);
- сведения об имущественном, финансовом положении (кроме случаев, прямо установленных в законе);
- состоянии здоровья.

Субъектами права здесь выступают:

- субъекты персональных данных - лица, к которым относятся соответствующие данные, и их наследники;
- держатели персональных данных - органы государственной власти и органы местного самоуправления, юридические и физические лица, осуществляющие на законных основаниях сбор, хранение, передачу, уточнение, блокирование, обезличивание, уничтожение персональных данных (баз персональных данных).

Персональные данные и работа с ними должны соответствовать следующим требованиям:

1. Персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства.
2. Персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме, за исключением случаев, прямо установленных в законе.
3. Персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации.
4. Персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться.
5. Персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или по миновании надобности.
6. Персональные данные охраняются в режиме конфиденциальной информации, исключающем их случайное или несанкционированное разрушение или случайную их утрату, а равно Несанкционированный доступ к данным, их изменение, блокирование или передачу.
7. Для лиц, занимающих высшие государственные должности, и кандидатов на эти должности может быть установлен специальный правовой режим для их персональных данных, обеспечивающий

открытость только общественно значимых данных.



КонсультантПлюс
надежная правовая поддержка

Федеральный закон от 27.07.2006 N 149-ФЗ
(ред. от 13.07.2015)
"Об информации, информационных
технологиях и о защите информации"
(с изм. и доп., вступ. в силу с 10.01.2016)

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ
И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят
Государственной Думой
8 июля 2006 года

Одобен
Советом Федерации
14 июля 2006 года

Список изменяющих документов
(в ред. Федеральных законов от 27.07.2010 № 227-ФЗ,
от 06.04.2011 № 65-ФЗ, от 21.07.2011 № 252-ФЗ,
от 28.07.2012 № 139-ФЗ, от 05.04.2013 № 50-ФЗ,
от 07.06.2013 № 112-ФЗ, от 02.07.2013 № 187-ФЗ,
от 28.12.2013 № 396-ФЗ, от 28.12.2013 № 398-ФЗ,
от 05.05.2014 № 97-ФЗ, от 21.07.2014 № 222-ФЗ,
от 21.07.2014 № 242-ФЗ, от 24.11.2014 № 364-ФЗ,
от 31.12.2014 № 531-ФЗ, от 29.06.2015 № 188-ФЗ,
от 13.07.2015 № 263-ФЗ, от 13.07.2015 № 264-ФЗ)

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:
- 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
 - 2) применении информационных технологий;
 - 3) обеспечении защиты информации.
2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным [законом](#).
- (в ред. Федерального закона от 02.07.2013 № 187-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

- В настоящем Федеральном законе используются следующие основные понятия:
- 1) информация - сведения (сообщения, данные) независимо от формы их представления;
 - 2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
 - 3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
 - 4) информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
 - 5) обладатель информации - лицо, самостоятельно создавшее информацию либо

получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

(п. 11.1 введен Федеральным законом от 27.07.2010 N 227-ФЗ)

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";

(п. 13 введен Федеральным законом от 28.07.2012 N 139-ФЗ, в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

14) страница сайта в сети "Интернет" (далее также - интернет-страница) - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет";

(п. 14 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

15) доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";

(п. 15 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

16) сетевой адрес - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

(п. 16 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

17) владелец сайта в сети "Интернет" - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте;

(п. 17 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

18) провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет";

(п. 18 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

19) единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

(п. 19 введен Федеральным законом от 07.06.2013 N 112-ФЗ)

20) поисковая система - информационная система, осуществляющая по запросу пользователя поиск в сети "Интернет" информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети "Интернет" для доступа к запрашиваемой информации, расположенной на сайтах в сети "Интернет", принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

(п. 20 введен Федеральным законом от 13.07.2015 N 264-ФЗ)

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- 2) установление ограничений доступа к информации только федеральными законами;
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения

доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- 1) информацию, свободно распространяемую;
 - 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
 - 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
 - 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.
4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования полномочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

- 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
- 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
- 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

- 1) соблюдать права и законные интересы иных лиц;
- 2) принимать меры по защите информации;
- 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

4. Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в

форме открытых данных.

(часть 4 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

5. Информация в форме открытых данных размещается в сети "Интернет" с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

(часть 5 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

6. В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

(часть 6 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее - организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

(в ред. Федерального закона от 27.07.2010 N 227-ФЗ)

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

КонсультантПлюс: примечание.

По вопросу, касающемуся порядка обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, см. Постановление Правительства РФ от 03.11.1994 N 1233.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица. Владелец сайта в сети "Интернет" обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления, указанного в [статье 15.7](#) настоящего Федерального закона, а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте в сети "Интернет".

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 10.1. Обязанности организатора распространения информации в сети "Интернет" (введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. Организатором распространения информации в сети "Интернет" является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет".

2. Организатор распространения информации в сети "Интернет" обязан в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности, указанной в [части 1](#) настоящей статьи.

3. Организатор распространения информации в сети "Интернет" обязан хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети "Интернет" и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, а также предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

4. Организатор распространения информации в сети "Интернет" обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия

организационных и тактических приемов проведения данных мероприятий. Порядок взаимодействия организаторов распространения информации в сети "Интернет" с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации.

5. Обязанности, предусмотренные настоящей статьей, не распространяются на операторов государственных информационных систем, операторов муниципальных информационных систем, операторов связи, оказывающих услуги связи на основании соответствующей лицензии, в части лицензируемой деятельности, а также не распространяются на граждан (физических лиц), осуществляющих указанную в [части 1](#) настоящей статьи деятельность для личных, семейных и домашних нужд. Правительством Российской Федерации в целях применения положений настоящей статьи определяется перечень личных, семейных и домашних нужд при осуществлении деятельности, указанной в [части 1](#) настоящей статьи.

6. Состав информации, подлежащей хранению в соответствии с [частью 3](#) настоящей статьи, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, а также порядок осуществления контроля за деятельностью организаторов распространения информации в сети "Интернет", связанной с хранением такой информации, и федеральный орган исполнительной власти, уполномоченный на осуществление этого контроля, определяются Правительством Российской Федерации.

Статья 10.2. Особенности распространения блогером общедоступной информации (введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. Владелец сайта и (или) страницы сайта в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет" (далее - блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данном сайте или странице сайта иными пользователями сети "Интернет", обязан обеспечивать соблюдение законодательства Российской Федерации, в частности:

1) не допускать использование сайта или страницы сайта в сети "Интернет" в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;

3) не допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства;

4) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

5) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

6) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

2. При размещении информации на сайте или странице сайта в сети "Интернет" не допускается:

1) использование сайта или страницы сайта в сети "Интернет" в целях сокрытия или фальсификации общественно значимых сведений, распространения заведомо недостоверной информации под видом достоверных сообщений;

2) распространение информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности,

языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

3. Блогер имеет право:

1) свободно искать, получать, передавать и распространять информацию любым способом в соответствии с законодательством Российской Федерации;

2) излагать на своих сайте или странице сайта в сети "Интернет" свои личные суждения и оценки с указанием своего имени или псевдонима;

3) размещать или допускать размещение на своих сайте или странице сайта в сети "Интернет" текстов и (или) иных материалов других пользователей сети "Интернет", если размещение таких текстов и (или) иных материалов не противоречит законодательству Российской Федерации;

4) распространять на возмездной основе рекламу в соответствии с гражданским законодательством, Федеральным законом от 13 марта 2006 года N 38-ФЗ "О рекламе" на своих сайте или странице сайта в сети "Интернет".

4. Злоупотребление правом на распространение общедоступной информации, выразившееся в нарушении требований [частей 1, 2 и 3](#) настоящей статьи, влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

5. Блогер обязан разместить на своих сайте или странице сайта в сети "Интернет" свои фамилию и инициалы, электронный адрес для направления ему юридически значимых сообщений.

6. Блогер обязан разместить на своих сайте или странице сайта в сети "Интернет" незамедлительно при получении решение суда, вступившее в законную силу и содержащее требование о его опубликовании на данных сайте или странице сайта.

7. Владельцы сайтов в сети "Интернет", которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года N 2124-1 "О средствах массовой информации" в качестве сетевых изданий, не являются блогерами.

8. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет". В целях обеспечения формирования реестра сайтов и (или) страниц сайтов в сети "Интернет" федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг сайтов и страниц сайтов в сети "Интернет";

2) утверждает методику определения количества пользователей сайта или страницы сайта в сети "Интернет" в сутки;

3) вправе запрашивать у организаторов распространения информации в сети "Интернет", блогеров и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", сайтов или страниц сайтов, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", включая рассмотрение соответствующих обращений граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) включает указанные сайт или страницу сайта в сети "Интернет" в реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет";

2) определяет провайдера хостинга или иное обеспечивающее размещение сайта или

страницы сайта в сети "Интернет" лицо;

3) направляет провайдеру хостинга или указанному в [пункте 2](#) настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать блогера;

4) фиксирует дату и время направления уведомления провайдеру хостинга или указанному в [пункте 2](#) настоящей части лицу в соответствующей информационной системе.

10. В течение трех рабочих дней с момента получения уведомления, указанного в [пункте 3 части 9](#) настоящей статьи, провайдер хостинга или указанное в [пункте 2 части 9](#) настоящей статьи лицо обязаны предоставить данные, позволяющие идентифицировать блогера.

11. После получения данных, указанных в [пункте 3 части 9](#) настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет блогеру уведомление о включении его сайта или страницы сайта в реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", с указанием требований законодательства Российской Федерации, применимых к данному сайту или странице сайта в сети "Интернет".

12. В случае, если доступ к сайту или странице сайта в сети "Интернет" на протяжении трех месяцев составляет в течение суток менее трех тысяч пользователей сети "Интернет", данный сайт или данная страница сайта в сети "Интернет" по заявлению блогера исключается из реестра сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", о чем блогеру направляется соответствующее уведомление. Данные сайт или страница сайта в сети "Интернет" могут быть исключены из этого реестра при отсутствии заявления блогера, если доступ к данным сайту или странице сайта в сети "Интернет" на протяжении шести месяцев составляет в течение суток менее трех тысяч пользователей сети "Интернет".

Статья 10.3. Обязанности оператора поисковой системы (введена Федеральным законом от 13.07.2015 N 264-ФЗ)

1. Оператор поисковой системы, распространяющий в сети "Интернет" рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, по требованию гражданина (физического лица) (далее в настоящей статье - заявитель) обязан прекратить выдачу сведений об указателе страницы сайта в сети "Интернет" (далее также - ссылка), позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя, за исключением информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость.

2. Требование заявителя должно содержать:

1) фамилию, имя, отчество, паспортные данные, контактную информацию (номера телефона и (или) факса, адрес электронной почты, почтовый адрес);

2) информацию о заявителе, указанную в [части 1](#) настоящей статьи, выдача ссылок на которую подлежит прекращению;

3) указатель страницы сайта в сети "Интернет", на которой размещена информация, указанная в [части 1](#) настоящей статьи;

4) основание для прекращения выдачи ссылок поисковой системой;

5) согласие заявителя на обработку его персональных данных.

3. В случае обнаружения неполноты сведений, неточностей или ошибок в требовании заявителя оператор поисковой системы вправе направить заявителю в течение десяти рабочих дней с момента получения указанного требования уведомление об уточнении представленных сведений. Оператор поисковой системы также вправе направить заявителю уведомление о

необходимости предоставления документа, удостоверяющего личность. Указанное уведомление может быть направлено заявителю однократно.

4. В течение десяти рабочих дней с момента получения уведомления, указанного в [части 3](#) настоящей статьи, заявитель принимает меры, направленные на восполнение недостающих сведений, устранение неточностей и ошибок, и направляет оператору поисковой системы уточненные сведения, а также документ, удостоверяющий личность (в случае необходимости).

5. В течение десяти рабочих дней с момента получения требования заявителя или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в [части 3](#) настоящей статьи) оператор поисковой системы обязан прекратить выдачу ссылок на информацию, указанную в требовании заявителя, при показе результатов поиска по запросам пользователей поисковой системы, содержащих имя и (или) фамилию заявителя, уведомить об этом заявителя или направить заявителю мотивированный отказ.

6. Оператор поисковой системы направляет заявителю уведомление об удовлетворении указанного в [части 1](#) настоящей статьи требования заявителя или мотивированный отказ в его удовлетворении в той же форме, в которой было получено указанное требование.

7. Заявитель, считающий отказ оператора поисковой системы необоснованным, вправе обратиться в суд с исковым заявлением о прекращении выдачи ссылок на информацию, указанную в требовании заявителя.

8. Оператор поисковой системы обязан не раскрывать информацию о факте обращения к нему заявителя с требованием, указанным в [части 1](#) настоящей статьи, за исключением случаев, установленных федеральными законами.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

3. Утратил силу. - Федеральный закон от 06.04.2011 N 65-ФЗ.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.
(в ред. Федерального закона от 06.04.2011 N 65-ФЗ)

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 11.1. Обмен информацией в форме электронных документов при осуществлении полномочий органов государственной власти и органов местного самоуправления
(введена Федеральным законом от 13.07.2015 N 263-ФЗ)

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные

публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулируемыми правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулируемыми правоотношения в установленной сфере деятельности.

3. Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи".

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным [законом](#);

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(п. 4 введен Федеральным законом от 21.07.2011 N 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных

(введена Федеральным законом от 29.06.2015 N 188-ФЗ)

1. В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый

реестр российских программ для электронных вычислительных машин и баз данных (далее - реестр российского программного обеспечения).

2. Правила формирования и ведения реестра российского программного обеспечения, состав сведений, включаемых в реестр российского программного обеспечения, в том числе об основаниях возникновения исключительного права у правообладателя (правообладателей), условия включения таких сведений в реестр российского программного обеспечения и исключения их из реестра российского программного обеспечения, порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливаются Правительством Российской Федерации.

3. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра российского программного обеспечения оператора реестра российского программного обеспечения - организацию, зарегистрированную на территории Российской Федерации.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти утверждает классификатор программ для электронных вычислительных машин и баз данных в целях ведения реестра российского программного обеспечения.

5. В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации и решения которой иностранное лицо не имеет возможности определять в силу особенностей отношений между таким иностранным лицом и российской некоммерческой организацией;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в [подпункте "б"](#) настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы для электронных вычислительных машин или базы данных либо права использования программы для электронных вычислительных машин или базы данных свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав на результаты интеллектуальной деятельности и средства индивидуализации, выполнение работ, оказание услуг в связи с разработкой, адаптацией и модификацией программы для электронных вычислительных машин или базы данных и для разработки, адаптации и модификации программы для электронных вычислительных машин или базы данных, в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российскими коммерческими организациями и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин или базы данных от реализации программы для электронных вычислительных машин или базы данных, включая предоставление прав использования, независимо от вида договора за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не

составляют государственную тайну, и программа для электронных вычислительных машин или база данных не содержит сведений, составляющих государственную тайну.

6. Правительством Российской Федерации могут быть установлены дополнительные требования к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения.

7. Программы для электронных вычислительных машин и базы данных, сведения о которых включены в реестр российского программного обеспечения, признаются происходящими из Российской Федерации.

8. Для целей настоящей статьи доля участия одной организации в другой организации или гражданина Российской Федерации в организации определяется в соответствии с порядком, установленным главой 14.1 Налогового кодекса Российской Федерации.

9. Для целей настоящей статьи контролируемой иностранным лицом российской коммерческой организацией или российской некоммерческой организацией признается организация, решения которой иностранное лицо имеет возможность определять в силу преобладающего прямого и (или) косвенного участия в этой организации, участия в договоре (соглашении), предметом которого является управление этой организацией, или иных особенностей отношений между иностранным лицом и этой организацией и (или) иными лицами.

10. Решение об отказе во включении в реестр российского программного обеспечения программ для электронных вычислительных машин или баз данных может быть обжаловано правообладателем программы для электронных вычислительных машин или базы данных в суд в течение трех месяцев со дня получения такого решения.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети "Интернет" в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

2.1. Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

(часть 2.1 введена Федеральным законом от 31.12.2014 N 531-ФЗ)

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными

правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

7. Порядок осуществления контроля за соблюдением требований, предусмотренных [частью 2.1](#) настоящей статьи и [частью 6 статьи 14](#) настоящего Федерального закона, устанавливается Правительством Российской Федерации.
(часть 7 введена Федеральным законом от 31.12.2014 N 531-ФЗ)

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд.

(часть 2 в ред. Федерального закона от 28.12.2013 N 396-ФЗ)

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 года N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", государственные информационные системы должны обеспечивать размещение такой информации в сети "Интернет" в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

4.1. Правительство Российской Федерации определяет случаи, при которых доступ с использованием сети "Интернет" к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

(часть 4.1 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

6. Правительство Российской Федерации утверждает требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, дальнейшего хранения содержащейся в их базах данных информации, включающие в себя перечень, содержание и сроки реализации этапов мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, дальнейшему хранению содержащейся в их базах данных информации.

(часть 6 в ред. Федерального закона от 31.12.2014 N 531-ФЗ)

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

(в ред. Федерального закона от 27.07.2010 N 227-ФЗ)

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет"

и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено (введена Федеральным законом от 28.07.2012 N 139-ФЗ)

1. В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (далее - реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра оператора реестра - организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в [части 2 настоящей статьи](#), являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами; (пп. "г" введен Федеральным законом от 05.04.2013 N 50-ФЗ)

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи;

(пп. "д" введен Федеральным законом от 21.07.2014 N 222-ФЗ)

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено.

6. Решение о включении в реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено,

может быть обжаловано владельцем сайта в сети "Интернет", провайдером хостинга, оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", в суд в течение трех месяцев со дня принятия такого решения.

7. В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети "Интернет" и уведомить его о необходимости незамедлительного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

8. В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр владелец сайта в сети "Интернет" обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети "Интернет" провайдер хостинга обязан ограничить доступ к такому сайту в сети "Интернет" в течение суток.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети "Интернет" мер, указанных в [частях 7 и 8 настоящей статьи](#), сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому сайту в сети "Интернет".

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с [частью 4 настоящей статьи](#) оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети "Интернет" или сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", на основании обращения владельца сайта в сети "Интернет", провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".

12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

13. Порядок ограничения доступа к сайтам в сети "Интернет", предусмотренный настоящей статьей, не применяется к информации, порядок ограничения доступа к которой предусмотрен [статьей 15.3](#) настоящего Федерального закона.

(часть 13 введена Федеральным законом от 28.12.2013 N 398-ФЗ)

Статья 15.2. Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

(введена Федеральным законом от 02.07.2013 N 187-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

2) направляет провайдеру хостинга или иному указанному в [пункте 1](#) настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по ограничению доступа к такой информации;

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в [пункте 1](#) настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в [пункте 2 части 2](#) настоящей статьи, провайдер хостинга или иное указанное в [пункте 1 части 2](#) настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно ограничить доступ к незаконно размещенной информации.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в [пункте 1 части 2](#) настоящей статьи лица уведомления о необходимости ограничить доступ к незаконно размещенной информации владелец информационного ресурса обязан удалить незаконно размещенную информацию или принять меры по ограничению доступа к ней. В случае отказа или бездействия владельца информационного

ресурса провайдер хостинга или иное указанное в [пункте 1 части 2](#) настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в [пункте 2 части 2](#) настоящей статьи.

(часть 4 в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

5. В случае непринятия провайдером хостинга или иным указанным в [пункте 1 части 2](#) настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в [частях 3 и 4](#) настоящей статьи, доменное имя сайта в сети "Интернет", его сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать информацию, содержащую объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети "Интернет", или к размещенной на нем информации.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в [пункте 1 части 2](#) настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу. В течение одного рабочего дня со дня получения от указанного федерального органа исполнительной власти уведомления об отмене мер по ограничению доступа к информационному ресурсу провайдер хостинга обязан проинформировать об этом владельца информационного ресурса и уведомить о возможности снятия ограничения доступа.

(в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые используются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к незаконно размещенной информации в соответствии с вступившим в законную силу судебным актом. В случае отсутствия у оператора связи технической возможности ограничить доступ к незаконно размещенной информации оператор связи обязан ограничить доступ к такому информационному ресурсу.

(часть 7 в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со [статьей 15.1](#) настоящего Федерального закона.

Статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона
(введена Федеральным законом от 28.12.2013 N 398-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в [части 1](#) настоящей статьи, незамедлительно:

1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети "Интернет", или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка. Данное требование должно содержать доменное имя сайта в сети "Интернет", сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать такую информацию;

2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;

3) направляет провайдеру хостинга или иному указанному в [пункте 2](#) настоящей части лицу уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в [пункте 2](#) настоящей части лицу в соответствующей информационной системе.

3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети "Интернет", или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

4. В течение суток с момента получения уведомления, указанного в [пункте 3 части 2](#) настоящей статьи, провайдер хостинга или иное указанное в [пункте 2 части 2](#) настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить информацию,

содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

5. В случае, если владелец информационного ресурса удалил информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

6. После получения уведомления, указанного в [части 5](#) настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети "Интернет".

7. После получения уведомления, указанного в [части 6](#) настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети "Интернет".

Статья 15.4. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети "Интернет"

(введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. В случае установленного вступившим в законную силу постановлением по делу об административном правонарушении неисполнения организатором распространения информации в сети "Интернет" обязанностей, предусмотренных [статьей 10.1](#) настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

2. В случае неисполнения организатором распространения информации в сети "Интернет" в указанный в уведомлении срок обязанностей, предусмотренных [статьей 10.1](#) настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет" и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети "Интернет", на основании вступившего в законную силу решения суда или решения уполномоченного федерального органа исполнительной власти.

3. Порядок взаимодействия уполномоченного федерального органа исполнительной власти с организатором распространения информации в сети "Интернет", порядок направления указанного в [части 1](#) настоящей статьи уведомления, порядок ограничения и возобновления доступа к указанным в [части 2](#) настоящей статьи информационным системам и (или) программам и порядок информирования граждан (физических лиц) о таком ограничении устанавливаются Правительством Российской Федерации.

Статья 15.5. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных

(введена Федеральным законом от 21.07.2014 N 242-ФЗ)

1. В целях ограничения доступа к информации в сети "Интернет", обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система "Реестр нарушителей прав субъектов

персональных данных" (далее - реестр нарушителей).

2. В реестр нарушителей включаются:

1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

3) указание на вступивший в законную силу судебный акт;

4) информация об устранении нарушения законодательства Российской Федерации в области персональных данных;

5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

3. Создание, формирование и ведение реестра нарушителей осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с критериями, определенными Правительством Российской Федерации, может привлечь к формированию и ведению реестра нарушителей оператора такого реестра - организацию, зарегистрированную на территории Российской Федерации.

5. Основанием для включения в реестр нарушителей информации, указанной в части 2 настоящей статьи, является вступивший в законную силу судебный акт.

6. Субъект персональных данных вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, на основании вступившего в законную силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

7. В течение трех рабочих дней со дня получения вступившего в законную силу судебного акта федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании указанного решения суда:

1) определяет провайдера хостинга или иное лицо, обеспечивающее обработку информации в информационно-телекоммуникационной сети, в том числе в сети "Интернет", с нарушением законодательства Российской Федерации в области персональных данных;

2) направляет провайдеру хостинга или иному указанному в [пункте 1](#) настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении законодательства Российской Федерации в области персональных данных с информацией о вступившем в законную силу судебном акте, доменном имени и сетевом адресе, позволяющих идентифицировать сайт в сети "Интернет", на котором осуществляется обработка информации с нарушением законодательства Российской Федерации в области персональных данных, а также об указателях страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанные в решении суда;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в [пункте 1](#) настоящей части лицу в реестре нарушителей.

8. В течение одного рабочего дня с момента получения уведомления, указанного в [пункте 2 части 7](#) настоящей статьи, провайдер хостинга или иное указанное в [пункте 1 части 7](#) настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно принять меры

по устранению нарушения законодательства Российской Федерации в области персональных данных, указанного в уведомлении, или принять меры по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

9. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в [пункте 1 части 7](#) настоящей статьи лица уведомления о необходимости устранения нарушения законодательства Российской Федерации в области персональных данных владелец информационного ресурса обязан принять меры по устранению указанного в уведомлении нарушения. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в [пункте 1 части 7](#) настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в [пункте 2 части 7](#) настоящей статьи.

10. В случае непринятия провайдером хостинга или иным указанным в [пункте 1 части 7](#) настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в [частях 8 и 9](#) настоящей статьи, доменное имя сайта в сети "Интернет", его сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных, а также иные сведения об этом сайте и информация направляются по автоматизированной информационной системе операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сетевому адресу, доменному имени, указателю страниц сайта в сети "Интернет".

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с [частью 4](#) настоящей статьи оператор реестра нарушителей исключает из такого реестра доменное имя, указатель страницы сайта в сети "Интернет" или сетевой адрес, позволяющие идентифицировать сайт в сети "Интернет", на основании обращения владельца сайта в сети "Интернет", провайдера хостинга или оператора связи не позднее чем в течение трех дней со дня такого обращения после принятия мер по устранению нарушения законодательства Российской Федерации в области персональных данных или на основании вступившего в законную силу решения суда об отмене ранее принятого судебного акта.

12. Порядок взаимодействия оператора реестра нарушителей с провайдером хостинга и порядок получения доступа к содержащейся в таком реестре информации оператором связи устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Статья 15.6. Порядок ограничения доступа к сайтам в сети "Интернет", на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет"

(введена Федеральным законом от 24.11.2014 N 364-ФЗ)

1. В течение суток с момента поступления по системе взаимодействия в адрес федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вступившего в законную силу соответствующего решения Московского городского суда указанный орган направляет операторам связи по системе взаимодействия требование о принятии мер по постоянному ограничению доступа к сайту в сети "Интернет", на котором неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет".

2. В течение суток с момента получения указанного в [части 1](#) настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к

соответствующему сайту в сети "Интернет". Снятие ограничения доступа к такому сайту в сети "Интернет" не допускается.

3. Сведения о сайтах в сети "Интернет", доступ к которым ограничен на основании решения Московского городского суда, размещаются на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в информационно-телекоммуникационной сети "Интернет".

Статья 15.7. Внесудебные меры по прекращению нарушения авторских и (или) смежных прав в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", принимаемые по заявлению правообладателя

(введена Федеральным законом от 24.11.2014 N 364-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", сайта в сети "Интернет", на котором без его разрешения или иного законного основания размещена информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", вправе направить владельцу сайта в сети "Интернет" в письменной или электронной форме заявление о нарушении авторских и (или) смежных прав (далее - заявление). Заявление может быть направлено лицом, уполномоченным правообладателем в соответствии с законодательством Российской Федерации.

2. Заявление должно содержать:

1) сведения о правообладателе или лице, уполномоченном правообладателем (если заявление направляется таким лицом) (далее - заявитель):

а) для физического лица - фамилию, имя, отчество, паспортные данные (серия и номер, кем выдан, дата выдачи), контактную информацию (номера телефона и (или) факса, адрес электронной почты);

б) для юридического лица - наименование, место нахождения и адрес, контактную информацию (номера телефона и (или) факса, адрес электронной почты);

2) информацию об объекте авторских и (или) смежных прав, размещенном на сайте в сети "Интернет" без разрешения правообладателя или иного законного основания;

3) указание на доменное имя и (или) сетевой адрес сайта в сети "Интернет", на котором без разрешения правообладателя или иного законного основания размещена информация, содержащая объект авторских и (или) смежных прав, или информация, необходимая для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет";

4) указание на наличие у правообладателя прав на объект авторских и (или) смежных прав, размещенный на сайте в сети "Интернет" без разрешения правообладателя или иного законного основания;

5) указание на отсутствие разрешения правообладателя на размещение на сайте в сети "Интернет" информации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет";

б) согласие заявителя на обработку его персональных данных (для заявителя - физического лица).

3. В случае, если заявление подается уполномоченным лицом, к заявлению прикладывается копия документа (в письменной или электронной форме), подтверждающего его полномочия.

4. В случае обнаружения неполноты сведений, неточностей или ошибок в заявлении владелец сайта в сети "Интернет" вправе направить заявителю в течение двадцати четырех часов с момента получения заявления уведомление об уточнении представленных сведений. Указанное уведомление может быть направлено заявителю однократно.

5. В течение двадцати четырех часов с момента получения уведомления, указанного в [части 4](#) настоящей статьи, заявитель принимает меры, направленные на восполнение

недостающих сведений, устранение неточностей и ошибок, и направляет владельцу сайта в сети "Интернет" уточненные сведения.

6. В течение двадцати четырех часов с момента получения заявления или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в [части 4](#) настоящей статьи) владелец сайта в сети "Интернет" удаляет указанную в [части 1](#) настоящей статьи информацию.

7. При наличии у владельца сайта в сети "Интернет" доказательств, подтверждающих правомерность размещения на принадлежащем ему сайте в сети "Интернет" информации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", владелец сайта в сети "Интернет" вправе не принимать предусмотренные [частью 6](#) настоящей статьи меры и обязан направить заявителю соответствующее уведомление с приложением указанных доказательств.

8. Правила настоящей статьи в равной степени распространяются на правообладателя и на лицензиата, получившего исключительную лицензию на объект авторских и (или) смежных прав.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в [пунктах 1 и 3](#) части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(п. 7 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее

защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

4. Провайдер хостинга, оператор связи и владелец сайта в сети "Интернет" не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

(часть 4 введена Федеральным законом от 02.07.2013 N 187-ФЗ; в ред. Федерального закона от 24.11.2014 N 364-ФЗ)

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации" (Собрание законодательства Российской Федерации, 1995, N 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года N 85-ФЗ "Об участии в международном информационном обмене" (Собрание законодательства Российской Федерации, 1996, N 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года N 15-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2003, N 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года N 86-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2003, N 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года N 58-ФЗ "О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2004, N 27, ст. 2711).

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль
27 июля 2006 года
N 149-ФЗ



КонсультантПлюс
надежная правовая поддержка

Федеральный закон от 27.07.2006 N 152-
ФЗ
(ред. от 21.07.2014)
"О персональных данных"
(с изм. и доп., вступ. в силу с 01.09.2015)

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О ПЕРСОНАЛЬНЫХ ДАННЫХ

Принят
Государственной Думой
8 июля 2006 года

Одобен
Советом Федерации
14 июля 2006 года

Список изменяющих документов
(в ред. Федеральных законов от 25.11.2009 № 266-ФЗ,
от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ,
от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ,
от 29.11.2010 № 313-ФЗ от 23.12.2010 № 359-ФЗ,
от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ,
от 05.04.2013 № 43-ФЗ, от 23.07.2013 № 205-ФЗ,
от 21.12.2013 № 363-ФЗ, от 04.06.2014 № 142-ФЗ,
от 21.07.2014 № 216-ФЗ, от 21.07.2014 № 242-ФЗ)

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

(часть 1 в ред. Федерального закона от 25.07.2011 № 261-ФЗ)

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

- 1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- 2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- 3) утратил силу. - Федеральный закон от 25.07.2011 № 261-ФЗ;
- 4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- 5) предоставлении уполномоченными органами информации о деятельности судов в

Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".
(п. 5 введен Федеральным законом от 28.06.2010 N 123-ФЗ)

Статья 2. Цель настоящего Федерального закона

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Статья 4. Законодательство Российской Федерации в области персональных данных

1. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской

Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

(часть 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

Глава 2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 5. Принципы обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Статья 6. Условия обработки персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и

правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

(в ред. Федерального закона от 05.04.2013 N 43-ФЗ)

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

(п. 5 в ред. Федерального закона от 21.12.2013 N 363-ФЗ)

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в [статье 15](#) настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно [статьями 10](#) и [11](#) настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее

обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со [статьей 19](#) настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Статья 7. Конфиденциальность персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 8. Общедоступные источники персональных данных

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку

персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в [пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11](#) настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в [пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11](#) настоящего Федерального закона, возлагается на оператора.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в [пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11](#) настоящего Федерального закона.

Статья 10. Специальные категории персональных данных

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных [частью 2](#) настоящей статьи.

2. Обработка указанных в [части 1](#) настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;
(п. 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
(п. 2.1 введен Федеральным законом от 25.11.2009 N 266-ФЗ)

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";
(п. 2.2 введен Федеральным законом от 27.07.2010 N 204-ФЗ)

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
(п. 2.3 введен Федеральным законом от 25.07.2011 N 261-ФЗ, в ред. Федерального закона от 21.07.2014 N 216-ФЗ)

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
(п. 3 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
(п. 6 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
(п. 7.1 введен Федеральным законом от 23.07.2013 N 205-ФЗ)

8) обработка персональных данных осуществляется в соответствии с законодательством

об обязательных видах страхования, со страховым законодательством;

(п. 8 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

(п. 10 введен Федеральным законом от 04.06.2014 N 142-ФЗ)

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных [частями 2 и 3](#) настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 11. Биометрические персональные данные

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных [частью 2](#) настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

(в ред. Федерального закона от 04.06.2014 N 142-ФЗ)

Статья 12. Трансграничная передача персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает

перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Глава 3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 14. Право субъекта персональных данных на доступ к его персональным данным

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных имеет право на получение сведений, указанных в [части 7](#) настоящей статьи, за исключением случаев, предусмотренных [частью 8](#) настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в [части 7](#) настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

3. Сведения, указанные в [части 7](#) настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в [части 7](#) настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в [части 7](#) настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в [части 7](#) настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в [части 4](#) настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в [части 3](#) настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [частями 4 и 5](#) настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств

обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- 1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- 2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
- 3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- 4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- 5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта

персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в [части 1](#) настоящей статьи.

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных [частью 2](#) настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в [части 3](#) настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 17. Право на обжалование действий или бездействия оператора

1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Глава 4. ОБЯЗАННОСТИ ОПЕРАТОРА

Статья 18. Обязанности оператора при сборе персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную [частью 7 статьи 14](#) настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных [частью 4](#) настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные настоящим Федеральным законом права субъекта персональных данных;

- 5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные [частью 3](#) настоящей статьи, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

- 2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

- 4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

- 5) предоставление субъекту персональных данных сведений, предусмотренных [частью 3](#) настоящей статьи, нарушает права и законные интересы третьих лиц.

5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в [пунктах 2, 3, 4, 8 части 1 статьи 6](#) настоящего Федерального закона.

(часть 5 введена Федеральным законом от 21.07.2014 N 242-ФЗ)

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

(введена Федеральным законом от 25.07.2011 N 261-ФЗ)

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

- 1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

- 2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со [статьей 19](#) настоящего Федерального закона;

- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике

оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в [части 1](#) настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в [части 1](#) настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных

вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с [частью 3](#) настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с [частью 5](#) настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в [части 5](#) настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в [части 6](#) настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в [части 6](#) настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Оператор обязан сообщить в порядке, предусмотренном [статьей 14](#) настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение [части 8 статьи 14](#) настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных

данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и принятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки

персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в [частях 3 - 5](#) настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Статья 22. Уведомление об обработке персональных данных

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных [частью 2](#) настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;
(п. 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) сделанных субъектом персональных данных общедоступными;

(п. 4 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

3. Уведомление, предусмотренное [частью 1](#) настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных [статьями 18.1 и 19](#) настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

(п. 7.1 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

(п. 10 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

(п. 10.1 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

(п. 11 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

(часть 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

(введена Федеральным законом от 25.07.2011 N 261-ФЗ)

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Глава 5. КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

Статья 23. Уполномоченный орган по защите прав субъектов персональных данных

1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации;

(п. 3.1 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в [пункте 7 части 3 статьи 22](#) настоящего Федерального закона;

(п. 5.1 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих

полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

(часть 5.1 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

(часть 2 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

Глава 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 25. Заключительные положения

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

2. После дня вступления в силу настоящего Федерального закона обработка

персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в [пунктах 5, 7.1, 10 и 11 части 3 статьи 22](#) настоящего Федерального закона, не позднее 1 января 2013 года.

(часть 2.1 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

3. Утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ.

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 [статьи 22](#) настоящего Федерального закона, уведомление, предусмотренное частью 3 [статьи 22](#) настоящего Федерального закона, не позднее 1 января 2008 года.

5. Отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации - городе федерального значения Москве, регулируются настоящим Федеральным законом, если иное не предусмотрено Федеральным законом "Об особенностях регулирования отдельных правоотношений в связи с присоединением к субъекту Российской Федерации - городу федерального значения Москве территорий и о внесении изменений в отдельные законодательные акты Российской Федерации".

(часть 5 введена Федеральным законом от 05.04.2013 N 43-ФЗ)

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль
27 июля 2006 года
N 152-ФЗ



КонсультантПлюс
надежная правовая поддержка

Федеральный закон от 25.07.2011 N
261-ФЗ
"О внесении изменений в Федеральный
закон "О персональных данных"

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН
О ВНЕСЕНИИ ИЗМЕНЕНИЙ
В ФЕДЕРАЛЬНЫЙ ЗАКОН "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

Принят
Государственной Думой
5 июля 2011 года

Одобен
Советом Федерации
13 июля 2011 года

Статья 1

Внести в Федеральный закон от 27 июля 2006 года N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, 4196; N 49, ст. 6409; N 52, ст. 6974; 2011, N 23, ст. 3263) следующие изменения:

1) в статье 1:

а) часть 1 изложить в следующей редакции:

"1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.";

б) пункт 3 части 2 признать утратившим силу;

2) статью 3 изложить в следующей редакции:

"Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.";

3) часть 2 статьи 4 изложить в следующей редакции:

"2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.";

4) статью 5 изложить в следующей редакции:

"Статья 5. Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или

неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.";

5) статью 6 изложить в следующей редакции:

"Статья 6. Условия обработки персональных данных

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.";

6) статью 7 изложить в следующей редакции:

"Статья 7. Конфиденциальность персональных данных

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.";

7) в статье 8:

а) в части 1 слова "предоставленные субъектом персональных данных" заменить словами "сообщаемые субъектом персональных данных";

б) в части 2 слова "могут быть" заменить словами "должны быть";

8) статью 9 изложить в следующей редакции:

"Статья 9. Согласие субъекта персональных данных на обработку его персональных данных

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11

части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.";

9) в статье 10:

а) в части 2:

пункт 2 изложить в следующей редакции:

"2) персональные данные сделаны общедоступными субъектом персональных данных;"

дополнить пунктом 2.3 следующего содержания:

"2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством,

законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;"

пункт 3 изложить в следующей редакции:

"3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;"

пункт 6 изложить в следующей редакции:

"6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;"

пункт 7 изложить в следующей редакции:

"7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;"

пункт 8 изложить в следующей редакции:

"8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;"

дополнить пунктом 9 следующего содержания:

"9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан.";

б) часть 4 дополнить словами ", если иное не установлено федеральным законом";

10) статью 11 изложить в следующей редакции:

"Статья 11. Биометрические персональные данные

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.";

11) статью 12 изложить в следующей редакции:

"Статья 12. Трансграничная передача персональных данных

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в

целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.";

12) статью 14 изложить в следующей редакции:

"Статья 14. Право субъекта персональных данных на доступ к его персональным данным

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с

оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящей Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

- 1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- 2) обработка персональных данных осуществляется органами, осуществившими

задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.";

13) в части 4 статьи 16 слова "в течение семи рабочих дней" заменить словами "в течение тридцати дней";

14) статью 18 изложить в следующей редакции:

"Статья 18. Обязанности оператора при сборе персональных данных

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- 1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.";

15) дополнить статьей 18.1 следующего содержания:

"Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.";

16) статью 19 изложить в следующей редакции:

"Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России,

органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение

персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.";

17) статью 20 изложить в следующей редакции:

"Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.";

18) статью 21 изложить в следующей редакции:

"Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно

обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных.

данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.";

19) в статье 22:

а) в части 2:

пункт 1 изложить в следующей редакции:

"1) обрабатываемых в соответствии с трудовым законодательством;"

пункт 3 после слов "не будут распространяться" дополнить словами "или раскрываться третьим лицам";

пункт 4 изложить в следующей редакции:

"4) сделанных субъектом персональных данных общедоступными;"

в пункте 7 слова "федеральных автоматизированных информационных систем" заменить словами "государственных автоматизированных информационных систем";

дополнить пунктом 9 следующего содержания:

"9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.";

б) в части 3:

абзац первый изложить в следующей редакции:

"3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:"

пункт 7 изложить в следующей редакции:

"7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;"

дополнить пунктом 7.1 следующего содержания:

"7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;"

дополнить пунктами 10 и 11 следующего содержания:

"10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.";

в) часть 7 изложить в следующей редакции:

"7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.";

20) главу 4 дополнить статьей 22.1 следующего содержания:

"Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.";

21) в статье 23:

а) в части 3:

пункт 5 после слов "в защиту прав субъектов персональных данных" дополнить словами ", в том числе в защиту прав неопределенного круга лиц,";

дополнить пунктом 5.1 следующего содержания:

"5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 настоящего Федерального закона";

б) дополнить частью 5.1 следующего содержания:

"5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.";

22) в статье 24:

а) слово "Лица" заменить словами "1. Лица", слова "несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность" заменить словами "несут предусмотренную законодательством Российской Федерации ответственность";

б) дополнить частью 2 следующего содержания:

"2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.";

23) в статье 25:

а) дополнить частью 2.1 следующего содержания:

"2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 настоящего

Федерального закона, не позднее 1 января 2013 года.";

б) часть 3 признать утратившей силу.

Статья 2

Признать утратившими силу:

1) пункт 2 статьи 1 Федерального закона от 27 декабря 2009 года N 363-ФЗ "О внесении изменений в статьи 19 и 25 Федерального закона "О персональных данных" (Собрание законодательства Российской Федерации, 2009, N 52, ст. 6439);

2) Федеральный закон от 23 декабря 2010 года N 359-ФЗ "О внесении изменения в статью 25 Федерального закона "О персональных данных" (Собрание законодательства Российской Федерации, 2010, N 52, ст. 6974).

Статья 3

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Действие положений Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" (в редакции настоящего Федерального закона) распространяется на правоотношения, возникшие с 1 июля 2011 года.

Президент
Российской Федерации
Д.МЕДВЕДЕВ

Москва, Кремль
25 июля 2011 года
N 261-ФЗ

Лекция 1

Правовые и организационные основы информационной безопасности

План лекции:

1. Правовые аспекты информационной безопасности
2. Ответственность за правонарушения в сфере защиты информации
3. Основные положения государственных стандартов по обеспечению безопасности информации
4. Организационные методы защиты информации в ФНС



Финансовый ущерб, наносимый киберпреступниками, растет день ото дня.

Согласно недавнему отчету компании НР, потери от действий киберпреступников в 2012 году, по сравнению с 2011 годом, увеличились в два с лишним раза

Угрозы информационной безопасности государства

- угрозы информационному обеспечению государственной политики
- угрозы развитию отечественной индустрии информации
- угрозы безопасности информационных и телекоммуникационных средств и систем

Государственная система защиты информации

представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Органы в Государственной системе защиты информации

- ▣ Межведомственная комиссия по защите государственной тайны
- ▣ Федеральная служба безопасности Российской Федерации и её территориальные органы
- ▣ Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
- ▣ Федеральные органы исполнительной власти, другие органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, ФСО, ФСБ, СВР, ГУСП, РАН, ЦБР и др.)
- ▣ Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации
- ▣ Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
- ▣ Научно-исследовательские организации по проблемам защиты информации
- ▣ Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации
- ▣ Предприятия, оказывающие услуги в области защиты информации
- ▣ Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации

Основные нормативно-правовые акты

- ▣ Конституция Российской Федерации
- ▣ Закон РФ "О безопасности" от 05.03.1992г. № 2446-1 (ред. от 28 декабря 2010 г. N 390-ФЗ)
- ▣ Закон РФ "О государственной тайне" от 21.07.1993г. №5485-1 (ред. от 08.11.2011 N 309-ФЗ)
- ▣ ФЗ РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006г. №149-ФЗ (ред. от 28.07.2012 N 139-ФЗ)
- ▣ ФЗ РФ "О коммерческой тайне" от 29 июля 2004 г. N 98-ФЗ (ред. от 11.07.2011 №200-ФЗ)
- ▣ ФЗ РФ "О персональных данных" от 27 июля 2006 г. N 152-ФЗ (ред. от 25.07.2011 №261-ФЗ)
- ▣ ФЗ "О техническом регулировании" от 27 декабря 2002 г. N 184-ФЗ (ред. от 03.12.2012 N 236-ФЗ)
- ▣ ФЗ РФ "Об обеспечении единства измерений" от 26 июня 2008 года № 102-ФЗ
- ▣ ФЗ РФ "Электронной цифровой подписи" от 10 января 2002 г. N 1-ФЗ
- ▣ ФЗ РФ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ
- ▣ ФЗ РФ "О связи" 7 июля 2003 г. N 126-ФЗ
- ▣ ФЗ "Об органах Федеральной Службы Безопасности в Российской Федерации" 03.04.95 №40-ФЗ (СЗ №15-95 г. ст.1269) от 07.02.2011 N 3-ФЗ
- ▣ ФЗ "О лицензировании отдельных видов деятельности" от 8 августа 2001 года, N 128-ФЗ (ред. от 04.03.2013 N 22-ФЗ)
- ▣ УП РФ "Вопросы Межведомственной комиссии по защите государственной тайны" от 6 октября 2004 г. № 1286 (ред. от 16.07.2012 N 1008)
- ▣ УП РФ "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" от 17 марта 2008 г. N 351
- ▣ УП РФ "Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. № 188 (ред. от 23.09.2005 N 1111)
- ▣ УП РФ "Вопросы Федеральной службы безопасности Российской Федерации" от 11 июля 2003 года №960
- ▣ УП РФ "Вопросы федеральной службы по техническому и экспортному контролю" от 16 августа 2004 г. № 1085 (с изменениями и дополнениями от 22 марта 2005 г. № 330; от 20 июля 2005 г. №846; от 30 ноября 2006 г. № 1321)
- ▣ Указ Президента РФ от 12.05.2009 N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»
- ▣ Постановления правительства Российской Федерации
- ▣ Государственные стандарты в области защиты информации
- ▣ Другие правовые акты федеральных органов власти в области защиты информации

Доктрина информационной безопасности РФ

- ▣ Утверждена приказом Президента РФ от 9 сентября 2000 г. N Пр-1895

Доктрина служит основой для:

- ▣ формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- ▣ подготовки предложений по совершенствованию правового, методического, научно - технического и организационного обеспечения информационной безопасности Российской Федерации;
- ▣ разработки целевых программ обеспечения информационной безопасности Российской Федерации.

От чего следует защищать информацию (ГОСТ Р 50922-2006 Защита информации. Основные термины и определения)

- ▣ Утечка (рассекречивание) информации - утрата информацией свойства секретности (конфиденциальности) в результате несанкционированного ознакомления с нею или несанкционированного документирования (снятия копий).
- ▣ Нарушение целостности информации - утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения.
- ▣ Модификация информации - изменение содержания или объема информации на ее носителях. Примечание: модификация: искажение (случайная), подделка (умышленная) и уничтожение.
- ▣ Уничтожение информации - случайное или умышленное стирание информации на ее носителях, в том числе хищение носителей и технических средств.
- ▣ Искажение информации - случайная несанкционированная модификация информации в результате внешних воздействий (помех), сбоев в работе аппаратуры или неумелых действий обслуживающего персонала.
- ▣ Подделка информации - умышленная несанкционированная модификация информации с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.
- ▣ Блокирование информации - утрата доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней для проведения операций по ознакомлению, документированию, модификации или уничтожению.

Основные гос. органы в системе защиты информации

- ▣ Федеральный закон "Об органах федеральной службы безопасности в Российской Федерации";
- ▣ Указ Президента Российской Федерации «Вопросы Федеральной службы по техническому и экспортному контролю»;
- ▣ Указ Президента Российской Федерации «Вопросы межведомственной комиссии по защите государственной тайны».

Основные организационно-технические мероприятия по защите государственной и служебной тайны

- ▣ лицензирование предприятий и организаций на право проведения работ и оказания услуг по защите информации;
- ▣ сертификация технических средств обработки информации и средств ее защиты;
- ▣ аттестация объектов информатизации.

Виды информации по категориям доступа (ст.5 ФЗ №149)

- ▣ Общедоступная информация
- ▣ Информация ограниченного доступа
 - сведения, отнесенные к государственной тайне
 - сведения конфиденциального характера

ст. 5 Закона РФ «О государственной тайне»

- ☐ Особой важности
- ☐ Совершенно Секретно
- ☐ Секретно

Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера»

- ☐ Персональные данные
- ☐ Тайна следствия и судопроизводства
- ☐ Служебная тайна
- ☐ Профессиональная тайна
- ☐ Коммерческая тайна
- ☐ Сведения о сущности изобретения

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
 - ☐ обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
 - ☐ соблюдение конфиденциальности информации ограниченного доступа;
 - ☐ реализацию права на доступ к информации.

Обладатель информации, оператор ИС обязаны обеспечить:

- ☐ предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- ☐ своевременное обнаружение фактов несанкционированного доступа к информации;
- ☐ предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- ☐ недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- ☐ возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- ☐ постоянный контроль за обеспечением уровня защищенности информации.

Статья 17. Ответственность за правонарушения в сфере информации, ИТ и защиты информации

Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Статья 17. Ответственность за правонарушения в сфере информации, ИТ и защиты информации

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

- ▣ либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;
- ▣ либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Виды ответственности:

- ▣ дисциплинарная (замечание; выговор; увольнение) Трудовой кодекс РФ, ст. 192 (ФЗ 2001 г. № 197-ФЗ)
- ▣ гражданская (возмещение причинённого ущерба) Гражданский кодекс РФ (ст. 15, 16) ФЗ «О защите прав потребителя» (ФЗ 1999 г. № 2-ФЗ)
- ▣ административная (предупреждение, административный штраф) КоАП (от 30.12.2001 г. №195-ФЗ) (ст.13.11-13.14) Трудовой кодекс РФ (от 30.12.2001 г. № 197-ФЗ) (ст. 57, 86, гл. 39 и др.) ФЗ «О защите прав потребителя»
- ▣ уголовная (штраф, лишение свободы) Уголовный кодекс РФ (от 13.06.1996 г. №63-ФЗ) (ст.138, 140, 183, 238, гл. 28 (ст. 272-274) и др.)

Наказание по Кодексу об Административных Правонарушениях		
№	Название статьи	Максимальное наказание
13.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	10.000 руб.
13.14	Разглашение информации с ограниченным доступом	5.000 руб.
13.12	Нарушение правил защиты информации	20.000 руб.+ конфискация + приостановление деятельности на срок до 90 суток
13.13	Незаконная деятельность в области защиты информации	20.000 руб.+ конфискация
5.27	Нарушение законодательства о труде и об охране труда	50.000 руб.+ приостановление деятельности на срок до 90 суток + дисквалификация должностного лица до 3-х лет
5.39	Отказ в предоставлении гражданину информации	1.000 руб.
19.4	Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль)	10.000 руб.
19.6	Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения	500 руб.
19.5	Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)	500.000 руб. +дисквалификация должностного лица до 3-х лет
19.7	Непредставление сведений (информации)	5.000 руб.
19.20	Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии)	20.000 руб. + приостановление деятельности на срок до 90 суток
20.25	Неуплата административного штрафа либо самовольное оставление места отбывания административного ареста	Двукратное увеличение штрафа
Наказание по Уголовному Кодексу		
№	Название статьи	Максимальное наказание
137	Нарушение неприкосновенности частной жизни	300.000 руб. + исправительные работы на срок до 240 часов + арест до 6-ти месяцев
140	Отказ в предоставлении гражданину информации	200.000 руб.+ лишение права занимать должность на срок до 5-ти лет

171	Незаконное предпринимательство	300.000 руб. + обязательные работы на срок до 1-го года + арест до 6-ти месяцев + лишение права занимать должность на срок до 5-ти лет
Наказание по Трудовому Кодексу		
237	Моральный вред, причиненный работнику неправомерными действиями или бездействием работодателя	Денежное вознаграждение по согласованию
195	Привлечение к дисциплинарной ответственности руководителя организации, руководителя структурного подразделения организации, их заместителей по требованию представительного органа работников	Увольнение
90	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	Увольнение + УК
81	Расторжение трудового договора по инициативе работодателя за разглашение охраняемой законом тайны	Увольнение

152-ФЗ «О персональных данных» (ред. №261-ФЗ)

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными и муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации

Статья 7. Конфиденциальность персональных данных

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. . Обеспечение безопасности персональных данных достигается, в частности:
 - 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
 - 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
 - 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
 - 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
 - 5) учетом машинных носителей персональных данных;
 - 6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
 - 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
 - 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Основные ГОСТы в области защиты информации:

- ▣ ГОСТ Р 50922-2006. Защита информации. Основные термины и определения
- ▣ ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
- ▣ ГОСТ 12.1.050-86 Методы измерения шума на рабочих местах (ред. от 31.05.2005)
- ▣ ГОСТ Р 50.1.053 - 2005 Информационные технологии, основные термины и определения в области технической защиты информации
- ▣ ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
- ▣ ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
- ▣ ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования
- ▣ ГОСТ Р 52069-2003. Защита информации. Система стандартов. Основные положения
- ▣ ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762-2008). Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения
- ▣ ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
- ▣ ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
- ▣ ГОСТ Р ИСО/МЭК ТО 13335-4-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ▣ ГОСТ Р ИСО/МЭК ТО 13335-5-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ▣ ГОСТ Р ИСО/МЭК 15408-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
- ▣ ГОСТ Р ИСО/МЭК ТО 15443-2011. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ.
- ▣ ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью
- ▣ ГОСТ Р ИСО/МЭК 18028-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности
- ▣ ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
- ▣ ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- ▣ ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
- ГОСТ Р ИСО/МЭК 27005-2009. Информационная технология. Методы и средства обеспечения безопасности.

- ▣ ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
- ▣ ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
- ▣ ГОСТ Р 52919-2008 Информационная технология. Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость. Комнаты и контейнеры данных
- ▣ ГОСТ Р ИСО/МЭК 18045-2008 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
- ▣ ГОСТ Р 54581-2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы
- ▣ ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
- ▣ ГОСТ Р ИСО/МЭК 18028-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности
- ▣ ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения:

Защита информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Виды защиты информации

Правовая защита информации: Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации; ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации: Защита информации с помощью ее криптографического преобразования.

Физическая защита информации: Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Нормативные документы ФНС:

- ▣ Концепция информационной безопасности Федеральной налоговой службы утверждена приказом Федеральной налоговой службы от 13 января 2012 г. № ММВ-7-4/6
- ▣ Приказ Федеральной налоговой службы от 11 февраля 2013 г. № ММВ-7-4/69 "Об утверждении Порядка подключения пользователей к федеральным информационным ресурсам и сервисам, сопровождаемым МИ ФНС России по ЦОД"
- ▣ Приказ ФНС России от 31.12.2009 N ММ-7-6/728 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в налоговых органах».

Концепция информационной безопасности ФНС

Определяет цели, задачи, методологические основы обеспечения безопасности информации в ФНС России, также определяет объекты защиты (защищаемые ИР), виды угроз, источники угроз, режим защиты ИР и т.д.

К защищаемым ИР ФНС России относятся:

ИР, содержащие информацию ограниченного доступа (распространения):

- ☐ государственная тайна (в соответствии с «Перечнем сведений, отнесенных к государственной тайне»);
 - ☐ конфиденциальная информация (конфиденциальные ИР);
- ИР, содержащие открытую информацию, которая подлежит защите

Конфиденциальные ИР:

- ☐ налоговые ИР;
- ☐ ИР персональных данных;
- ☐ служебные ИР;
- ☐ технологические ИР;
- ☐ ИР ключевых систем информационной инфраструктуры (КСИИ).

Основные методы противодействия угрозам ИБ (Приложение 5)

- ☐ Правовые методы
- ☐ Экономические методы
- ☐ Организационные методы
- ☐ Инженерно-технические методы
- ☐ Технические методы
- ☐ Программно-аппаратные методы

Концепция информационной безопасности ФНС: организационные методы защиты информации

- ☐ выбор местоположения и размещения объекта информатизации;
- ☐ физическая защита и организация охраны;
- ☐ ограничение доступа в помещения, в которых установлены технические средства обработки информации;
- ☐ подбор и работа с персоналом;
- ☐ организация инструктажа персонала;
- ☐ организация учета оборудования и носителей;
- ☐ контроль выполнения требований по защите;
- ☐ противопожарная охрана;
- ☐ обеспечение надежного сервисного обслуживания;
- ☐ организация взаимодействия с компетентными органами.

Приказ ФНС от 11 февраля 2013 г. № ММВ-7-4/69

Настоящий порядок регламентирует работы по предоставлению услуги удаленного доступа к ФИР и сервисам, а также администрированию учетных записей (в том числе технологических).

Порядок подготовки, учета, использования, передачи, хранения и уничтожения документов, сопровождающих предоставление услуги и формируемых на основе ФИР

- ▣ Администрирование пользователей осуществляется распределённо
- ▣ Предоставление услуги удаленного доступа пользователю и администрирование учетных записей пользователей (в т.ч. ПК ВАИ) выполняются в веб-интерфейсе программного обеспечения федерального уровня АИС «ФЦОД».

Услуга сотруднику налогового органа или подведомственной организации может быть предоставлена только при выполнении всех необходимых требований по защите информации и наличии комплекта документов, а именно должностного регламента сотрудника, заявки на предоставление доступа. Ответственность за проверку выполнения указанных требований возлагается непосредственно на начальника отдела информационной безопасности налогового органа.

Ответственный сотрудник отдела информационной безопасности:

- ▣ проверяет соответствие рабочих мест требованиям Приложения N 7 к настоящему Порядку;
- ▣ заполняет «Журнал регистрации администраторов (пользователей) услуги удаленного доступа к информационным ресурсам и сервисам, сопровождаемым МИ ФНС России по ЦОД».

На основании выполненных работ по установке, настройке и подключению рабочих мест оформляется акт подготовки автоматизированного рабочего места к работе с услугой удаленного доступа к федеральным информационным ресурсам и сервисам (далее — Акт, Приложение N 9 к настоящему Порядку), который хранится в отделе информационной безопасности налогового органа.

Отделом информационной безопасности проводится инструктаж пользователей под роспись в «Журнале учета инструктажей пользователей услуги удаленного доступа к федеральным информационным ресурсам и сервисам, сопровождаемым МИ ФНС России по ЦОД» (Приложение N 8).

Контроль использования услуги осуществляется отделом информационной безопасности согласно Приложению N 12 к настоящему Порядку в рамках установленных организационных мер с применением программных средств подсистемы удаленного доступа.

Приложение N 7 Требования по защите от несанкционированного доступа

1. Обеспечить размещение автоматизированного рабочего места пользователя (далее — АРМ) в отдельном выделенном сегменте сети, свободный доступ в который из других подсетей налогового органа запрещается. В случае отсутствия сегментации сети в налоговом органе доступ к ФИР осуществляется с выделенных для этого АРМ;
2. Обеспечить невозможность выхода в сети общего пользования (ИНТЕРНЕТ) с АРМ;
3. Обеспечить отсутствие доступа с АРМ к любым почтовым сервисам;
4. Обеспечить идентификацию пользователей на АРМ при помощи аппаратного ключа и пароля (двухфакторная аутентификация);
5. Обеспечить очистку файла виртуальной памяти при перезагрузке АРМ или его выключении;
6. Обеспечить антивирусную защиту АРМ пользователей с поддержкой в актуальном состоянии вирусных сигнатур;
7. Обеспечить контроль за подключением неавторизованных переносных устройств (flash носителей) к АРМ. (Использовать только зарегистрированные в установленном в ФНС России порядке внешние носителями информации);
8. Организовать регистрацию событий, связанных с идентификацией и аутентификацией пользователей на выделенном АРМ;
9. Не допускать к работе на АРМ лиц, не имеющих доступ к услуге удаленного доступа;
10. Не допускать использование на АРМ средств удаленного управления (RAdmin, VNC, Remote Desktop и т.д.);
11. Не допускать предоставление общего доступа к папкам (файлам) АРМ;
12. Проводить не реже одного раза в квартал сканирование АРМ на наличие уязвимостей с установкой при необходимости обновлений операционной системы и используемого программного обеспечения;
13. Не допускать использования программного обеспечения, не относящегося к работе с ФИР;
14. Не допускать возможности сохранения реквизитов доступа пользователей средствами операционной системы или используемого для доступа к ФИР программного обеспечения, за исключением сервисной учетной записи;
15. Организовать опечатывание корпуса АРМ и периодическую проверку целостности печатей (пломбы, стикеров безопасности) с целью контроля несанкционированного вскрытия корпуса АРМ;
16. Обеспечить запрет несанкционированной загрузки операционной системы с внешних носителей.

Допускается использование АРМ одновременно как для работы с программными комплексами регионального и местного уровней (например, с ПК «Регион», системой «ЭОД»), так и для доступа к федеральным информационным ресурсам, с соблюдением выше перечисленных требований.

3.2. Политика и программа безопасности.

Защита информации как некогда актуальна на сегодняшний момент. Мы живем в информационном обществе и поглощаем её ежедневно. Информация порой становится дороже самих материальных благ. Соответственно возникает необходимость в защите. Каждое предприятие имеет свои базы данных, которыми интересуются конкуренты. Сейчас безопасность предприятия подразумевает не только физическую, материальную сохранность, но и информационную.

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

- ✓ невозможность миновать защитные средства;
- ✓ усиление самого слабого звена;
- ✓ невозможность перехода в небезопасное состояние;
- ✓ минимизация привилегий;
- ✓ разделение обязанностей;
- ✓ эшелонированность обороны;
- ✓ разнообразие защитных средств;
- ✓ простота и управляемость информационной системы;
- ✓ обеспечение всеобщей поддержки мер безопасности;
- ✓ адекватность (разумная достаточность);
- ✓ системность;
- ✓ прозрачность для легальных пользователей;
- ✓ равностойкость звеньев.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть "тайных" модемных входов или тестовых линий, идущих в обход экрана. Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Принцип адекватности (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Вряд ли деклассированный пролетарий потратит деньги на металлическую дверь, суперзамок и сигнализацию, если в квартире непропитые вещи можно пересчитать по пальцам.

Системность. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забывать о важности системного подхода. Он состоит в том, что система защиты должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств.

Прозрачность для легальных пользователей. Можно заставлять пользователей перед каждой операцией для надежной идентификации вводить 10-значный пароль, прикладывать палец к сканеру и произносить кодовую фразу. Но не разбегутся ли после этого сотрудники.

Равностойкость звеньев. Звенья - это элементы защиты, преодоление любого из которых означает преодоление всей защиты (например, окно и дверь в равной степени открывают вору путь в квартиру). Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае прочность защиты (или ее уровня, см. ниже) определяется прочностью самого слабого звена.

Обеспечение безопасности информации в крупных **автоматизированных системах** является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить.

Объектом защиты в современных АИС выступает территориально распределенная гетерогенная сеть со сложной структурой, предназначенная для распределенной обработки данных, часто называемая **корпоративной сетью**. Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных.

Решение проблем безопасности АИС заключается в построения целостной системы защиты информации. При этом защита от физических угроз, например доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов **политики безопасности**, решение которых обеспечит надежное и бесперебойное функционирование информационной системы.

Главными этапами построения политики безопасности являются следующие:

- обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается **Концепция информационной безопасности ИС**, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;
- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
- организация хранения информации в ИС;
- организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);
- регламентация допуска персонала к той или иной информации;
- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается схема безопасности, структура которой должна удовлетворять следующим условиям:

1. Защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи.
2. Разграничение потоков информации между сегментами сети.
3. Защита критичных ресурсов сети.
4. Защита рабочих мест и ресурсов от несанкционированного доступа (*НСД*).
5. Криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10 - 15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

С практической точки зрения политику безопасности целесообразно

рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносятся управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности,

организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);

- раздел, освещающий вопросы **физической защиты**;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение **непрерывной работы** организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности

нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

С него начать

Прежде чем строить какую-то систему защиты, определим, что и от кого (чего) мы хотим защитить. Нельзя защитить все и от всего. Согласитесь, не вся информация для вас одинаково ценна.

Итак, для начала выделите перечень информации (файлов), которые необходимо защитить, и ее физическое размещение (сразу станет ясно, что защищать лучше информацию, которая хранится на одном **компьютере**). **Прикиньте, во что может обойтись простой компьютеров, потеря электронной почты за день или утрата важных данных.**

Второе, что необходимо уяснить - от кого мы защищаем информацию. Кто тот злоумышленник (или их несколько), который теми или иными средствами может завладеть вашей информацией? Одновременно надо оценить силы злоумышленника - какие он может иметь организационные и технические возможности для доступа к информации (ведь злоумышленник может быть и сотрудником фирмы), сколько времени и денег ему не жалко на добычу информации. Потенциальный злоумышленник в принципе может и отсутствовать, а безопасности информации могут угрожать случайные факторы (вирусные эпидемии выход из строя компьютеров и т. д.).

Третье, что надо оценить - это угрозы информации. Различают следующие группы угроз:

- несанкционированный доступ к информации (чтение, копирование или изменение информации, ее подлоги навязывание);
- нарушение работоспособности компьютеров и прикладных программ, что может повлечь остановку производственных процессов;
- уничтожение информации.

В каждой из этих трех групп можно выделить десятки конкретных угроз, однако пока остановимся. Заметим только, что угрозы могут быть преднамеренными и случайными, а случайные, в свою очередь, обусловленные естественными факторами (например, стихийные бедствия) и человеческим фактором (ошибочные действия персонала). Случайные угрозы, в которых отсутствует злой умысел, обычно опасны только возможностью потери информации и нарушения работоспособности системы, от чего достаточно легко застраховаться. Преднамеренные же угрозы более серьезны с точки зрения потери для бизнеса, ибо здесь приходится бороться не со слепым (пусть и беспощадным в своей силе) случаем, но с думающим противником.

Выяснение того, что, от кого и от чего мы будем защищать - большой шаг на

пути к ответу на главный вопрос: как защищать? Так что на первый этап не жалко потратить времени, тем более что в небольшой фирме для мозгового штурма начальнику и его приближенным достаточно одного рабочего дня. Можно все это провести в виде импровизированной деловой игры, в том числе и с самим собой.

Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- * управление рисками (**оценка рисков**, выбор эффективных средств защиты);
- * **координация** деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- * **стратегическое планирование**;
- * **контроль** деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупается и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис. Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими

характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначена для обслуживания новым сервисом?

- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?

- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?

- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?

- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных

модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Тема «управление рисками» рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, нужно только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Типовую организацию вполне устроит типовый набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области И Б). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова «Анализ рисков, управления рисками» (Jet Info, 1999, 1).

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по *

Анализ рисков - важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet-системы, нужно учитывать следующие обстоятельства:

- новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное - его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля;

- новые (сетевые) сервисы и ассоциированные с ними угрозы.

Как правило, в Intranet-системах следует придерживаться принципа «все, что не разрешено, запрещено», поскольку «лишний» сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение «все непонятное опасно».

Важным понятием политики безопасности является ее избирательность.

Основой избирательной политики безопасности является избирательное управление доступом (ИУД), которое подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной.

Матрица доступа представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту - строка. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как «доступ на чтение», «доступ на запись», «доступ на исполнение» и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей ИУД. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата - зависимое условие), часы (время - зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа — наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных АИС.

Основу полномочной политики безопасности составляет полномочное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически ненисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула, включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: «простым условием защиты» и «свойством». В упрощенном виде, они определяют, что информация может передаваться только «наверх», то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, - если не выше.

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Основное назначение полномочной политики безопасности — регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах Минобороны США для обработки информации с различными грифами

секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами:

- отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);
- высокой стоимостью реализации и большими накладными расходами.

Помимо управления доступом субъектов к объектам системы проблема защиты информации имеет еще один аспект. Чтобы получить информацию о каком-либо объекте системы, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой требуемого объекта. Иными словами, при помощи каналов утечки информации. По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и др. в зависимости от особенностей системы и установленной защиты объектов. Эта особенность связана с тем, что при взаимодействии двух субъектов возникает некоторый поток информации от одного к другому.

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие информационные потоки в системе являются «легальными», то есть не ведут к утечке информации, а какие - ведут. Таким образом, возникает необходимость разработки правил, регулирующих управление информационными потоками в системе.

Для этого необходимо построить модель системы, которая может описывать такие потоки. Такая модель называется потоковой. Модель описывает условия и

свойства взаимного влияния (интерференции) субъектов, а также количество информации, полученной субъектом в результате интерференции.

Управление информационными потоками в системе не есть самостоятельная политика, так как оно не определяет правил обработки информации. Управление информационными потоками применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты.

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным системам из-за существования в них скрытых каналов. Тем не менее, управление доступом обеспечивает достаточно надежную защиту в простых системах, не обрабатывающих особо важную информацию. В противном случае средства защиты должны дополнительно реализовывать управление информационными потоками. Организация такого управления в полном объеме достаточно сложна, поэтому его обычно используют для усиления надежности полномочной политики: ненисходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные - запрещенными.

Отметим, что кроме способа управления доступом политика безопасности включает еще и другие требования, такие как подотчетность, гарантии и т.д.

Избирательное и полномочное управление доступом, а также управление информационными потоками - своего рода три кита, на которых строится вся защита.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносятся управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;

- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала,, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение **непрерывной работы организации**;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи

настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень

безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного

Программа безопасности

После того, как сформулирована политика безопасности, можно приступить к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и

устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис, рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

— какого рода информация предназначена для обслуживания новым сервисом?

каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?

— каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?

— есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?

— каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

— каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются

необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи.

Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Тема управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, нужно только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Типовую организацию вполне устроит типовый набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими

параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова "Анализ рисков, управления рисками" (Jet Info, 1999,11).

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по *

Организация защиты информации в корпоративной сети

Обеспечение безопасности информации в крупных **автоматизированных** системах является сложной задачей. Реальную стоимость содержащейся в таких системах информации подсчитать сложно, а безопасность информационных ресурсов трудно измерить или оценить.

Объектом защиты в современных АИС выступает территориально распределенная гетерогенная сеть со сложной структурой, предназначенная для распределенной обработки данных, часто называемая *корпоративной сетью*. Характерной особенностью такой сети является то, что в ней функционирует оборудование самых разных производителей и поколений, а также неоднородное программное обеспечение, не ориентированное изначально на совместную обработку данных.

Решение проблем безопасности АИС заключается в построении целостной системы защиты информации. При этом защита от физических угроз, например доступа в помещения и утечки информации за счет ПЭМИ, не вызывает особых проблем. На практике приходится сталкиваться с рядом более общих вопросов политики безопасности, решение которых обеспечит надежное и бесперебойное функционирование информационной системы.

Главными этапами построения политики безопасности являются следующие:

- обследование информационной системы на предмет установления ее организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается **Концепция информационной безопасности ИС**, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;
- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
- организация хранения информации в ИС;
- организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);
- регламентация допуска персонала к той или иной информации;
- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается **схема безопасности**, структура которой должна удовлетворять следующим условиям:

1. Защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи,
2. Разграничение потоков информации между сегментами сети.
3. Защита критичных ресурсов сети.
4. Защита рабочих мест и ресурсов от несанкционированного доступа (НСД).
5. Криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10-15% стоимости информации тратится на продукты, обеспечивающие безопасность

функционирования сетевой информационной системы.

Защита от несанкционированного проникновения и утечки информации

Основным источником угрозы несанкционированного проникновения в АИС является канал подключения к внешней сети, например, к Internet. Вероятность реализации угрозы зависит от множества факторов, поэтому говорить о едином способе защиты в каждом конкретном случае не представляется возможным. Распространенным вариантом защиты является **применение межсетевых экранов** или брандмауэров.

Брандмауэр - *барьер между двумя сетями: внутренней и внешней, обеспечивает прохождение входящих и исходящих пакетов в соответствии с правилами, определенными администратором сети.* Брандмауэр устанавливается у входа в корпоративную сеть и все коммуникации проходят через него. Возможности межсетевых экранов позволяют определить и реализовать правила разграничения доступа как для внешних, так и для внутренних пользователей корпоративной сети, скрыть, при необходимости, структуру сети от внешнего пользователя, блокировать отправку информации по «запретным» адресам, контролировать использование сети и т.д. Вход в корпоративную сеть становится узким местом, прежде всего для злоумышленника.

Разграничение потоков информации между сегментами сети

В зависимости от характера информации, обрабатываемой в том или ином сегменте сети, и от способа взаимодействия между сегментами реализуют один из следующих вариантов.

В первом варианте не устанавливается никакого разграничения информационных потоков, т.е. защита практически отсутствует. Такой вариант оправдан в случаях, когда ни в одном из взаимодействующих сегментов не хранится и не обрабатывается критичная информация или когда сегменты сетевой информационной системы содержат информацию одинаковой важности и находятся в одном здании, в пределах контролируемой зоны.

Во втором варианте разграничение достигается средствами коммуникационного оборудования (маршрутизаторы, переключатели и т.п.). Такое разграничение не позволяет реализовать защитные функции в полном объеме поскольку, во-первых, коммуникационное оборудование изначально не рассматривается как средство защиты и, во-вторых, требуется детальное представление о структуре сети и циркулирующих в ней информационных потоков.

В третьем варианте предполагается применение брандмауэров. Данный способ применяется, как правило, при организации взаимодействия между сегментами через сеть Internet, когда уже установлены брандмауэры, предназначенные для контроля за потоками информации между информационной системой и сетью Internet.

Защита критичных ресурсов АИС

Наиболее критичными ресурсами корпоративной сети являются серверы, а основным способом вмешательства в нормальный процесс их функционирования является проведение атак с использованием уязвимых мест в аппаратном и программном обеспечении. Атака может быть реализована как из внешней сети, так и из внутренней. Основная задача заключается не столько в своевременном обнаружении и регистрации атаки, сколько в противодействии ей.

Наиболее мощными инструментами защиты, предназначенными для оперативного реагирования на подобные нападения, являются специальные системы, наподобие системы RealSecure, производимой американской корпорацией Internet Security Systems, Inc., которые позволяют своевременно обнаружить и предотвратить наиболее известные атаки, проводимые по сети.

Защита рабочих мест и ресурсов от НСД

До настоящего времени большинство автоматизированных систем

ориентируется только на *встроенные защитные механизмы сетевых операционных систем*. При правильном администрировании такие механизмы обеспечивают достаточную защиту информации на серверах корпоративной сети.

Однако обработка информации, подлежащей защите, производится рабочих станциях, подавляющее большинство которых (более 90%) работает под управлением MS DOS или Windows'95 и не имеет средств обеспечения безопасности, так как эти операционные системы не содержат встроенных механизмов защиты. Как следствие, на незащищенном рабочем месте может обрабатываться критичная информация, доступ к которой ничем не ограничен. Для рабочих станций рекомендуется применять дополнительные средства защиты, часть из которых описана в предыдущем разделе.

Криптографическая защита информационных ресурсов

Шифрование является одним из самых надежных способов защиты данных от несанкционированного ознакомления. Особенностью применения подобных средств в России является жесткая законодательная регламентация. Для защиты конфиденциальной информации разрешается применять только сертифицированные ФАПСИ продукты. В настоящее время в корпоративных сетях они устанавливаются только на тех рабочих местах, где хранится информация, имеющая очень высокую степень важности.

Этапы построения политики безопасности

По окончании работ *первого этапа* - обследования информационной системы - необходимо иметь полное представление о том, в каком состоянии находится корпоративная сеть и о том, что нужно сделать, чтобы обеспечить в ней защиту информации.

На основе данных обследования можно перейти ко *второму этапу* - выбору, приобретению, установке, настройке и эксплуатации систем защиты в соответствии с разработанными рекомендациями.

Любое средство защиты создает дополнительные неудобства в работе пользователя, при этом препятствий тем больше, чем меньше времени уделяется настройке систем защиты. Администратор безопасности должен ежедневно обрабатывать данные регистрации, чтобы своевременно корректировать настройки, обеспечивающие адаптацию к изменениям в технологии обработки информации. Без этого любая система защиты, какой бы хорошей она ни была, обречена на медленное вымирание.

Третий этап - обучение администраторов безопасности работе со средствами защиты. В процессе обучения администратор получает базовые знания о технологии обеспечения информационной безопасности, об имеющихся в операционных системах подсистемах безопасности и о возможностях систем защиты, о технологических приемах, используемых при их настройке и эксплуатации.

Четвертый этап - информационное обслуживание по вопросам безопасности. Наличие своевременной информации об уязвимых местах и способах защиты способствует принятию адекватных мер обеспечения безопасности. Источники подобных сведений - книги, журналы, Web-серверы и т.п. Однако администратор безопасности не всегда имеет достаточное количество времени для поиска необходимых сведений в этом море информации. Поэтому при выборе системы защиты необходимо учитывать возможности обеспечения последующей информационной поддержки.

Пятый этап - периодический аудит системы информационной безопасности. Корпоративная сеть является постоянно изменяющейся структурой: появляются новые серверы и рабочие станции, меняется программное обеспечение и его настройки, состав информации, персонал, работающий в организации, и т.д. Все это приводит к тому, что степень защищенности системы постоянно изменяется и, что наиболее опасно, снижается.

Чтобы адаптировать систему информационной безопасности к новым условиям

работы, необходимо отслеживать изменения и своевременно реагировать на них. Многие работы по анализу состояния защищенности корпоративной сети могут быть выполнены при помощи специальных программных средств, например Internet Scanner и System Security Scanner из семейства SAFESUITE корпорации Internet Security Systems Inc. Такие программные средства существенно облегчают работу администратора безопасности по поиску ошибок в настройках и выявлению критичного программного обеспечения, а также позволяют в автоматизированном режиме отслеживать состояние корпоративной сети, своевременно обнаруживать и устранять возможные источники проблем.

Составной частью работ пятого этапа является корректировка Плана защиты в соответствии с реальным состоянием корпоративной сети, поскольку самая совершенная схема рано или поздно устаревает и становится препятствием на пути совершенствования технологии обработки данных.

Следует помнить, что не существует стандартных решений, одинаково хорошо работающих в разных условиях. Всегда возможны и необходимы дополнения к рассмотренному общему плану организации защиты корпоративной сети, учитывающие особые условия той или иной организации. Однако реализация комплекса рассмотренных мероприятий с учетом возможных дополнений способна обеспечить достаточный уровень защищенности информации в корпоративной сети.

3.2. Подходы, принципы, методы и средства обеспечения безопасности.

Под обеспечением безопасности информационных систем понимают меры, предохраняющие информационную систему от случайного или преднамеренного вмешательства в режимы ее функционирования (243).

Существует два принципиальных подхода к обеспечению компьютерной безопасности (34).

- **Фрагментарный.** Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.).

Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком - локальность действия, т.е. фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов от конкретной угрозы. Но не более того.

- **Комплексный.** Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам (рис.) и традиционно рассматривается в виде трех дополняющих друг друга направлений. Организация защищенной среды обработки информации позволяет в рамках существующей политики безопасности обеспечить соответствующий уровень безопасности АИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

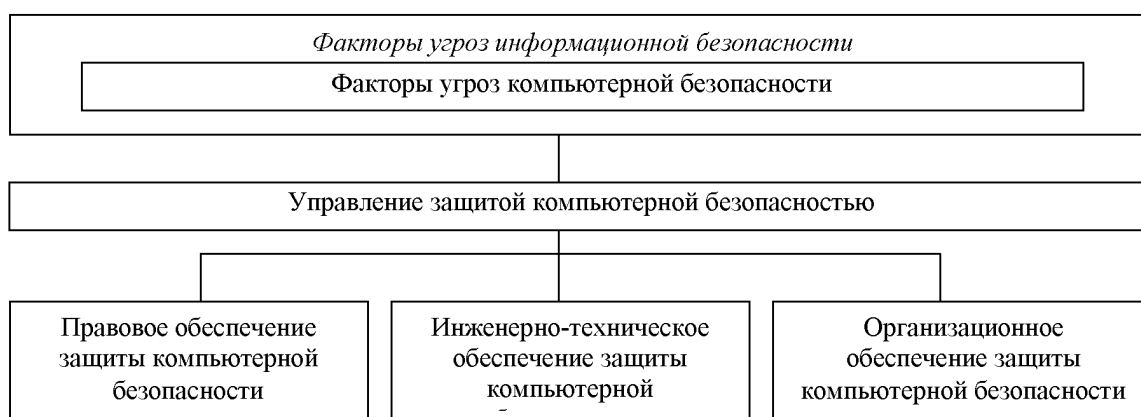


Рис. 10

Процесс управления защитой информации включает в себя компоненты, представленные на рис. 11.

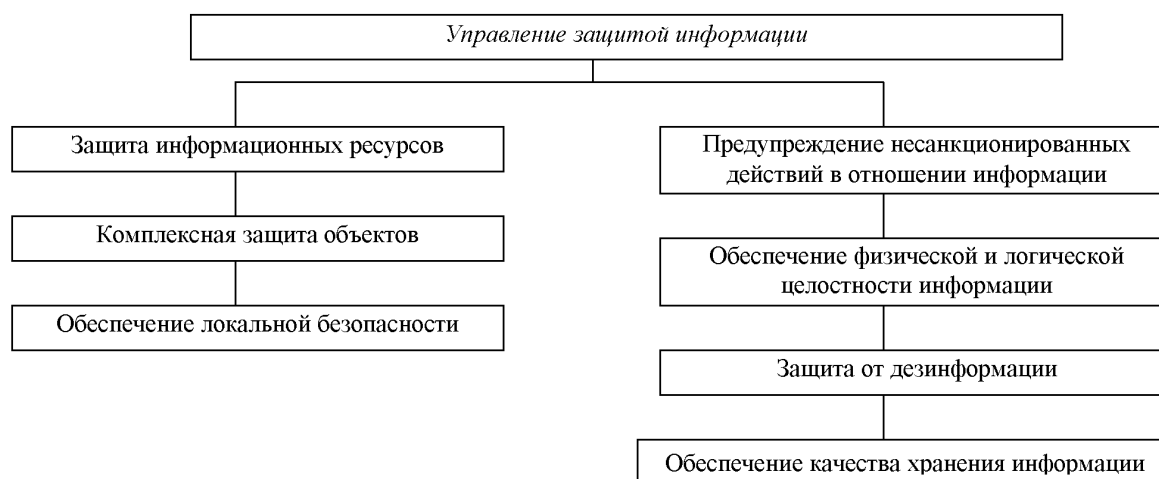


Рис.11

Особенностью *системного подхода* к защите информации является создание защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические. Организация подобной защищенной среды позволяет гарантировать определенный уровень безопасности автоматизированной информационной системы.

Системный подход к защите информации базируется на следующих методологических принципах:

- конечной цели - абсолютного приоритета конечной (глобальной) цели;
- единства - совместного рассмотрения системы как целого' и как совокупности частей (элементов);
- связности - рассмотрения любой части системы совместно с ее связями с окружением;
- модульного построения - выделения модулей в системе и рассмотрения ее как совокупности модулей;
- иерархии - введения иерархии частей (элементов) и их ранжирования;
- функциональности - совместного рассмотрения структуры и функции с приоритетом функции над структурой;
- развития - учета изменяемости системы, ее способности к развитию, расширению, замене частей, накоплению информации;
- децентрализации - сочетания в принимаемых решениях и управлении централизации и децентрализации;
- неопределенности - учета неопределенностей и случайностей в системе.

Современные исследователи выделяют следующие методологические, организационные и реализационные *принципы информационной* (в том числе компьютерной) *безопасности*.

Принцип законности. Состоит в следовании действующему законодательству в области обеспечения информационной безопасности.

Принцип неопределенности. Возникает вследствие неясности поведения субъекта, т.е. кто, когда, где и каким образом может нарушить безопасность объекта защиты.

Принцип невозможности создания идеальной системы защиты. Следует из принципа неопределенности и ограниченности ресурсов указанных средств.

Принципы минимального риска и минимального ущерба. Вытекают из невозможности создания идеальной системы защиты. В соответствии с ним необходимо учитывать конкретные условия существования объекта защиты для любого момента времени.

Принцип безопасного времени. Предполагает учет абсолютного времени, т.е. в течение которого необходимо сохранение объектов защиты; и относительного времени, т.е. промежутка времени от момента выявления злоумышленных действий до достижения цели злоумышленником.

Принцип «защиты всех ото всех». Предполагает организацию защитных мероприятий против всех форм угроз объектам защиты, что является следствием принципа неопределенности.

Принципы персональной ответственности. Предполагает персональную ответственность каждого сотрудника предприятия, учреждения и организации за соблюдение режима безопасности в рамках своих полномочий, функциональных обязанностей и действующих инструкций.

Принцип ограничения полномочий. Предполагает ограничение полномочий субъекта на ознакомление с информацией, к которой не требуется доступа для нормального выполнения им своих функциональных обязанностей, а также введение запрета доступа к объектам и зонам, пребывание в которых не требуется по роду деятельности.

Принцип взаимодействия и сотрудничества. Во внутреннем проявлении предполагает культивирование доверительных отношений между сотрудниками, отвечающими за безопасность (в том числе информационную), и персоналом. Во внешнем проявлении - налаживание сотрудничества со всеми заинтересованными организациями и лицами (например, правоохранительными органами).

Принцип комплексности и индивидуальности. Подразумевает невозможность обеспечения безопасности объекта защиты каким-либо одним мероприятием, а лишь совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям.

Принцип последовательных рубежей безопасности. Предполагает как можно более раннее оповещение о состоявшемся посягательстве на безопасность того или иного объекта защиты или ином неблагоприятном происшествии с целью увеличения вероятности того, что заблаговременный сигнал тревоги средств защиты обеспечит сотрудникам, ответственным за безопасность, возможность вовремя определить причину тревоги и организовать эффективные мероприятия по противодействию.

Принципы равнопрочности и равномогности рубежей защиты. Равнопрочность подразумевает отсутствие незащищенных участков в рубежах защиты. Равномогность предполагает относительно одинаковую величину защищенности рубежей защиты в соответствии со степенью угроз объекту защиты.

- Комплексный подход к построению системы защиты при ведущей роли организационных мероприятий. Он означает оптимальное сочетание программных аппаратных средств и организационных мер защиты, подтвержденное практикой создания отечественных и зарубежных систем защиты.

- Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки. Пользователям предоставляется минимум строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.

- Полнота контроля и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в ЭИС без ее предварительной регистрации.

- Обеспечение надежности системы защиты, т.е. невозможность снижения ее уровня при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.

- Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

- Экономическая целесообразность использования систем защиты. Она выражается в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации АИС без системы защиты информации.

Методы и средства обеспечения безопасности экономического объекта представлены на рис. 12

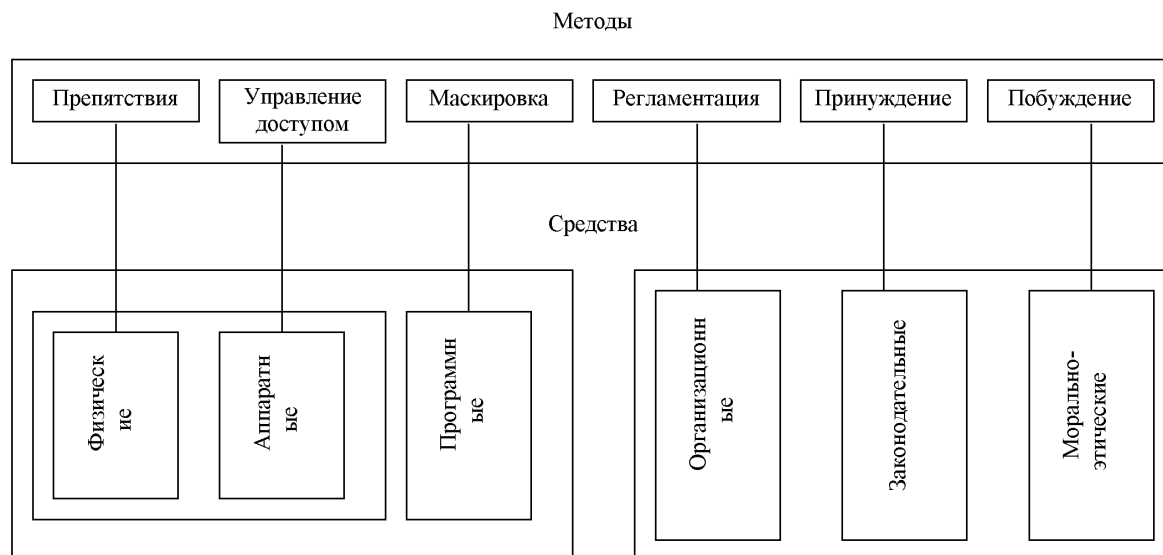


Рис. 12. Методы и средства информационной безопасности экономического объекта.

Методами обеспечения защиты информации на предприятии являются следующие:

Препятствие - метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

Управление доступом - метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);
- аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- регистрацию обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий).

Маскировка - метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация - метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение - метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

Побуждение - метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью следующих основных средств: физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических.

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты - это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия.

Аппаратно-программные средства защиты - средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.

Криптографические средства - средства защиты с помощью преобразования информации (шифрование).

Организационные средства - организационно-технические и организационно-правовые мероприятия по регламентации поведения персонала.

Законодательные средства - правовые акты страны, которые регламентируют

правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства - нормы, традиции в обществе, например: Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ в США.

Все рассмотренные средства защиты разделены на *формальные* (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и *«неформальные»* (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность).

Для реализации мер безопасности используются различные механизмы шифрования (криптографии).

Криптография - это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.

Сущность криптографических методов заключается в следующем.

Готовое к передаче сообщение - будь то данные, речь либо графическое изображение того или иного документа, обычно называется *открытым*, или незащищенным текстом. В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено подслушивающим лицом посредством умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается, преобразуясь в шифрограмму, или *закрытый текст*. Санкционированный пользователь, получив сообщение, дешифрует или раскрывает его посредством обратного преобразования шифрограммы. Вследствие чего получается исходный открытый текст.

Шифрование может быть *симметричным* и *асимметричным*. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования - другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием внедряются следующие *механизмы безопасности*:

- цифровая электронная подпись;
- контроль доступа;
- обеспечение целостности данных;
- обеспечение аутентификации;
- постановка трафика;
- управление маршрутизацией;
- арбитраж или освидетельствование.

Механизмы цифровой подписи основываются на алгоритмах асимметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание получателем. Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической, контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя.

Механизмы контроля доступа осуществляют проверку полномочий объектов АИС (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке.

Механизмы обеспечения целостности данных применяются к отдельному блоку и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока и обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности

потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

Механизмы постановки трафика, называемые также механизмами заполнения текста, используют для засекречивания потока данных. Они основываются на генерации объектами АИС блоков, их шифровании и организации передачи по каналам сети. Тем самым нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами АИС, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит через арбитра, что позволяет ему впоследствии подтвердить упомянутые характеристики.

Отметим типичные недостатки, присущие системе безопасности экономических объектов:

- узкое, несистемное понимание проблемы безопасности объекта;
- пренебрежение профилактикой угроз, работа по принципу «Появилась угроза - начинаем ее устранять»;
- некомпетентность в экономике безопасности, неумение сопоставлять затраты и результаты;
- «технократизм» руководства и специалистов службы безопасности, интерпретация всех задач на языке знакомой им области.

3.2. Организационно-техническое обеспечение компьютерной безопасности.

Организационное обеспечение - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий (101).

Организационное обеспечение компьютерной безопасности включает в себя ряд мероприятий:

- организационно-административные;
- организационно-технические;
- организационно-экономические.

Организационно-административные мероприятия предполагают (101):

- минимизацию утечки информации через персонал (организация мероприятий по подбору и расстановке кадров, создание благоприятного климата в коллективе и т. д.);
- организацию специального делопроизводства и документооборота для конфиденциальной информации, устанавливающих порядок подготовки, использования, хранения, уничтожения и учета документируемой информации на любых видах носителей;
- выделение специальных защищенных помещений для размещения средств вычислительной техники и связи, а также хранения носителей информации;
- выделение специальных средств компьютерной техники для обработки конфиденциальной информации;
- организацию хранения конфиденциальной информации на промаркированных отчуждаемых носителях в специально отведенных для этой цели местах;
- использование в работе сертифицированных технических и программных средств, установленных в аттестованных помещениях; организацию регламентированного доступа пользователей к работе со средствами компьютерной техники, связи и в хранилище (архив) носителей конфиденциальной информации;
- установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;
- контроль соблюдения требований по защите конфиденциальной информации.

Система организационных мероприятий, направленных на максимальное предотвращение утечки информации через персонал включает:

- оценка у претендентов на вакантные должности при подборе кадров таких личностных качеств, как порядочность, надежность, честность и т. д.;
- ограничение круга лиц, допускаемых к конфиденциальной информации;
- проверка надежности сотрудников, допускаемых к конфиденциальной информации, письменное оформление допуска;
- развитие и поддержание у работников компании корпоративного духа, создание внутренней среды, способствующей проявлению у сотрудников чувства принадлежности к своей организации, позитивного отношения человека к организации в целом (лояльность);
- проведение инструктажа работников, участвующих в мероприятиях, непосредственно относящихся к одному из возможных каналов утечки информации.

Все лица, принимаемые на работу, проходят инструктаж и знакомятся с памяткой о сохранении служебной или коммерческой тайны. Памятка разрабатывается системой безопасности с учетом специфики организации.

Сотрудник, получивший доступ к конфиденциальной информации, подписывает индивидуальное письменное обязательство об ее неразглашении. Обязательство составляется в одном экземпляре и храниться в личном деле сотрудника не менее 5 лет после его увольнения. При увольнении из организации сотрудником дается подписка.

Функции отобрания обязательства и подписок возлагаются на кадровый аппарат организации.

Служащий организации, подписывая подобного рода документ, должен четко представлять, что конкретно из конфиденциальной информации является тайной организации. В том числе по этой причине необходимо, чтобы вся конфиденциальная информация была обособлена от остальных сведений, а документы, ее содержащие, носили соответствующий гриф.

Использование обязательств о сохранении конфиденциальной информации позволяет обеспечить ее юридическую защиту, к которой имеет (или имел) доступ персонал организации.

Все руководители, сотрудники и технический персонал должны быть охвачены регулярной подготовкой по вопросам обеспечения информационной безопасности. При этом должно быть два вида обучения: первоначальное и систематическое.

С увольняющимися сотрудниками проводятся беседы, направленные на предотвращение разглашения конфиденциальной информации. Эти обязательства, как правило, подкрепляются соответствующей подпиской.

Организацией конфиденциального делопроизводства является:

- документирование информации;
- учет документов и организация документооборота;
- обеспечение надежного хранения документов;
- проверка наличия, своевременности и правильности их исполнения;
- своевременное уничтожение документов.

В табл. 4 изложены организационные мероприятия, обеспечивающие защиту документальной информации (106).

Таблица 4

Обеспечение информационной безопасности организации

Составные части делопроизводства	Функции обеспечения ИБ при работе с документами	Способы выполнения
Документирование	Предупреждение: - необоснованного изготовления документов; - включение в документы избыточной конфиденциальной информации; - необоснованного завышения степени конфиденциальности документов; - необоснованной рассылки	Определение перечня документов Осуществление контроля за содержанием документов и степени конфиденциальности содержания Определение реальной степени конфиденциальности сведений, включенных в документ Осуществление контроля за размножением и рассылкой документов
Учет документов	Предупреждение утраты (хищения) документов	Контроль за местонахождением документа
Организация документооборота	Предупреждение: - необоснованного ознакомления с документами; - неконтролируемой передачи документов	Установление разрешительной системы доступа исполнителей к документам Установление порядка приема-передачи документов между сотрудниками

Хранение документов	Обеспечение сохранности документов Исключение из оборота документов, потерявших ценность	Выделение специально оборудованных помещений для хранения документов, исключающих доступ к ним посторонних лиц Установление порядка подготовки документов для уничтожения
Уничтожение документов	Исключение доступа к бумажной «стружке»	Обеспечение необходимых условий уничтожения Осуществление контроля за правильностью и своевременностью уничтожения документов
Контроль наличия, своевременности и правильности исполнения документов	Контроль наличия документов, выполнения требований обработки, учета, исполнения и сдачи	Установление порядка проведения наличия документов и порядка их обработки

При выборе и оборудовании специальных защищенных помещений для размещения СКТ и связи, а также хранения носителей информации рекомендуется придерживаться следующих требований (101). Оптимальной формой помещения является квадратная или близкая к ней. Помещение не должно быть проходным для обеспечения контроля доступа, желательно размещать его недалеко от постов охраны, что снижает шансы незаконного проникновения.

Помещение должно быть оборудовано пожарной и охранной сигнализацией, системой пожаротушения, рабочим и аварийным освещением, кондиционированием, средствами связи.

Рабочие помещения должны быть закрыты от посещения посторонних лиц. Всех посетителей (кроме деловых партнеров) должны встречать и сопровождать по территории фирмы работники кадрового аппарата, службы безопасности или охраны. Посетителям взамен удостоверений личности, выдаются разовые карточки гостя, размещаемые на груди или лацкане пиджака. Исключается доступ посторонних лиц в хранилища конфиденциальных документов, зал совещаний, отдел маркетинга, службу безопасности и т.д.

Хранение конфиденциальной информации, полученной в результате резервного копирования, должно осуществляться на промаркированных отчуждаемых носителях в специально отведенных для этой цели местах.

Комплекс организационно-технических мероприятий состоит:

- в ограничении доступа посторонних лиц внутрь корпуса оборудования за счет установки различных запорных устройств и средств контроля;
- в отключении от ЛВС, Internet тех СКТ, которые не связаны с работой с конфиденциальной информацией, либо в организации межсетевых экранов;
- в организации передачи такой информации по каналам связи только с использованием специальных инженерно-технических средств;
- в организации нейтрализации утечки информации по электромагнитным и акустическим каналам;
- в организации защиты от наводок на электрические цепи узлов и блоков автоматизированных систем обработки информации;
- в проведении иных организационно-технических мероприятий, направленных на обеспечение компьютерной безопасности.

Организационно-технические мероприятия по обеспечению компьютерной

безопасности предполагают активное использование инженерно-технических средств защиты.

Например, в открытых сетях для защиты информации применяют межсетевые экраны (МЭ).

Межсетевые экраны - это локальное или функционально-распределенное программно-аппаратное средство (комплекс средств), реализующее контроль за информацией, поступающей в автоматизированные системы или выходящей из них.

Проведение организационно-экономических мероприятий по обеспечению компьютерной безопасности предполагает:

- стандартизацию методов и средств защиты информации;
- сертификацию средств компьютерной техники и их сетей по требованиям информационной безопасности;
- страхование информационных рисков, связанных с функционированием компьютерных систем и сетей;
- лицензирование деятельности в сфере защиты информации.

Инженерно-техническое обеспечение компьютерной безопасности - это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности предприятия (101).

По области применения технические средства противодействия подразделяются на две категории:

1. Устройства пассивного противодействия:

- детекторы радиоизлучений;
- средства защиты помещений;
- средства защиты телефонных аппаратов и линий связи;
- средства защиты информации от утечки по оптическому каналу;
- генераторы акустического шума;
- средства защиты компьютерной техники и периферийных устройств и др.

2. Устройства активного противодействия:

- системы поиска и уничтожения технических средств разведки;
- устройства постановки помех.

Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения (ИТО). Противодействие угрозам несанкционированного доступа к информации (утечке) с помощью специальных технических средств основывается на двух ключевых идеях:

- ликвидация (ослабление) канала утечки информации;
- исключение возможности злоумышленника принимать и воспринимать информацию.

Методы обеспечения информационной безопасности организации на основе ИТО. Методы обеспечения информационной безопасности организации в части угроз НСД к информации реализуют вышеизложенные принципы. Противодействие утечке (НСД) информации осуществляется методом скрытия информации. На рис. 13 приведена классификация методов обеспечения информационной безопасности, основанных на использовании инженерно-технических средств. (101)



Рис. 13. Классификация методов обеспечения информационной безопасности на основе технических средств.

Для эффективного применения технических средств обеспечения информационной безопасности необходимо комплексное проведение организационных (в части технических средств), организационно-технических и технических мероприятий. В настоящее время существует развитый арсенал мер и средств обеспечения информационной безопасности от воздействия угроз НСД. Многие из них являются альтернативными, поэтому необходимо выбрать их оптимальный состав.

Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения).

Одним из основных направлений противодействия утечке информации по техническим каналам и обеспечения безопасности информационных ресурсов является проведение специальных проверок (СП) по выявлению электронных устройств перехвата информации и специальных исследований (СИ) на побочные электромагнитные излучения и наводки технических средств обработки информации, аппаратуры и оборудования, в том числе и бытовых приборов.

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

- Своевременному определению возможных каналов утечки информации.
- Определению энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).
- Оценке возможности средств злоумышленников обеспечить контроль этих каналов.
- Обеспечению исключения или ослабления энергетики каналов утечки соответствующими организационными, организационно-техническими или техническими мерами и средствами.

Защита информации от утечки по визуально-оптическому каналу - это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

С целью защиты информации от утечки по визуально-оптическому каналу

рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);
- уменьшить отражательные свойства объекта защиты;
- уменьшить освещенность объекта защиты (энергетические ограничения);
- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- применять средства маскирования, имитации и другие с целью защиты и введение в заблуждение злоумышленника;
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;
- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;
- применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

В качестве оперативных средств сокрытия находят широкое применение аэрозольные завесы. Это взвешенные в газообразной среде мельчайшие частицы различных веществ, которые в зависимости от размеров и агрегатного сочетания образуют дым, копоть, туман. Они преграждают распространение отраженного от объекта защиты света. Хорошими светопоглощающими свойствами обладают дымообразующие вещества.

Аэрозольные образования в виде маскирующих завес обеспечивают индивидуальную или групповую защиту объектов и техники, в том числе и выпускаемую продукцию.

Защита информации по акустическому каналу - это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры.

Организационные меры предполагают проведение архитектурно-планировочных, пространственных и режимных мероприятий, а организационно-технические - пассивных (звукоизоляция, звукопоглощение) и активных (звукоподавление) мероприятий. Не исключается проведение и технических мероприятий за счет применения специальных защищенных средств ведения конфиденциальных переговоров.

Архитектурно-планировочные меры предусматривают предъявление определенных требований на этапе проектирования зданий и помещений или их реконструкцию и приспособление с целью исключения или ослабления неконтролируемого распространения звуковых полей непосредственно в воздушном пространстве или в строительных конструкциях в виде структурного звука. Эти требования могут предусматривать как выбор расположения помещений в пространственном плане, так и их оборудование необходимыми для акустической безопасности элементами, исключающими прямое или отраженное в сторону возможного расположения злоумышленника распространение звука. В этих целях двери оборудуются тамбурами, окна ориентируются в сторону охраняемой (контролируемой) от присутствия посторонних лиц территории и пр.

Режимные меры предусматривают строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами - в них очень много

поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний.

В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства. К активным средствам относятся генераторы шума - технические устройства, вырабатывающие шумоподобные электронные сигналы.

Эти сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях или вне их, а вибрационные - для маскирующего шума в ограждающих конструкциях. Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания.

Защита информации от утечки по электромагнитным каналам - это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок в технических средствах обработки и передачи информации сводятся к рациональным конструкторско-технологическим решениям, к числу которых относятся:

- экранирование элементов и узлов аппаратуры; ослабление электромагнитной, емкостной, индуктивной связи между элементами и токонесущими проводами;
- фильтрация сигналов в цепях питания и заземления и другие меры, связанные с использованием ограничителей, развязывающих цепей, систем взаимной компенсации.

Экранирование позволяет защитить их от нежелательных воздействий акустических и электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить (или исключить) паразитное влияние внешних излучений.

Эксплуатационные меры ориентированы на выбор мест установки технических средств с учетом особенностей их электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны. В этих целях возможно осуществлять экранирование помещений, в которых находятся средства с большим уровнем побочных электромагнитных излучений (ПЭМИ).

Защита от прослушивания средствами ИТО обеспечивается:

- применением звукопоглощающих облицовок, специальных дополнительных тамбуров дверных проемов, двойных оконных переплетов (при использовании направленного микрофона и стетоскопа);
- оклеиванием стекол светопрозрачным материалом, рассеивающим лазерный луч (при использовании лазерных средств);
- использованием специальных аттестованных помещений, исключающих появление каналов утечки акустической конфиденциальной информации.

Средства обнаружения закладных микрофонов включают:

- средства радиоконтроля помещений;
- средства поиска неизлучающих закладных устройств;
- средства подавления закладных устройств.

Защита информации от утечки по материально-вещественному каналу - это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода информации за пределы контролируемой зоны в виде производственных или промышленных отходов.

В практике производственной и трудовой деятельности отношение к отходам, прямо скажем, бросовое. В зависимости от профиля работы предприятия отходы могут быть в виде испорченных накладных, фрагментов исполняемых документов,

черновиков, бракованных заготовок деталей, панелей, кожухов и других устройств для разрабатываемых моделей новой техники или изделий.

По виду отходы могут быть твердыми, жидкими, газообразными. И каждый из них может бесконтрольно выходить за пределы охраняемой территории. Жидкости сливаются в канализацию, газы уходят в атмосферу, твердые отходы - зачастую просто на свалку. Особенно опасны твердые отходы. Это и документы, и технология и используемые материалы, и испорченные комплектующие. Все это совершенно достоверные, конкретные данные.

Меры защиты этого канала в особых комментариях не нуждаются.

Следует отметить, что при защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

- Выявление возможных каналов утечки.
- Обнаружение реальных каналов.
- Оценка опасности реальных каналов.
- Локализация опасных каналов утечки информации.
- Систематический контроль за наличием каналов и качеством их защиты.

Защита информации от утечки по техническим каналам - это комплекс мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

Постулаты такой защиты:

- Безопасных технических средств нет.
- Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

- Любой канал утечки информации может быть обнаружен и локализован.

«На каждый яд есть противоядие».

- Канал утечки информации легче локализовать, чем обнаружить.

Для непосредственной организации обеспечения информационной безопасности структурой и штатным расписанием предусматриваются специальные подразделения и сотрудники. Основные функции таких служб заключаются в следующем:

- На этапе проектирования (совершенствования) системы информационной безопасности:

- формирование требований к системе информационной безопасности;
- участие в разработке компонентов и системы информационной безопасности

в целом.

- На этапе эксплуатации:
- планирование, организация и обеспечение функционирования системы информационной безопасности;

- обучение пользователей и технического персонала организации формам и методам эксплуатации технических средств;

- контроль за соблюдением пользователями и техническим персоналом правил работы и эксплуатации технических средств в части обеспечения информационной безопасности.

Организационно-правовой статус службы безопасности. Многогранность организационной сферы обеспечения безопасности обуславливает создание специальной службы безопасности (СБ), осуществляющей все организационные мероприятия. СБ формируется на основе анализа, оценки и прогнозирования деятельности организации в части решения задач обеспечения ее безопасности.

Служба безопасности - система штатных органов управления и подразделений, предназначенных для обеспечения безопасности организации.

Правовой основой формирования СБ является решение руководства о создании СБ, оформленное соответствующим приказом или распоряжением, либо решением вышестоящей организации, в состав которой входит данная организация.

СБ предприятия подчиняется руководителю службы безопасности, который

находится в подчинении руководителя организации. Штатная структура и численность СБ определяется реальными потребностями организации.

Структура и задачи службы безопасности представлены на рис. 14 (106).

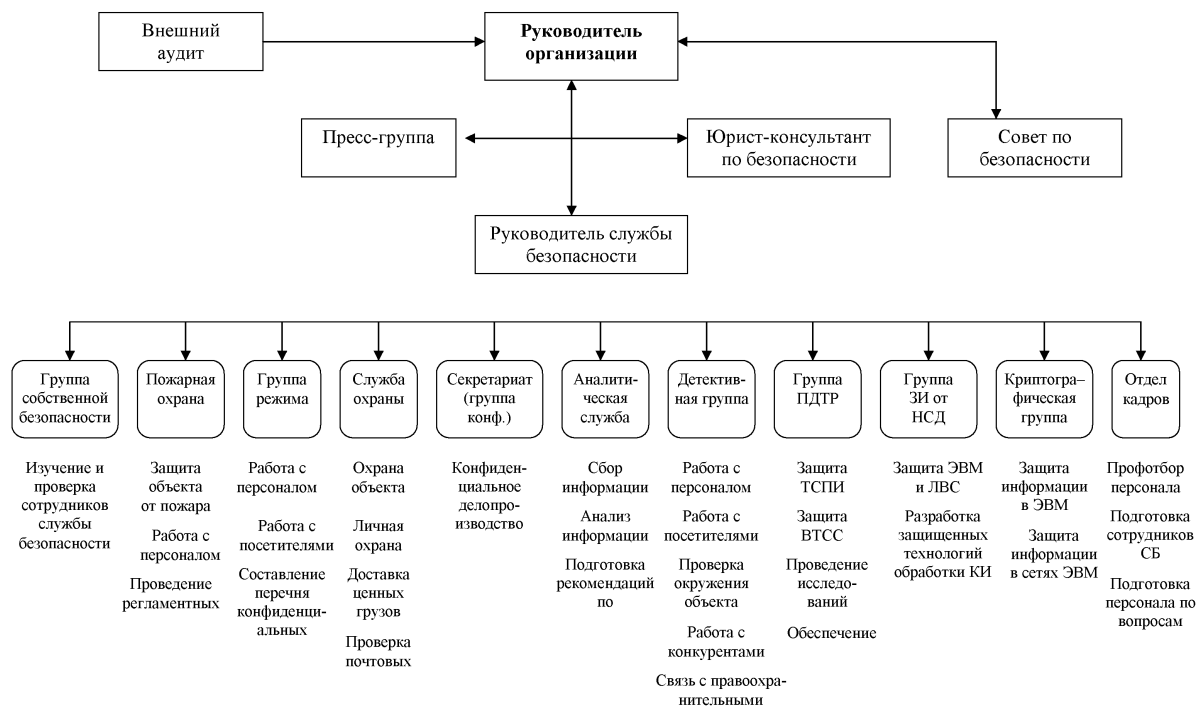
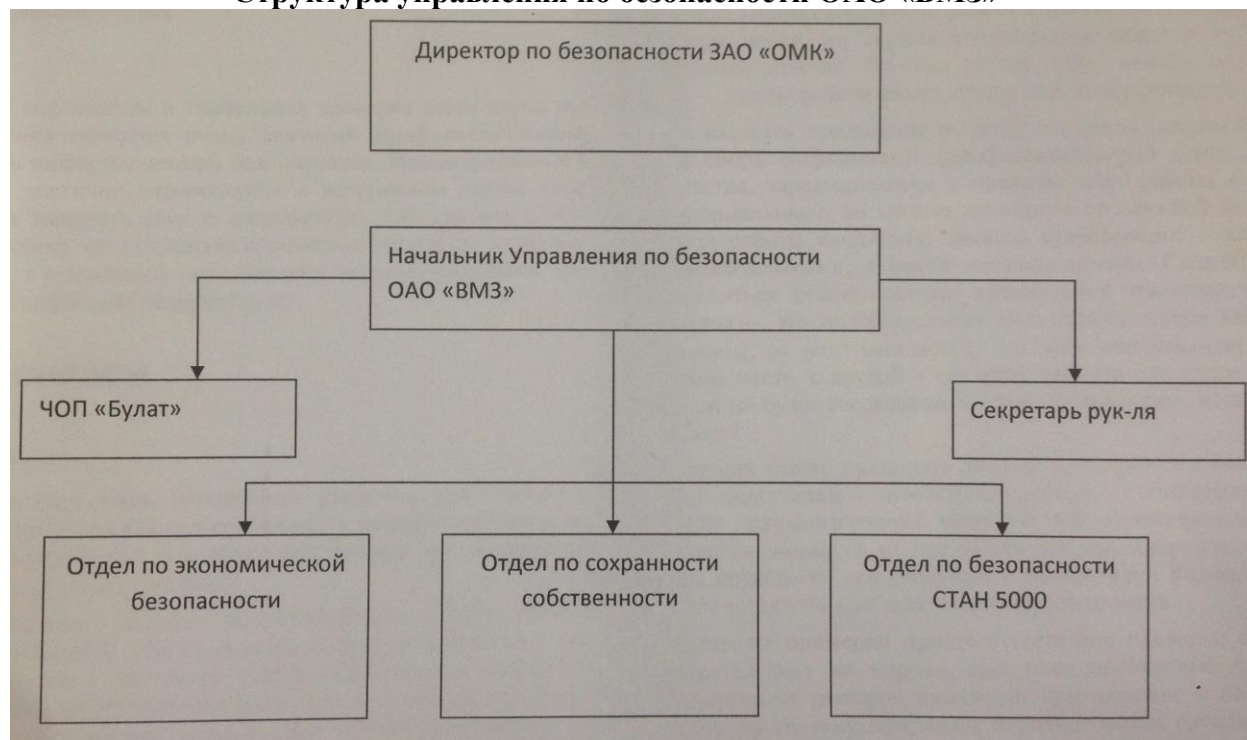
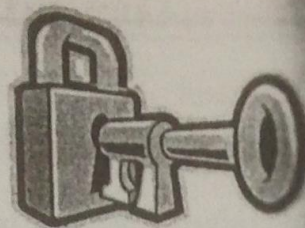


Рис. 14. Структура и задачи службы безопасности.

Структура управления по безопасности ОАО «ВМЗ»



Глава 26



Работа с персоналом и оборудованием

Методическая работа с персоналом и тщательная проверка всего парка используемого оборудования являются очень важными профилактическими мероприятиями в плане информационной безопасности. Рассматриваемые в данной главе вопросы частично пересекаются с материалом других глав, однако авторы решили выделить данное направление. Это связано с тем, что речь в основном пойдет не о специализированных продуктах информационной безопасности, а о знакомых каждому пользователю принтерах, мониторах и другом неспецифичном оборудовании.

Работа с персоналом

Общие вопросы

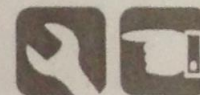
Говоря о безопасности персонала, необходимо разделять два понятия — безопасность самого персонала как человеческого и информационного ресурса и защиту от персонала как источника или основы злоумышленных воздействий на информационные системы.

Вопросам защиты персонала в случаях стихийных бедствий будет уделено внимание в *главе 31*. Нападения, угрозы, шантаж и прочие воздействия злоумышленников на персонал — это объект уголовного права и в общем случае находится в компетенции уполномоченных государственных органов, с которыми служба информационной безопасности организации может сотрудничать, в любом случае играя второстепенную роль. Для конкретной организации ситуация может быть иная, и такие вопросы будут решаться собственной службой безопасности, однако все равно используемые в данном случае оперативные, розыскные и иные мероприятия выходят за рамки книги.

Иной взгляд авторы имеют на персонал как возможный источник злонамеренных воздействий на информационную безопасность предприятия либо, когда некомпетентность, ошибки, халатность или иные действия персонала

послужили основой для угрозы безопасности организации. Причем угрозы безопасности по причине некомпетентности и низкой квалификации персонала в зависимости от региона, социального состава и других причин, могут иметь значимость не меньшую, а иногда и большую, чем угрозы безопасности по причине злого умысла.

Прием на работу



Начало анализа персонала начинается, соответственно, с этапа приема на работу. Подразделение по работе с персоналом имеет собственные критерии отбора людей, но служба безопасности может и должна принимать в этом активное участие. На наш взгляд, такая оценка складывается из двух частей — предыдущего опыта и текущей квалификации.

Что касается предыдущего опыта, то здесь должны быть отработаны системы сбора информации (профессиональный опыт, знания, персональные качества, характеристики с прежних мест работы как официальные, так и неформальные), возможно, контакты со службой безопасности с прежнего места работы кандидата; анализа информации — какие качества являются положительными, а какие отрицательными. Скажем, готовность кандидата поделиться особенностями организации производства на прежнем месте работы — это положительная или отрицательная характеристика? С одной стороны, от него ожидается, что весь накопленный опыт он применит на новом месте, с другой — где гарантия, что при очередной смене места работы он не будет рассказывать о той организации, куда теперь принимается на работу?

Текущий статус кандидата должен проверяться с точки зрения его технической подготовки и способности работать с информационными системами, а также психологического склада и черт характера для выявления тенденций развития личности (в том числе как злонамеренных, так и просто создающих неудобства при общении в коллективе). Возможно участие в этом процессе штатного или приглашенного психолога.

Одним из примеров простого теста для проверки способностей кандидата является тест на пароль. Для него необходимо небольшое программное обеспечение, которое имитирует приглашение к вводу пароля в информационную систему, сохраняет пароль и может продемонстрировать его представителю службы безопасности. Возможно, перед испытанием кандидату следует дать ознакомиться с требованиями организации к паролям пользователей. Далее кандидату предлагается придумать и ввести собственный пароль (например, мотивируя тем, что ему будет предоставлена возможность тестовой работы в системе). После ввода пароля можно попросить кандидата еще раз войти в систему, но при этом система выдаст ему сообщение об ошибке с предложением обратиться в службу безопасности, либо сообщит, например, что время его последнего входа не соответствует тому, ко-

торое реально было сделано только что, или что со времени последнего входа было две-три попытки ввода неверного пароля. Настораживающими факторами в данном случае являются следующие.

- Слишком долгие размышления по придумыванию пароля. Комбинация из букв, цифр и спецсимволов нормальный пользователь с опытом работы в информационных системах сможет придумать за 30—60 секунд, либо вообще использовать один из своих старых паролей. Долгие раздумья скорее всего означают, что кандидат впервые сталкивается с такими требованиями к безопасности и, возможно, в дальнейшем он будет испытывать трудности с их соблюдением. Правда, долгие раздумья могут означать, что он действительно изобретает сложный пароль, но это, возможно, будет проверять после его ввода.
- Попытки запроса подсказок пароля типа "Помогите мне подобрать пароль". Это означает, что пользователь не осознает важность сохранения пароля в секрете. Дополнительной проверкой может послужить промывка проверяющего, например: "Скажите, какой пароль вы сейчас вводили?" — ведь кандидат предупрежден, что получает вход в систему, пусть и в тестовом режиме.
- Ошибки при подтверждении пароля. Если пользователь не может сосредоточиться настолько, чтобы два раза ввести одинаковую комбинацию из 10—15 символов, то это может быть негативным знаком. При этом следует делать поправку на возможное волнение кандидата при проверке.
- Слишком простой введенный пароль. Если кандидат, ознакомившись с требованиями организации к паролям, все же игнорирует их, надеясь, что пароль не будет никому известен, то это также негативная тенденция.
- Отсутствие реакции на тревожные сообщения системы при последующем входе в нее. Если система проинформировала пользователя об ошибке при вводе пароля, а затем пропустила его, а также дала неверную дату/время последнего входа или сообщила о неверных вводах пароля, которых не было со стороны пользователя, — это важные сигналы, о которых кандидат должен проинформировать службу безопасности.

Если кандидат принят на работу и становится реальным пользователем субъектом информационного пространства, то служба информационной безопасности должна обеспечить себе правовое пространство для дальнейшей работы с данным пользователем, в том числе для случаев возможного преследования данного пользователя при выявлении с его стороны нарушений. Для этого необходимо произвести следующие мероприятия.

- Ознакомить с существующими нормативами (правилами, инструкциями, методическими указаниями и т. п.) в сфере информационной безопасности и обеспечить уверенность, что в дальнейшем он не сошлется на их незнание, в том числе взять подписку.

Если кандидат заключит с организацией контракт, то в него без сомнения должен войти ряд положений по информационной безопасности, особенно если они не отражены адекватно в законодательстве государства. Например, что субъект обязуется признавать цифровую подпись руководителя наравне с обычной подписью на бумаге.

Если организация выдвигает повышенные требования к сохранению конфиденциальности своей информации, возможно, это также необходимо включить в список подписываемых субъектом положений. При этом следует соблюдать действующее законодательство страны, с тем чтобы возлагаемые на субъекта обязательства не нарушали его конституционных прав.

Если организация собирается использовать элементы вмешательства в частные разделы рабочей деятельности сотрудника, например, регулярно или выборочно перлюстрировать его электронную почту или отслеживать посещения интернет-сайтов, то работник должен быть как минимум об этом предупрежден.

Если сотруднику предоставляется в его распоряжение персональный компьютер, то необходимо довести до сотрудника, что данная единица техники остается собственностью организации, а значит, организация будет определять политику его использования. При этом установка на компьютер игр, обучающих программ, музыки и видеофильмов чаще всего не входит в цель организации. А поскольку данный сотрудник становится ответственным за данный компьютер, он должен обеспечивать в рамках своих возможностей соответствие требованиям нормативов, в том числе по информационной безопасности.

Если за данным персональным компьютером будет работать два и более человек, то целесообразно назначить одного, наиболее подготовленного, ответственным за (или контролирующим) соблюдение требований информационной безопасности на данном компьютере.

Методическая работа с персоналом



Несмотря на любую квалификацию пользователя, поскольку развитие информационного пространства предприятия не стоит на месте, необходимо регулярное обучение сотрудников как работе в новых информационных системах, так и мерам безопасности в этих системах. Кроме того, развитие технической части мирового информационного пространства может порождать от пользователей дополнительные более или менее квалифицированные знания по ряду аспектов (например, как в случае с известным вирусом «Nimikova» — отличать расширения jpg от jpg.vbs). Это означает, что следует разрабатывать систему оперативного оповещения сотрудников о необходимых мероприятиях, а также возможное проведение регулярных семинаров для наиболее подготовленной части сотрудников. Для больших, рас-

пределенных корпораций желательно применять способ подготовки персональных методических материалов, их рассылки и обязательного ознакомления сотрудников с ними.

Как бы старательно и качественно не работали сотрудники, периодически приходится проверять их деятельность. Проверки могут быть выборочными или регулярными, их диапазон может простираться от анализа регистрационных журналов данной конкретной информационной системы до полного сканирования содержимого жесткого диска и внешних носителей пользователя. При таких проверках, по всей видимости, будут периодически обнаруживаться какие-то нарушения в работе пользователей, в том числе и в их вине. О том, как производится расследование инцидентов, речь пойдет в главе 33, а вот степень зависимости вины пользователя в том или ином нарушении и размер наказания должны определить уполномоченные лица конкретной организации.

Хотелось бы дать один совет: не всегда суровое наказание даже за маленький проступок — это хорошее решение проблемы. По опыту известно, что даже при информированности пользователей о том, что их деятельность — это предмет наблюдения соответствующих служб, значительная часть из них все равно будет пытаться искать мелкие выгоды для себя в процессе своей рабочей деятельности. Возможно, это будет посещение развлекательных сайтов в Интернете или установка компьютерных игр. В таких случаях напоминание в виде электронного письма с примерным содержанием: *«Вы посетили сайт www.xxx.com и провели на нем 42 минуты рабочего времени. Рекомендуем вам во избежание неприятностей не посещать сайты, не связанные с вашей рабочей деятельностью. Служба безопасности»* — будет хорошей профилактикой развития злоупотребления корпоративными ресурсами.

Однако даже если данный незначительный инцидент формально «прошлет», тем не менее он должен быть зафиксирован в некоем «черном списке», куда вносятся все нарушения информационной безопасности пользователей с первого дня работы. Такой документ полезен, во-первых, поскольку пользователи склонны забывать о своих нарушениях (в этом случае данный документ будет полезен при некоем переполнении списка мелких нарушений условно прощенных для этого пользователя). Во-вторых, с помощью данного документа можно отслеживать тенденции в развитии работы пользователя с точки зрения информационной безопасности.

Мелкой, но тем не менее важной деталью является вопрос идентификации работника при межличностном общении. В организации, насчитывающей несколько десятков человек, специалист по безопасности может знать каждого сотрудника лично, но в большой организации, где персонал составляет 1000 и более человек, вопросы распознавания личности, особенно для новых работников, станут уязвимостью, которая может быть использована, например, средствами социальной инженерии, о которой шла речь в главе 10.

Ближайшим примером является обращение пользователя по телефону с просьбой замены пароля той или иной причине. Каким образом проверить соответствие реально пользователя названному `username`? Если пользователь находится неподалеку, наиболее простой способ — пригласить его прибыть к администратору с документами, подтверждающими личность. Кстати, для этих целей хошим корпоративным стандартом считается ношение на груди опознавательного пропуска с необходимой информацией (желательно продумать меры воспрепятствования их подделке). Но что, если пользователь географически удален от администратора, а вопросы бизнеса требуют обеспечения быстрого начала работы в информационной системе? В этом случае встает в действие система временных паролей для однократного входа (с немедленной заменой), для которой в Интернете разработаны два основных варианта решения проблемы.

- Контрольный вопрос. При регистрации в учетную запись пользователя, доступ к которой есть только у администратора, заносится вопрос и соответствующий ответ, которые известны только данному пользователю. Таким образом, перед сменой пароля администратор аутентифицирует пользователя по ответу на контрольный вопрос. Если система позволяет, следует сохранять несколько вопросов для одного пользователя, также следует заменять вопросы, после их использования.
- Альтернативная обратная связь. После обращения пользователя администратор фиксирует номер телефона и, проверив корректность номера, перезванивает пользователя сам. Кроме того, временный пароль высылается пользователю по электронной почте, возможно, даже не самому пользователю, а его непосредственному руководителю.

Следует только учесть важность того, чтобы временный пароль был достаточно уникальным, с тем чтобы в каждый конкретный момент не было известно о том, какой временный пароль использован для данного работника.

Бывший кадровый состав предприятия



Другой важный момент — взаимоотношения с сотрудником, который собирается покинуть организацию. Естественно, должны быть проведены некоторые технические мероприятия по блокированию или удалению учетных записей данного сотрудника как пользователя информационных систем. Но для этого служба безопасности как минимум должна быть оповещена о предстоящем увольнении сотрудника. Также в этой ситуации необходим контакт с подразделением, работающим с персоналом.

Для ряда увольняющихся сотрудников, а возможно и для всех, целесообразно проводить собеседования в ходе которых напомнить о продолжении действия обязательств, взятых на себя сотрудником по отношению к организации (если заключены контракты и договоренности не теряют своей силы при увольнении сотрудника). Возможно, остаются еще какие-либо

дополнительные заинтересованности уходящего сотрудника в организации. В любом случае предпочтительнее сохранить хорошие отношения между уходящим сотрудником и организацией.

Служба безопасности организации должна решить, как она будет поступать с запросами на характеристики бывших сотрудников организации, устраивающихся на работу на новое место. Возможно, предприятие считает, что оно не должно предоставлять такие сведения, но тогда следует учесть, что и на аналогичный запрос самого предприятия на нового кандидата может прийти отказ в ответе. По общим соображениям целесообразнее организовать взаимодействие между службами безопасности предприятий отрасли, предварительно определив перечень данных, которые могут быть сообщены коллегам. Подобное сотрудничество при правильной организации позволит только улучшить состояние информационной безопасности отдельных предприятий.

Работа с оборудованием



Безопасность оборудования также складывается из вариантов, когда оборудование само представляет угрозу и когда оборудование является объектом на который направлена угроза.

Когда организация приобретает оборудование информационных технологий, она вынуждена ему доверять, так как в большинстве случаев организация не имеет достаточного количества ресурсов для анализа сложной техники на отсутствие недокументированных возможностей — *аппаратных закладок* (англ. *hardware backdoor*). Причины возникновения таких закладок — это вопрос конкуренции между предприятиями или политики отдельных государств, но в любом случае он вне рассмотрения данной книги. Даже если в организации присутствуют квалифицированные специалисты по информационным технологиям или информационной безопасности, они не возьмут на себя смелость подтверждать или опровергать наличие аппаратных закладок. В отличие от методик и средств обнаружения программных закладок в большинстве случаев для анализа аппаратного обеспечения необходимы специальные лаборатории и персонал отдельной высокой квалификации.

По этой причине оборудование необходимо приобретать только после сертификации уполномоченным органом государства, либо если таковой организации отсутствует — у известных производителей (брендов), которые дорожат репутацией и не заинтересованы в скандалах по поводу аппаратных закладок в их технике. В данном случае увеличение цены оборудования — это плата за гарантию отсутствия "пятой колонны" внутри предприятия.

Если предположить, что в оборудовании нет встроенных со злым умыслом недокументированных возможностей, в нем тем не менее может присутствовать

повышать уязвимость для информационной безопасности. Чаще всего в связи с такой уязвимостью употребляют термин *ПЭМИН* — *побочное электромагнитное излучение и наводки* (англ. *side-channel*). Данное явление основывается на том, что при своей работе оборудование выделяет в окружающее пространство неконтролируемым образом некоторую информацию в том или ином виде, причем эту информацию можно перехватить, обработать и использовать несанкционированным образом. Наибольшее внимание в информационных технологиях привлекают ПЭМИН, возникающие в средах передачи данных (проводах, кабелях и т. д.) и генерируемые при работе мониторов пользователей. Однако прежде чем приобретать сложное и дорогостоящее оборудование для защиты от ПЭМИН следует произвести анализ рисков.

- 3. Возможно, достаточно обеспечить шифрование данных при передаче по линиям связи, в этом случае не только сложная аппаратура улавливания электромагнитных наводок, но и прямое внедрение перехватчика пакетов ничего не даст злоумышленнику.
- 4. Для удаленного перехвата информации с экрана монитора требуется очень дорогостоящее и сложное оборудование. А что получит самый злобный конкурент, если он даже сможет заглядывать через плечо наиглавнейшему системному администратору? Возможно, он сможет получить эту информацию более легким и простым путем.

Следует учесть, что обычно анализируются риски для среднего предприятия. Если говорить, например, об учреждениях министерства обороны, где в электронном виде хранится информация класса "государственная тайна", рассуждения будут, конечно, совсем другими.

Вспустим, обеспечена ситуация, когда все оборудование организации функционирует надежным и доверенным способом. Однако присутствует возможность внедрения в информационное пространство предприятия постоянного оборудования, принесенного сотрудниками и посетителями.

В данном случае оборону необходимо эшелонировать двумя ступенями: контролировать внос оборудования в здание организации и проверять отсутствие посторонних включений в информационную сеть. И для первого, и для второго способов существуют различные средства и методы — от визуального осмотра до автоматизированного обнаружения.

Особого внимания заслуживают в данном случае внешние носители (которые также можно отнести к оборудованию), а также средства для чтения/записи на внешние носители и порты для внешнего подключения таких устройств. В данном случае внешние носители могут быть средством поставки зловредных информационных объектов/субъектов в информационное пространство предприятия и средством изъятия конфиденциальной информации из информационных объектов предприятия.

Наиболее надежным, хотя и непростым решением будет физическое отключение/удаление устройств считывания/записи и блокировка/отключение свободных портов (COM, LPT, USB, инфракрасная связь и т. п.). При этом необходимо создание отдельной службы, в распоряжении которой останутся одно или несколько устройств работы с внешними носителями. Физически размещать эту службу целесообразно недалеко от входа в здание, с тем чтобы все вносимые и выносимые внешние носители могли быть представлены ее сотрудникам. В функции службы будет входить:

- ☐ проверка отсутствия на принесенном внешнем носителе зловредных элементов (вирусов, троянских программ, постороннего программного обеспечения);
- ☐ копирование или электронная доставка информации с принесенного внешнего носителя на рабочую станцию или сервер, в распоряжение того пользователя, для которого информация предназначена;
- ☐ получение от пользователя информации, предназначенной к выносу из организации на внешнем носителе;
- ☐ проверка отсутствия в информации для выноса конфиденциальных данных и запись информации на внешние носители.

Единственным допустимым исключением для этой службы может быть только служба регулярного резервного копирования критической информации с отдельным регламентом работы.

Заканчивая разговор о внешних носителях, необходимо упомянуть о проблеме стирания информации с внешних носителей, после того как информация была доставлена по назначению. Вопрос затрат на возможное восстановление якобы уничтоженной информации с внешнего носителя, — это вопрос стоимости самой информации, которую необходимо восстановить. В любом случае следует учесть, что многократная перезапись или физическое разрушение корпуса или даже записываемой поверхности — это еще не гарантия невозможности восстановления. Если вопрос о гарантировании уничтожении информации достаточно острый, то следует проанализировать возможность приобретения специальной аппаратуры. При этом необходимо различать аппаратуру с полным разрушением внешнего носителя и с возможностью его последующего использования.

Другой важной особенностью оборудования информационных технологий является наличие большого количества мелких деталей, которые обладают рядом неприятных для информационной безопасности качеств:

- ☐ они самоценны, т. е. имеют отдельную стоимость по отношению к основному оборудованию;
- ☐ соотношение цена/масса/размер некоторых деталей в определенные периоды развития рынка превышает аналогичное соотношение, например даже для золота;

- они могут быть заменены на похожие детали худшего качества и меньшей стоимости, при этом замена не будет очевидна для конечного пользователя;
- они пользуются устойчивым спросом на рынках, где не требуются документы, подтверждающие легальное происхождение данных деталей.

Более ярким примером в данном случае могут быть платы оперативной памяти. Только квалифицированный пользователь сможет заметить отличие в работе компьютера с 128 или с 96 Мбайтами оперативной памяти. Таким образом, пропаша или подмена может быть не выявлена достаточно долго, до очередной подробной инвентаризации (при отсутствии автоматизированных средств инвентаризации). Приемлемым средством снижения данного риска будет использование кожухов для сокрытия мелких деталей (практически у всего оборудования такие кожухи присутствуют) и опечатывание кожухов печатью уполномоченного подразделения — скажем, информационной безопасности или технической поддержки. При этом важно, чтобы целостность печати регулярно проверялась самим пользователем оборудования, в противном случае эта мера будет носить лишь фиктивный характер.

Угрозы и уязвимости информационной системы ОАО «ВМЗ»

Угроза	Уязвимости
1. Автоматизированное рабочее место сотрудника.	
1. Физический доступ нарушителя к рабочему месту.	1. Отсутствие системы контроля доступа сотрудников к чужим рабочим местам. 2. Отсутствие системы видеонаблюдения на предприятии.
2. Разглашение конфиденциальной информации, хранящейся на рабочем месте сотрудника организации.	1. Отсутствие соглашения о неразглашении между работником и работодателем. 2. Нечеткая регламентация ответственности сотрудников предприятия.
3. Разрушение (повреждение, утрата) конфиденциальной информации при помощи специализированных программ и вирусов.	1. Отсутствие ограничения доступа пользователей к сети интернет и к внутренней корпоративной сети.
2. Конфиденциальная информация.	
1. Физический доступ нарушителя к носителям.	1. Неорганизованность контрольно-пропускного режима в организации. 2. Отсутствие видеонаблюдения в организации.
2. Разглашение конфиденциальной информации, используемой в документах, вынос носителей за пределы контролируемой зоны.	1. Отсутствие соглашения о неразглашении конфиденциальной информации 2. Нечеткое распределение ответственности за документы (носители конфиденциальной информации) между сотрудниками организации.
3. Несанкционированное копирование, печать и размножение носителей конфиденциальной информации.	1. Нечеткая организация конфиденциального документооборота в организации. 2. Неконтролируемый доступ сотрудников к копировальной и множительной технике

Инструкция о порядке действий в нештатных ситуациях

Общие положения

[min] Настоящая инструкция предназначена для организации порядка действий при возникновении нештатных ситуаций.

[min] Инструкция регламентирует действия персонала подразделений при возникновении нештатных ситуаций.

Инструкция разработана на основе (*указать документы, в том числе по пожарной безопасности и гражданской обороне, соответственно включить оттуда разделы*).

Общий порядок действий при возникновении нештатных ситуаций

[min] При возникновении нештатных ситуаций во время работы ЭВМ сотрудник, обнаруживший нештатную ситуацию немедленно ставит в известность своего администратора информационной безопасности.

[min] Администратор информационной безопасности проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего начальника и вызывает сотрудника (*указать, например, отдела информатизации или отдела технической защиты информации*) подразделения банка для дальнейших действий.

[MAX] По факту возникновения нештатной ситуации составляется акт, с описанием ситуации. К акту прилагаются, если есть, поясняющие материалы (копии экрана, распечатка журнала событий и др.)

[MAX] При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

[MAX] Особенности действий при возникновении наиболее распространенных нештатных ситуаций.

Сбой программного обеспечения. Администратор информационной безопасности совместно с сотрудником (*указать*) отдела выясняют причину сбоя ПО. Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а так же файлов, если это необходимо) направляются разработчику ПО.

Отключение электричества. Администратор информационной безопасности совместно с сотрудником (*указать*) отдела проводят анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных

из последней резервной копии с составлением акта.

Сбой в локальной вычислительной сети (ЛВС). Администратор информационной безопасности совместно с сотрудником (*указать*) отдела проводят анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

Выход из строя сервера. Сотрудник, ответственный за эксплуатацию сервера, совместно с (*указать*) проводит меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы банка. При необходимости производятся работы по восстановлению ПО и данных из резервных копий с составлением акта.

Потеря данных. При обнаружении потери данных администратор информационной безопасности совместно с (*указать*) проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

Обнаружен вирус. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником.

Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ банка с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий с составлением акта. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС) банка.

Обнаружена утечка информации (дырка в системе защиты). При обнаружении утечки информации ставится в известность администратор информационной безопасности и начальник подразделения. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

Взлом системы (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера ставится в известность администратор информационной безопасности и начальник подразделения. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий с составлением акта. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС банка, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ банка. По факту взлома сервера проводится служебное расследование.

Попытка несанкционированного доступа (НСД). При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

Компрометация ключей. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

Компрометация пароля. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.). При необходимости, проводится служебное расследование.

Физическое повреждение ЛВС или ПЭВМ. Ставится в известность администратор информационной безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное

расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться документами (*указать*) для соответствующих подразделений банка.

Профилактика против возникновения нештатных ситуаций

[min] *Отделом технической защиты информации (или указать)* периодически, не реже (*указать период*), должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

[min] В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов банка и инструкций по эксплуатации оборудования и ПО.

[MAX] Ниже приведены рекомендации по предотвращению некоторых типичных нештатных ситуаций.

Сбой программного обеспечения. Применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.)

Отключение электричества. Использовать источники бесперебойного питания на ответственных (а лучше - на всех) технологических участках банка. Разработать инструкцию по аварийному переходу на резервный источник питания (если такой имеется в наличии) или аварийному завершению работы и сохранению данных. Желательно иметь в наличии резервный источник электроэнергии (дизель- генератор и др.)

Сбой ЛВС. Обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем.

Выход из строя сервера. Применять надежные программно-технические средства, продуманную политику администрирования. Допускать к работе с серверным оборудованием только квалифицированных специалистов.

Потеря данных. Периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администраторами информационной безопасности (и сотрудниками) разъяснительные и обучающие собрания. Обеспечить комплексную защиту информации в банке.

Обнаружен вирус. Соблюдать требования «Инструкции по организации антивирусной защиты».

Обнаружена утечка информации (дырка в системе защиты). Применять обновления ПО по устранению программных «дыр» в системе защиты по мере их появления (обнаружения). Построить комплексную систему защиты информации в банке. Регулярно проводить анализ журналов попыток НСД и совершенствование системы защиты информации. Также См. «Потеря данных»

Взлом системы (Web-сервера, файл-сервера и др.) или несанкционированный доступ (НСД). См. «Обнаружена утечка информации (дырка в системе защиты)».

Попытка несанкционированного доступа (НСД). По возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением Администратора информационной безопасности о попытках НСД.

Компрометация ключей. Соблюдать требования «Инструкции по обращению с ключевыми материалами шифрования и ЭЦП».

Компрометация паролей. Соблюдать требования «Инструкции по организации парольной защиты».

Физическое повреждение ЛВС или ПЭВМ. Физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним. С также «Сбой ЛВС».

Стихийное бедствие. Проводить обучающие собрания и тренировки персонала банка по вопросам гражданской обороны.

Инструкция по работе с эталонным программным обеспечением (ПО)

Порядок получения ПО от разработчика

[min] Все программное обеспечение (ПО), получаемое от разработчика должно быть подвергнуто антивирусной проверке.

[min] С полученного ПО необходимо изготовить рабочие копии, которые будут использоваться для установки и работы ПО. Исключения составляют носители информации, с которых невозможно изготовить копии по причине их защиты от копирования или невозможности изготовления копии.

[min] Носители информации оригинала (эталона), и копий ПО должны быть маркированы и учтены в подразделении (*указать*) банка.

[MAX] С эталона ПО необходимо снять значения хеш-функций для контроля целостности информации и зафиксировать эти значения в акте приема-передачи и формуляре носителей ПО.

[MAX] Для получения хеш-функций применяется программа CRC.EXE из состава операционной системы PC DOS 7.0 (*или указать программу*).

[min] С поступающими обновлениями ПО, в процессе его сопровождения разработчиком, необходимо поступать так же, как и с первоначальной версией ПО.

Проверка целостности эталонного ПО

[MAX] Перед повторным созданием рабочих копий необходимо проверить значения хеш-функций эталонного ПО для подтверждения его целостности.

Хранение эталонного ПО

[min] Эталонное ПО должно храниться в специально предназначенном для этой цели месте. Место хранения эталонного ПО должно исключать возможность резких перепадов температур, влияние сильных электромагнитных полей, прямых солнечных лучей, а также других явлений, способных привести к разрушению эталонной информации и (или) ее носителей.

[MAX] Эталонное ПО должно храниться на маркированных учтенных носителях информации. На каждый носитель информации должен быть составлен формуляр с описанием содержимого носителя информации. Формуляр должен содержать следующую информацию: наименование ПО, состав ПО и его хеш-функции, ФИО лица, производящего проверку и регистрацию ПО, дату регистрации ПО.

[min] Носители информации, для хранения эталонного ПО должны быть переведены с состояния «только чтение» или «защита от записи», если иное не предусмотрено документацией на ПО.

[min] Документация по установке эталонного ПО должна храниться вместе с ним.

Установка ПО

[min] Установка и настройка ПО производится только с рабочих копий ПО, за исключением случаев, когда изготовление копий невозможно.

[MAX] Установка (изменение) программного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только в присутствии и под контролем администратора информационной безопасности (АИБ) того технологического участка, в котором эксплуатируется данное программное обеспечение.

[MAX] Установка ПО производится с составлением акта установки.

Обновление ПО

[min] Обновление ПО производится в соответствии с сопроводительной документацией на пакет обновления и регистрируется в специальном журнале изменения ПО.

Положение об администраторах информационной безопасности (АИБ)

Общие положения

Настоящее Положение определяет задачи, функции, обязанности, права и ответственность администратора информационной безопасности (АИБ).

[MAX] АИБ назначается Приказом по банку из числа сотрудников, задействованных на данном технологическом участке (отдел информатизации, РКЦ, и др.). Технологический участок, на котором назначается АИБ должен быть четко определен в Приказе.

[MAX] АИБ подчиняется руководителю подразделения, в котором он состоит.

[min] АИБ в своей работе руководствуется настоящим Положением и другими нормативными документами банка (перечислить).

[min] Инструктивно-методическое руководство деятельностью АИБ осуществляется *Отделом технической защиты информации (ОТЗИ)* банка (или указать др.)

[min] АИБ в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в своем подразделении.

[min] АИБ устанавливается надбавка к заработной плате в размере до (*указать*).

Основные задачи и функции администратора информационной безопасности

Основными задачами АИБ являются:

[min] Организация эксплуатации технических и программных средств защиты информации.

[min] Текущий контроль работы средств и систем защиты информации.

[MAX] Контроль за работой пользователей автоматизированных систем, выявление и регистрация попыток несанкционированного доступа (НСД) к автоматизированным системам и защищаемым информационным ресурсам.

[MAX] Организация и контроль резервного копирования в подразделении.

АИБ выполняет следующие основные функции:

[min] Обеспечение функционирования средств и систем защиты информации в пределах инструктивно-методических документов (*указать*).

[min] Обучение персонала и пользователей вычислительной техники правилам безопасной обработки информации и правилам работы со средствами защиты информации.

[MAX] Обучение персонала и пользователей вычислительной техники правилам безопасной обработки, передачи и хранения информации при помощи автоматизированных систем.

[min] Участие в проведении служебных расследований, фактов нарушения или угрозы нарушения безопасности защищаемой информации.

[min] Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих из других подразделений и сторонних организаций.

[min] Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

[MAX] Текущий контроль технологического процесса автоматизированной обработки информации ограниченного распространения и электронных платежных документов.

[min] Организация учета и хранения носителей электронных ключей с грифом "Для служебного пользования", используемых в технологии обработки защищаемой информации.

[min] Текущий контроль за соблюдением требований инструкций и положений при эксплуатации средств и систем защиты информации.

[MAX] Контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нем.

[min] Контроль за санкционированным изменением ПО, заменой и ремонтом средств вычислительной техники на своем технологическом участке.

Обязанности администратора информационной безопасности

[min] Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на него обязанностей.

[min] Немедленно докладывать непосредственному начальнику, а в его отсутствии начальнику (*указать*), о выявленных нарушениях и несанкционированных действиях пользователей и персонала, а также принимать необходимые меры по устранению нарушений.

[min] Совместно со специалистами *ОТЗИ* принимать меры по восстановлению работоспособности средств и систем защиты информации.

[min] Проводить инструктаж обслуживающего персонала и пользователей средств вычислительной техники по правилам работы с используемыми средствами и системами защиты информации.

Права администратора информационной безопасности

[min] Требовать от пользователей банковских автоматизированных систем безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

[min] Вносить предложения и требовать прекращения обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации.

[MAX] Обращаться в *ОТЗИ* с просьбой об оказании технической и методической помощи в работе по обеспечению технической защиты информации.

[MAX] Готовить предложения в *ОТЗИ* по совершенствованию используемых систем защиты информации и отдельных их компонентов.

Ответственность администратора информационной безопасности

[min] На АИБ возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными в настоящем Положении.

[MAX] АИБ несет ответственность по действующему законодательству за разглашение сведений, составляющих государственную тайну и сведения ограниченного распространения, ставших известными ему в соответствии с родом работы.

Инструкция о резервном копировании информации

Периодичность резервного копирования данных

[min] Резервное копирование данных должно производиться в соответствии с графиком резервного копирования.

[min] График резервного копирования должен быть составлен для каждого вида информации, подлежащей периодическому резервному копированию и утвержден (начальником структурного подразделения).

[min] Для каждого вида информации в соответствии с графиком резервного копирования должны быть назначены лица, ответственные за резервное копирование данной информации.

Порядок резервного копирования данных

[min] Резервное копирование информации производится в соответствии с документацией на используемое программное обеспечение.

[MAX] (*дописать свои пункты*).

Хранение резервных копий данных

[min] Резервные копии данных должны храниться вместе с инструкцией по восстановлению данных из резервных копий.

[min] Хранение резервных копий должно быть организовано в отдельном помещении (или комнате) от используемых данных.

[MAX] (*дописать свои пункты*).

Восстановления ПО и данных после сбоя

[min] Восстановление ПО из резервной копии производится в соответствии с документацией на используемое программное обеспечение с составлением акта.

[MAX] *(дописать свои пункты).*

«УТВЕРЖДАЮ»
Генеральный директор
ОАО «Пример»
.....А. Королев
20 января 2006 года
М.П.

ПОЛОЖЕНИЕ
о коммерческой тайне
Открытого акционерного общества
«П р и м е р»

**Нижний Новгород,
2006**

Статья 7. Обязанности работников Общества, допущенных к документам, содержащим сведения конфиденциального характера.

1. Передача документов от одного работника к другому осуществляется под роспись в журнале выдачи документов, содержащих сведения конфиденциального характера (Коммерческую тайну Общества).

1 Работникам Общества ЗАПРЕЩАЕТСЯ:

✓ сообщать устно или письменно кому бы то ни было, сведения конфиденциального характера (коммерческую тайну Общества), если это не вызвано служебной необходимостью;

✓ использовать документы, содержащие сведения конфиденциального характера, в корыстных целях в качестве конкурентного действия соперничающих юридических лиц;

✓ выполнять работу с документами, содержащими сведения конфиденциального характера, на дому;

✓ выносить документы, содержащие сведения конфиденциального характера, Из помещений Общества, снимать с них копии или производить выписки без письменного разрешения Генерального директора Общества;

✓ вести служебные междугородные или международные переговоры по незащищенным каналам связи по вопросам, содержащим сведения конфиденциального характера;

✓ использовать документы, содержащие сведения конфиденциального характера, в целях раскрытия их в средствах массовой информации;

✓ обрабатывать документы, содержащие сведения конфиденциального характера, на персональном компьютере без осуществления мер, обеспечивающих защиту от несанкционированного доступа к таким документам.

Статья 8. Учет, хранение, обращение и уничтожение документов (носителей), составляющих коммерческую тайну Общества.

1. Учет входящих, внутренних и исходящих документов, содержащих сведения конфиденциального характера, осуществляется по журналам учета (реестрам).

Листы журналов (реестров) должны быть пронумерованы, прошнурованы и г креплены печатью Общества.

2. В журналах учета (реестрах) отражаются данные о движении документов, содержащих сведения конфиденциального характера, с момента их получения (ПОДГОТОВКИ) ДО завершения исполнения и подшивки в дело, отправки адресатам или уничтожения.

Передача Документов работникам осуществляется под роспись в соответствующем журнале (реестре).

3. Дополнительно размноженные экземпляры документа, содержащего сведения конфиденциального характера, учитываются за этим же номером, о чем делается отметка на размноженном документе.

На каждом отпечатанном экземпляре такого документа проставляется в левом верхнем углу регистрационный номер, в правом гриф «Коммерческая тайна», Полное фирменное наименование и место нахождения Общества.

4. Электронные носители (дискеты, диски, флэш-карты и другие) предназначенные для записи сведений конфиденциального характера, учитываются в соответствующих журналах (реестрах).

5. Документы, содержащие сведения конфиденциального характера, должны храниться в опечатываемых металлических шкафах или сейфах.

6. В случае хищения или утраты документов, содержащих сведения конфиденциального характера, Генеральный директор Общества должен назначить служебное расследование.

7. При уничтожении документов, утративших практическое значение, в журнале их учета (реестре) делаются заверительные подписи работника и Генерального

директора Общества.

Статья 9. Ответственность работников (контрагентов) Общества за разглашение (утрату), а равно передачу сведений конфиденциального характера.

1. Нарушение настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Работник Общества, который в связи с исполнением трудовых обязанностей, получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются Общество (работодатель) и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

3. Лицо, которое использовало информацию, составляющую коммерческую тайну Общества, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с Федеральным законом «О коммерческой тайне» быть привлечено к ответственности.

4. По требованию Общества - обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 3 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

5. Работники Общества несут персональную ответственность за соблюдение ими порядка работы с документами, составляющими коммерческую тайну Общества

6. Ответственность за сохранность информации, составляющей коммерческую тайну Общества, возлагается на заместителей Генерального директора и Главного бухгалтера Общества.

7. Степень ответственности за разглашение информации, составляющей коммерческую тайну Общества, определяется важностью разглашенных сведений и ущербом, нанесенным Обществу конкретным работником.

8. Для работника Общества наказание за незаконное получение и разглашение сведений, составляющих коммерческую тайну Общества, может выражаться в виде:

- ✓ замечания;
- ✓ выговора;
- ✓ лишения премии;
- ✓ возмещения через суд причиненных убытков, в соответствии с расчетом убытков, представленного потерпевшей стороной (Обществом);
- ✓ привлечения к уголовной ответственности в соответствии со статьей 183 Уголовного кодекса Российской Федерации за незаконное получение и разглашение сведений, составляющих коммерческую тайну Общества.

9. Контроль за выполнением требований настоящего Положения осуществляет Генеральный директор Общества.

Статья 10. Заключительные положения.

1. Настоящее Положение утверждается приказом Генерального директора Общества. Изменения и дополнения в настоящее Положение вносятся по решению Генерального директора Общества.

2. Если в результате изменения законодательства Российской Федерации отдельные статьи настоящего Положения вступают в противоречие с Законом, указанные статьи утрачивают силу и до момента внесения изменений и дополнений в настоящее Положение применяются нормы законодательства Российской Федерации.

3. Все приложения к настоящему Положению являются его неотъемлемой частью и имеют юридическую силу наравне с Положением.

Генеральный директор
ОАО «Пример»
Королев
М.П.

В.А.

Лекция

Требования РД ФСТЭК и ФСБ по организации защиты информации

План лекции:

1. Нормативно-технические документы по защите информации
2. Основные положения СТР-К. Классы защищённости СВТ, АС, МЭ, ПО СЗИ.
3. Требования РД по защите персональных данных.
4. Рекомендации по проведению аттестации объекта информатизации.

Основные документы

- ▣ Специальные требования и рекомендации по защите информации от утечки по техническим каналам (СТР-К)
- ▣ Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)
- ▣ Документы, устанавливающие критерии оценки защищенности информации (нормы эффективности защиты) и методы их контроля (в том числе при проведении сертификационных испытаний)
- ▣ РД. Показатели защищенности информации, обрабатываемой средствами ВТ и в АС, от НСД
- ▣ РД. Защита от несанкционированного доступа к информации. Общие технические требования
- ▣ Методики оценки защищенности информации от утечки по техническим каналам. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

Нормативно-методические документы по защите информации от НСД

- ▣ РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- ▣ РД. Концепция защиты СВТ и АС от несанкционированного доступа к информации.
- ▣ РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- ▣ РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- ▣ РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

Нормативные документы по защите ПД

- ▣ Порядок проведения классификации информационных систем персональных данных. (Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20)
- ▣ Приказ ФСТЭК №58 от 5.02.2010г. "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"
- ▣ Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.)
- ▣ Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.)
- ▣ Приказ ФСТЭК от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
- ▣ Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (УТВЕРЖДЕНЫ руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144)
- ▣ Типовые Требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (УТВЕРЖДЕНЫ руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622)
- ▣ Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (УТВЕРЖДЕН Руководством 8 Центра ФСБ России 08 августа 2009 года №149/7/2/6-1173)

Требования и рекомендации СТР-К распространяются на защиту:

- ▣ конфиденциальной информации - служебной тайны и информации с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным,
- ▣ а также информации о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющей идентифицировать его личность (персональные данные) *(В соответствии с Федеральным законом «О персональных данных»)*

РД определяет основные вопросы защиты информации:

- ▣ организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- ▣ состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- ▣ требования и рекомендации по защите речевой информации при осуществлении переговоров, в том числе с использованием технических средств;
- ▣ требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- ▣ порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- ▣ особенности защиты информации при разработке и эксплуатации автоматизированных систем, использующих различные типы средств вычислительной техники и информационные технологии;
- ▣ порядок обеспечения защиты информации при взаимодействии абонентов с информационными сетями общего пользования.

Защищаемые объекты информатизации

- ▣ средства и системы информатизации (средства вычислительной техники (СВТ), автоматизированные системы (АС) различного уровня и назначения на базе средств вычислительной техники, программные средства
- ▣ технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- ▣ защищаемые помещения.

Далее в СТРК-К определены:

- ▣ возможные каналы утечки и источники угроз безопасности информации
- ▣ способы перехвата информации или воздействия на нее с использованием технических средств,
- ▣ виды аппаратуры перехвата или воздействия на информацию и технические средства

РД, устанавливающие классы защищённости ОИ от НСД:

- ▣ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- ▣ Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации.

РД, устанавливающие классы защищённости ОИ от НСД:

- ▣ Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации.
- ▣ Защита информации. Специальные защитные знаки. Классификация и общие требования.
- ▣ Защита от несанкционированного доступа к информации. Часть 1 ПО средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей.

Классы защищённости от НСД к информации для АС определяются:

- ▣ наличием в АС информации различного уровня конфиденциальности;
- ▣ уровнем полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- ▣ режимом обработки данных в АС - коллективный или индивидуальный.

Всего 9 классов по 3 группам: 3А,3Б; 2А,2Б; 1А-1Д

Рекомендуемые классы защищённости АС для КИ:

3Б – для однопользовательских АС,

2Б – для АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.

1Д, 1Г – для многопользовательских АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности

Классы защищенности от НСД к информации для СВТ

подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- ▣ первая группа содержит только один седьмой класс;
- ▣ вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- ▣ третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- ▣ четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Самый низкий класс – седьмой, самый высокий – первый.

Для межсетевых экранов (МЭ)

устанавливается пять классов защищенности МЭ.

Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

Программное обеспечение средств защиты информации

Самый высокий уровень контроля - первый, достаточен для ПО, используемого при защите информации с грифом «ОВ».

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».

Самый низкий уровень контроля - четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.

3. Требования РД по защите персональных данных.

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

(ФЗ-№152 «О персональных данных»)

РД по защите ПДн

- ▣ Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.;
- ▣ Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г."
- ▣ Приказ ФСБ, ФСТЭК, Мининформсвязи «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 13 февраля 2008 г. N 55/86/20,
- ▣ Приказ ФСТЭК от 5 февраля 2010 г. N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных"

Категории обрабатываемых в ИС персональных данных (Пр.№58)

1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

4 - обезличенные и (или) общедоступные персональные данные

ИСПДн присваивается 4 класса

- ☐ К1 – самый высокий
- ☐ К4 – самый низкий

ИСПДн 4 класса - перечень мероприятий определяется организацией в зависимости от возможного ущерба.

Для ИСПДн 3 класса

при много– или однопользовательском режиме обработки с равными или разными правами доступа, необходимо обеспечить следующее:

- ☐ управление доступом;
- ☐ регистрация и учет;
- ☐ обеспечение целостности;
- ☐ физическая охрана информационной;
- ☐ периодическое тестирование функций системы защиты;
- ☐ наличие средств восстановления системы защиты персональных данных.

при межсетевом взаимодействии:

- ☐ фильтрацию на сетевом уровне;
- ☐ управление доступом;
- ☐ регистрация и учет;
- ☐ обеспечение целостности;
- ☐ фильтрацию пакетов служебных протоколов;
- ☐ периодическое тестирование функций системы защиты;
- ☐ наличие средств восстановления.

Для ИСПДн 2 класса

при много– или однопользовательском режиме обработки с равными или разными правами доступа, предъявляются те же требования что и для ИСПДн 3 класса.

при межсетевом взаимодействии:

- ☐ фильтрацию на сетевом уровне;
- ☐ фильтрацию пакетов служебных протоколов;
- ☐ фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- ☐ фильтрацию с учетом любых значимых полей сетевых пакетов;
- ☐ регистрацию и учет фильтруемых пакетов;
- ☐ управление доступом;
- ☐ регистрация и учет;
- ☐ регистрацию запуска программ и процессов (заданий, задач);
- ☐ обеспечение целостности;
- ☐ периодическое тестирование функций системы защиты;
- ☐ наличие средств восстановления.

Для ИСПДн 1 класса

при много – или однопользовательском режиме обработки с равными или разными правами доступа:

- ☐ управление доступом;
- ☐ регистрация и учет;
- ☐ обеспечение целостности;
- ☐ физическая охрана информационной;
- ☐ периодическое тестирование функций системы защиты;
- ☐ наличие средств восстановления системы защиты персональных данных.

Рекомендации по проведению аттестации ИСПДн

Аттестации подлежат автоматизированные системы (АС) и защищаемые помещения (ЗП)

Проводить аттестацию вправе органы по аттестации объектов информатизации, которые аккредитуются ФСТЭК России (сайт ФСТЭК – аккредитованные органы) и получают от нее лицензию на право проведения аттестации объектов информатизации.

Проведение аттестации

- ▣ Приведение ИСПДн в соответствие с требованиями СТР-К по технической защите информации
- ▣ Определение класса ИСПДн по защите от НСД по РД (АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д)

Проведение аттестации

- ▣ Выполнение требований сборника временных методик. Данный сборник включает в себя методики оценки защищенности конфиденциальной информации от утечки по техническим каналам: акустическому, виброакустическому, электроакустическим преобразований во вспомогательных технических средствах и системах (ВТСС), побочных электромагнитных излучений и наводок от основных технических средств и систем (ОТСС), а также наводок на ВТСС и их коммуникациях.

Перечень документов для проведения аттестации ИСПДн :

- ▣ Техническое задание (ТЗ) на объект информатизации (ОИ; объектом информатизации может являться АС, а следовательно, и ИСПДн). Это техническое задание с описанием того, чего Заказчик ждёт от Исполнителя.
- ▣ Технический паспорт на ОИ. Этот документ должен описывать техническую сторону ИСПДн: сколько рабочих мест, серийные номера компьютерной техники, их месторасположение в кабинетах (схемы, планы помещений) и др.
- ▣ Приемо-сдаточная документация на ОИ. Сюда можно отнести протоколы заземления, установки охранной и пожарной сигнализации и т.д.
- ▣ Акт классификации автоматизированной системы (АС).
- ▣ Состав технических и программных средств, входящих в состав АС. В данном документе указываются программные и технические средства обработки информации (программное обеспечение, используемое на рабочих местах, сетевое оборудование: маршрутизаторы, коммутаторы и т.д.).
- ▣ Планы размещения основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС). То есть план помещения с указанием на нем расположения рабочих станций, непосредственно участвующих в обработке ПДн, и технических средств, не задействованных в этом процессе, но находящихся в этом же помещении.
- ▣ Состав и схемы размещения средств защиты информации (СЗИ). Описание того, какие активные средства защиты информации используются в Вашей организации.
- ▣ План контролируемой зоны (КЗ) предприятия. То есть подведомственной вашей организации территории.
- ▣ Схемы и характеристики линий передачи данных (ЛВС), охранно-пожарной системы, телефонной линии, электропитания и заземления ОИ. Данную информацию можно получить у электриков.
- ▣ Перечень защищаемых в АС ресурсов с документальным подтверждением степени конфиденциальности каждого ресурса.
- ▣ Организационно - распорядительная документация разрешительной степени доступа персонала к защищаемым ресурсам АС. То есть список лиц, имеющих допуск к ИСПДн, а значит, и к ПДн, обрабатываемым в вашей организации.
- ▣ Описание технологического процесса обработки информации в АС. В этом документе описываются все процессы и этапы обработки информации, от момента сбора (получения) информации до момента ее уничтожения (помещения в архив).
- ▣ Инструкции пользователям АС и администратору безопасности информации.
- ▣ Инструкции по эксплуатации СЗИ.
- ▣ Сертификаты соответствия требованиям по безопасности информации на средства и системы обработки и передачи информации, используемые СЗИ. В государственной организации можно использовать только те СЗИ (генераторы шума, системы защиты от несанкционированного доступа), которые имеют сертификат соответствия ФСТЭК России.
- ▣ Данные по уровню подготовки кадров, обеспечивающих ЗИ. То есть, информация о курсах повышения квалификации или прохождении какого-либо обучения в области защиты информации.

Рекомендуемый состав документации на ОИ

- ▣ Акты внедрения средств ЗИ
- ▣ Протоколы аттестационных испытаний и заключение по их результатам
- ▣ Аттестат соответствия ОИ требованиям по безопасности информации
- ▣ Приказ (указание, решение) о назначении лиц, ответственных за эксплуатацию ОИ
- ▣ Приказ (указание, решение) о разрешении обработки в АС (обсуждении в ЗП) КИ

Состав эксплуатационной документации ОИ по ЗИ

- ▣ Технический паспорт объекта информатизации (АС и ЗП).
- ▣ Технологические инструкции пользователям АС и администратору безопасности информации.
- ▣ Инструкции и руководства по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также для сотрудников службы безопасности.
- ▣ Нормативная и методическая документация по ЗИ и контролю.
- ▣ Эксплуатационная документация на средства контроля эффективности ЗИ.
- ▣ Сертификаты на технические средства (ТС) и СЗИ.
- ▣ Заключение по результатам спецпроверок ЗП и ТС.

В организации должны быть разработаны документы:

- ▣ порядок учёта и хранения в подразделениях организации, а также уничтожения носителей информации (магнитные ленты, аудио - и видеокассеты и др.);
- ▣ порядок хранения и использования аппаратуры звуко- и видеозаписи информации, исключающий несанкционированный доступ к ней;
- ▣ обоснование подключения абонентского пункта к сети;
- ▣ журнал учёта пользователей абонентского пункта;
- ▣ аттестат соответствия на абонентские пункты (АРМ).

Документы необходимые организации для обработки ПДн

Данный перечень документов является рекомендательным, но максимальным, исходя из всех нормативно-правовых актов РФ. Документы, основанием для которых является только СТР-К, необходимы для государственных и муниципальных учреждений. Шаблоны некоторых документов Вы можете взять <http://dehack.ru/docs/>

№ п/п	Разрабатываемый документ	Требования нормативных документов
1	Приказ «Об утверждении формы согласия на обработку персональных данных, уведомления об обработке персональных данных физического лица, уведомления об устранении нарушений допущенных при обработке персональных данных и уведомления об уничтожении персональных данных физического лица»	п.2 ст.5 ФЗ №-152 п.2 ст.15 ФЗ №-152 п.3 ст.21 ФЗ №-152 п.4 ст.21 ФЗ №-152 п.3 ст.21 ФЗ №-152 п.3 ст.18 №152-ФЗ п.1 ст.6 ФЗ №-152
2	Приказ "об утверждении Положения об обработке ПДн" приложение: Положение об обработке ПДн	п.2 ст.5 ФЗ №-152 п.1 ст.14 ФЗ №-152 п.3 ст.21 ФЗ №-152 п.4 ст.21 ФЗ №-152 п.6 ПП №687
3	Форма типового договора о сохранении конфиденциальности ПДн	п.1 ст.7 ФЗ №-152
4	Приказ "об утверждении журнала обращений субъектов ПДн" приложение: Журнал обращений субъектов ПДн, инструкция по ведению журнала	п.1 ст.14 ФЗ №-152
5	Типовая форма запроса субъекта ПДн на доступ к своим ПДн	п.3 ст.14 ФЗ №-152
6	Уведомление об обработке ПДн	п.1 ст.22 ФЗ №-152
7	Приказ "об утверждении журнала учёта средств защиты информации" приложение: Журнал учёта средств защиты информации, инструкция по заполнению журнала	п.2.16 СТР-К п.5.1.3 СТР-К
8	Приказ "о создании постоянно действующей экспертной комиссии по защите информации (ПДЭК по ЗИ)" приложения: положение о ПДЭК по ЗИ, план заседаний	п.2. Приказ ФСТЭК №55/86/20 п.6.3.8 СТР-К
9	Протокол заседание ПДЭК по ЗИ "Определение исходных данных для классификации ИСПДн"	п.2. Приказ №55/89/20
10	Акт классификации ИСПДн	п.2. Приказ №55/89/20 п.3.8 СТР-К п.5.6.4 СТР-К
11	Приказ "об утверждении инструкции по КПР И ВОР"	р.8 ч.2 ПП №687

	приложения: инструкция по КПП и ВОР, журнал пропуска на территорию объекта	р.2.1 ч.2 приказ ФСТЭК №58 Р.2.1 ч.2 приказ ФСТЭК №58
12	Приказ "о назначении сотрудника/подразделение ответственного за осуществление мероприятий по защите информации". Приложение: список сотрудников ответственных за осуществление мероприятий по защите информации	п.3.21 СТР-К п.5.3.5 СТР-К п.6.3.3 СТР-К п.6.3.1 СТР-К п.6.3.11 СТР-К
13	Приказ "о допуске сотрудников к обработке ПДн", приложение: список сотрудников, допущенных к обработке ПДн в ИСПДн; список сотрудников допущенных к неавтоматизированной обработке ПДн	п.6 ч.2 ПП №687 р.13 ч.3 ПП №687 п.6.3.2 СТР-К
14	Приказ "об утверждении регламента проведения внутренних проверок соблюдения правил защиты информации" приложение: Регламент проведения внутренних проверок соблюдения правил защиты информации; план проведения внутренних проверок соблюдения правил защиты информации	приказ ФСТЭК №58
15	Приказ "об установлении границ контролируемой зоны", приложение: границы контролируемой зоны	р.2.1 ч.2 п.3.8 СТР-К п.5.1.3 СТР-К
16	Приказ "об утверждении инструкции по резервному копированию", приложение: Инструкция по резервному копированию	Р.2.1 ч.2 приказ ФСТЭК №58
17	Приказ "об утверждении частной модели угроз безопасности ПДн в ИСПДн", приложение: Частная модель угроз безопасности ПДн в ИСПДн	п.3.8 СТР-К
18	Приказ "о вводе системы защиты информации в эксплуатацию", приложение: описание системы защиты информации	п.3.20 СТР-К п.3.21 СТР-К
19	Заключение о готовности к эксплуатации системы защиты информации	
20	Приказ "об обучении сотрудников правилам защиты информации", приложение: программа обучения правилам защиты информации; план проведения обучения правилам защиты информации, журнал инструктажей по информационной безопасности;	
21	Приказ "об утверждении журнала учета носителей информации, содержащих защищаемую информацию", приложения: журнала регистрации носителей информации, содержащих защищаемую информацию; инструкция по заполнению журнала	р.2.1 ч.2 приказ ФСТЭК №58 п.5.1.3 СТР-К п.5.2.6 СТР-К п.5.3.4 СТР-К п.5.3.5 СТР-К п.5.3.6 СТР-К п.5.3.7 СТР-К
22	Приказ "об утверждении разрешительной системы доступа к ПДн", приложение: разрешительная система доступа	р.2.1. ч.2 приказ ФСТЭК №58 п.5.1.3 СТР-К п.5.3.2 СТР-К п.4.2.10 СТР-К

		п.5.6.6 СТР-К
		п.6.3.2 СТР-К
23	Технический паспорт (перечень ОТСС организации, перечень ВТСС организации, перечень используемого ПО, список помещений для хранения и обработки ПДн; список мест хранения ПДн в ИСПДн; список сейфов и других мест хранения ПДн; схема ЛВС; схема ОПС; схема сетей электропитания и заземления)	р.13 ч.3 ПП №687 р.2.1. ч.2 приказ ФСТЭК №58 п.3.8 СТР-К п.5.1.3 СТР-К п.3.18 СТР-К п.2.7 СТР-К п.4.2.1 СТР-К
24	Приказ "об утверждении перечня персональных данных", приложения: перечень ПДн	р.2.1. ч.2 приказ ФСТЭК №58
25	Приказ "об утверждении журнала регистрации действий пользователей, обслуживающего персонала и посторонних лиц", приложения: журнал регистрации действий пользователей, обслуживающего персонала и посторонних лиц, инструкция по заполнению журнала	р.2.1 ч.2 приказ ФСТЭК №58 п.5.1.3 СТР-К
26	Приказ "об утверждении инструкции пользователя ИСПДн", приложение: Инструкция пользователя ИСПДн	р.2.1 ч.2 приказ ФСТЭК №58 п.5.3.2 СТР-К п.5.5.3 СТР-К п.5.6.2 СТР-К п.5.6.3 СТР-К п.6.1.4 СТР-К п.6.3.6 СТР-К
27	Приказ "об утверждении инструкции администратора ИСПДн", приложение: Инструкция администратора ИСПДн	р.2.1 ч.2 приказ ФСТЭК №58 п.5.3.2 СТР-К п.5.5.3 СТР-К п.5.6.2 СТР-К п.5.6.3 СТР-К п.6.1.4 СТР-К п.6.3.6 СТР-К
28	Приказ "об утверждении инструкции по передаче ПДн"	
29	Приказ "об утверждении инструкции по антивирусному контролю", приложение: Инструкция по антивирусному контролю	п.6.1.4 СТР-К
30	Приказ "об утверждении мест хранения и обработки ПДн", приложения: список помещений для хранения и обработки ПДн; список мест хранения ПДн в ИСПДн; список сейфов и других мест хранения ПДн; допуск сотрудников в защищаемые помещения)	р.13 ч.3 ПП №687 р.2.1. ч.2 приказ ФСТЭК №58 п.5.1.3 СТР-К п.4.2.1 СТР-К
31	Модель угроз безопасности информации (по методикам ФСБ)	п.2.3 ТТ ФСБ 149/6/6-622
32	Приказ "об утверждении списка лиц допущенных к работе с СКЗИ", приложение: список лиц допущенных к работе с СКЗИ	п.2.3 ТТ ФСБ 149/6/6-622
33	Акт ввода СКЗИ в эксплуатацию	п.2.3 ТТ ФСБ

		149/6/6-622
34	Приказ "об утверждении журнала поэкземплярного учета СКЗИ" приложения: журнал поэкземплярного учёта СКЗИ, инструкция по заполнению журнала, журнал учёта пользователей СКЗИ	п.2.3 ТТ ФСБ 149/6/6-622
35	Журнал учета и выдачи носителей с ключевой информацией	Необходим только в случае использования одноразовых ключей п.3.6 ТТ ФСБ 149/6/6-622
36	Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ	п.3 ТТ ФСБ 149/6/6-622
37	Положение о порядке организации и проведения работ по защите конфиденциальной информации	п.3.5 СТР-К
38	Описание технологического процесса обработки информации	п.3.8 СТР-К
39	План мероприятий по обеспечению конфиденциальности информации Техническое задание на создание СЗИ	п.3.8 СТР-К п.3.13 СТР-К
40	Регламент проведения совещаний и (или) переговоров	п.4.2.5 СТР-К п.4.2.11 СТР-К п.4.2.12 СТР-К п.4.2.14 СТР-К п.4.3.2 СТР-К п.4.4.1 СТР-К п.4.4.2 СТР-К п.5.3.2 СТР-К
41	Регламент обеспечения защиты информационных ресурсов АП при подключении к Сети и при удаленном доступе к АП через Сеть	п.6.3.12.1 СТР-К; п.6.3.13.1 СТР-К
42	Проверка документов: Эксплуатационная документация по СКЗИ; Лицензии и сертификаты на СКЗИ; Документы, подтверждающие функциональные обязанности сотрудников; Документы, подтверждающие прохождение обучения сотрудников; Копии нормативных документов	Типовые Треб. ФСБ 149/6/6-622
43	Получение аттестата соответствия	п.2.17 СТР-К п.3.19 СТР-К п.3.20 СТР-К
44	Приказ "об утверждении перечня сведений конфиденциального характера", приложение: Перечень сведений конфиденциального характера	п.2.7 СТР-К п.3.6 СТР-К п.3.8 СТР-К п.5.1.3 СТР-К
45	Обоснование для создания СЗИ	п.3.8 СТР-К п.3.9 СТР-К п.3.12 СТР-К п.6.2.1 СТР-К
46	Приказ "о техническом проектировании СЗИ и назначении ответственных за исполнение", приложение: Технический проект на создание СЗИ	п.3.18 СТР-К п.3.21 СТР-К

47	Технический паспорт на ЗП	п.4.2.1 СТР-К
48	Перечень защищаемых помещений	п.4.2.1 СТР-К
49	Приказ "о допуске сотрудников в защищаемые помещения", приложение: Список сотрудников допущенных в ЗП	п.4.2.1 СТР-К п.5.1.3 СТР-К
50	Заключение об эффективности принятых мер	п.3.19 СТР-К п.6.3.8 СТР-К п.6.3.9 СТР-К
51	Приказ "о назначении ответственного за хранение и использование аппаратуры звуко- и видеозаписи информации	п.4.4.3 СТР-К
52	Инструкция по использованию аппаратуры звуко- и видеозаписи	п.4.4.3 СТР-К
53	Отчет о выполнении требований стандартов РФ по электромагнитной совместимости, по безопасности и по санитарным нормам	п.5.2.4 СТР-К
54	Руководство по защите информации от утечки по техническим каналам	п.3.5 СТР-К

Шаблоны некоторых документов:
http://dehack.ru/PDn/dokumenty_neobxodimye_organizatsii_dlja_obrabotki_pdn/shablony_dokumentov/

Документы для подключения к ФИР и сервисам ФНС:

- ▣ О возложении ответственности за обеспечение информационной безопасности на объекте информатизации (ОИ)
- ▣ Об утверждении политики информационной безопасности ОИ
- ▣ Об утверждении руководства по ИБ ОИ
- ▣ Информационно-логический паспорт ОИ(включая схему и пояснительную записку о реализованном закрытом контуре ЛВС
- ▣ Порядок обработки персональных данных на ОИ
- ▣ Об утверждении порядка доступа к информационным, программным и аппаратным ресурсам на ОИ
- ▣ Об утверждении порядка использования средств криптозащиты и управления ключевой информацией на ОИ. Журналы средств криптозащиты и формуляры
- ▣ О порядке организации хранения электронных копий документов ограниченного доступа, полученных по телекоммуникационным каналам связи
- ▣ Об утверждении порядка защиты компонентов информационной системы ОИ от вредоносного программного обеспечения
- ▣ О порядке сдачи под охрану служебных помещений с оборудованием, имеющим подключение к системе телекоммуникаций ФНС России
- ▣ Об утверждении памятки пользователя по информационной безопасности
- ▣ О назначении должностных лиц по функционалу:
- ▣ Администратор ИБ (включая определение ответственности за техническое сопровождение средств криптозащиты, разграничение доступа пользователей закрытого контура ЛВС к ИР ФНС, актуализацию нормативных документов ОИ по вопросам ИБ)
- ▣ Оператор средств криптозащиты
- ▣ Администратор СЭД Lotus Notes
- ▣ Администратор антивирусной защиты
- ▣ Администратор ЛВС (системный администратор)

Методы защиты информации

- Правовые
- Организационные
- Технические
- Программные

Технические средства защиты информации

- 1. Источники бесперебойного питания**
- 2. Специальные устройства защиты от утечки по техническим каналам**
- 3. Специальные устройства защиты компьютерной информации**
- 4. Специальные устройства поиска средств негласного получения информации**

Источники бесперебойного питания



UPS APC Back ES 700VA



DNS SMART PRO LCD 800VA

2500 руб



APC Back-Up CS 500VA



IPPON Back Office 1000

Специальные устройства защиты от утечки по техническим каналам

Аппаратура виброакустической защиты помещений VNG-006DM
(сертификат №126/3)



Предназначена для создания широкополосных виброакустических и акустических помех в речевом диапазоне частот.

Аппаратура обеспечивает предотвращение негласного контроля речевой информации через ограждающие конструкции и инженерно-технические коммуникации выделенных помещений

**СИГМА» УСТРОЙСТВО ЗАЩИТЫ ПОМЕЩЕНИЯ ОТ ПРОСЛУШИВАНИЯ
ЧЕРЕЗ ТЕЛЕФОННЫЙ АППАРАТ (сертификат ФСТЭК России № 1004)**



предназначено для предотвращения несанкционированного прослушивания помещения через телефонный аппарат, а также исключение утечки речевой информации из помещения за счет акустоэлектрических преобразований в телефонном аппарате

**«ЦИКАДА-С» УСТРОЙСТВО ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО
ЭЛЕКТРОСЕТИ (сертификат ФСТЭК России № 463/1)**



предназначено для защиты от утечки информации по сети электропитания, а также для противодействия устройствам негласного съема акустической информации из помещений, использующих для ее передачи электрическую сеть

Генератор шума ГШ-2500

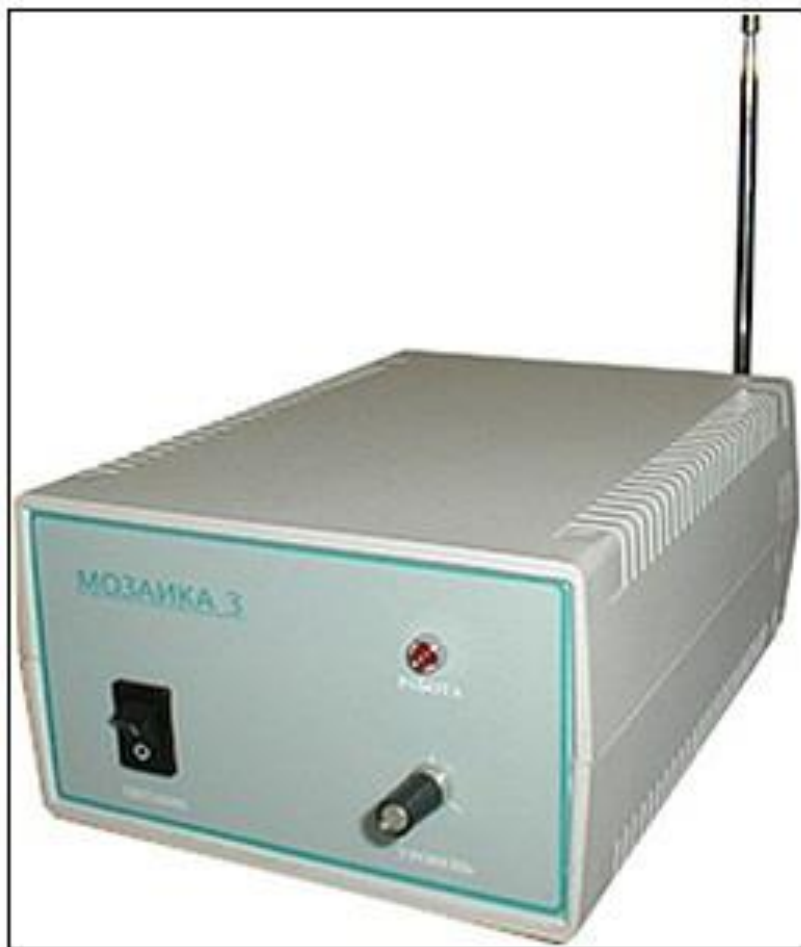


Предназначен для защиты объектов вычислительной техники первой, второй и третьей категорий от утечки информации по каналам побочных электромагнитных излучений и наводок, далее по тексту ПЭМИН, путем формирования и излучения в окружающее пространство электромагнитного поля шума, далее по тексту ЭМПШ, и путем наведения маскирующего сигнала в отходящие цепи в диапазоне частот от 0,1 до 2000 МГц. Генератор шума формирует маскирующее электромагнитное поле и в диапазоне частот ниже 0,1 МГц (до 0,01 МГц). Уровни спектральной плотности шума в диапазоне частот от 0,01 до 0,1 МГц не нормируются.

Генератор шума ГШ-2500 включен в Государственный реестр сертифицированных средств защиты информации Системы сертификации № РОСС RU.0001.01БИ00 (ФСТЭК России) и используется на объектах информатизации для исключения утечки информации ограниченного доступа (государственная тайна, конфиденциальная информация, в том числе персональные данные) по каналам ПЭМИН.

Масса 500 грамм.

«МОЗАИКА-3» Устройство блокирования работы систем мобильной связи



Подавитель сотовых телефонов "Мозаика-3" предназначен для предотвращения возможности использования каналов систем мобильной связи в качестве канала передачи информации аудио и видео закладных устройств. Отличительной особенностью изделия "Мозаика-3" является: возможность подавления сотовой связи стандартов NMT 450i и CDMA-2000 (Skylink).

Возможно встраивание изделия в корпус, предоставленный заказчиком. Изделие «Мозаика-3» может изготавливаться в варианте с увеличенной мощностью – «Мозаика-3М» (опция).

Мозаика мини предназначена для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS, DAMPS, CDMA, а также блокирования работы телефонов названных систем мобильной связи.

Отличительные особенности:

мобильность

малые размеры

камуфлирован под малогабаритный приемник.

«СОНАТА-Р2» УСТРОЙСТВО ЗАЩИТЫ ОБЪЕКТОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (сертификат ФСТЭК России № 1129)



предназначено для защиты объектов вычислительной техники до 1-ой категории включительно от утечки информации за счет побочных электромагнитных излучений и наводок на сети электропитания, линии заземления, инженерные коммуникации и линии вспомогательных технических средств

Специальные устройства защиты компьютерной информации и аутентификации пользователя

Модули доверенной загрузки

загрузка операционной системы с внутреннего жесткого диска компьютера, которая происходит только после выполнения процедур идентификации и аутентификации пользователя, а также проверки целостности программной и аппаратной среды рабочего места, в том числе целостности объектов загружаемой ОС.

При этом должна обеспечиваться невозможность загрузки пользователем другой операционной системы (в т.ч. с внешних носителей информации).

В течение многих лет аппаратно-программный модуль доверенной загрузки компьютера является одним из самых надежных и распространенных отечественных средств компьютерной безопасности.

«Доверенная загрузка» – это загрузка различных ОС только с заранее определенных постоянных носителей (например – с НЖМД) только после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием пошагового механизма проверки целостности) и аппаратной идентификации/аутентификации пользователя.

Иными словами – это загрузка строго определенной, не измененной ОС и только в том случае, если подтверждено, что в компьютере не произошло никаких несанкционированных изменений (на аппаратном уровне и критичной части приложений) и что включает его именно тот пользователь, который имеет право на нем работать именно в это время.

При этом должна обеспечиваться невозможность загрузки пользователем другой ОС (с внешних носителей информации и др.).

Модуль доверенной загрузки представляет собой комплекс аппаратно-программных средств, устанавливаемый в рабочее место вычислительной системы (персональный компьютер, сервер, ноутбук, специализированный компьютер и др.) и обеспечивающий контроль доступа пользователя к рабочему месту и контроль целостности программной среды рабочего места.

«АНКАД» (www.ancud.ru) КРИПТОН-ЗАМОК (М-526, М-526А, М-526Б)



- для обеспечения разграничения и контроля доступа пользователей к техническим средствам вычислительной сети
- разграничения доступа к аппаратным ресурсам компьютеров
- контроля целостности установленной на компьютере программной среды

Фирма «АНКАД» (www.ancud.ru) широко известна своими криптографическими аппаратными средствами защиты информации.

Желание разработчиков реализовать разграничение и контроль доступа пользователей к защищаемому компьютеру, разграничение доступа к аппаратным ресурсам компьютера, контроль целостности компьютерной программной среды привело их к созданию аппаратно-программных МДЗ семейства «КРИПТОН-ЗАМОК».

Изделия «КРИПТОН-ЗАМОК» - это комплексы аппаратно-программных средств, который предназначены для обеспечения разграничения и контроля доступа пользователей к техническим средствам вычислительной сети (сервера и рабочие станции), на которых будет обрабатываться информация, в том числе и с высоким грифом секретности, разграничения доступа к аппаратным ресурсам компьютеров, а также контроля целостности установленной на компьютере программной среды под любые ОС, использующие файловые системы FAT12, FAT16, FAT32 и NTFS (Windows NT 4.0 и Windows 2000/XP/2003), а так же Ext2, Ext3 (Unix-системы).

- «КРИПТОН-ЗАМОК/К» – предназначен для создания нескольких контуров безопасности компьютера, модуль позволяет осуществить загрузку конфигурации компьютера в соответствии с индивидуальными настройками системы для каждого пользователя, разделение пользователей по физическим дискам и сетевым контурам;
- «КРИПТОН-ЗАМОК/У» – предназначен для работы с модулями криптографической защиты информации;
- «КРИПТОН-ЗАМОК/УК» – модуль для создания нескольких контуров безопасности компьютера и работы с модулями криптографической защиты информации;
- «КРИПТОН-ЗАМОК/М» – предназначен для реализации доверенной загрузки операционной системы со съемного жесткого диска (контейнер Mobile Rack для шины IDE).

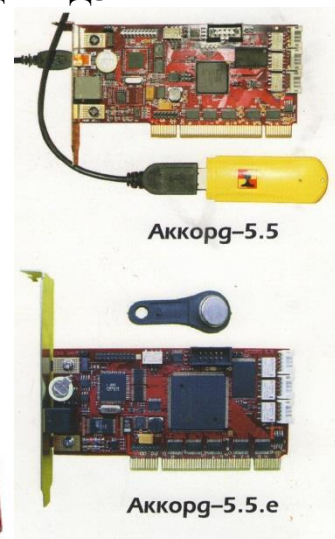
Идентификация и аутентификация пользователей в МДЗ семейства «КРИПТОН-ЗАМОК» осуществляется с помощью идентификаторов iButton.

Контроль целостности программной среды (контрольные суммы рассчитываются по алгоритму вычисления хэш-функции по ГОСТ Р34.11-94) реализуется для файловых систем FAT 12, FAT 16, FAT 32, NTFS, EXT2FS, EXT3FS.

Устройство обеспечивает аппаратную блокировку от несанкционированной загрузки ОС с внешних носителей: дискет, CD/DVD-дисков, USB-дисков и USB flash-накопителей.

В МДЗ осуществляется ведение журнала регистрации и учета событий безопасности, расположенного в энергонезависимой памяти на плате изделия.

В настоящее время фирма «АНКАД» выпустила версию МДЗ для шины PCI-E x1 Rev 1.1 – «КРИПТОН-ЗАМОК/Е, в которой реализован ряд новых возможностей. Например, разработчики повысили производительность устройства (на плате встроены процессор с тактовой частотой 200 МГц и память объемом 256 Мб), создали независимый USB-интерфейс для подключения внешних носителей, внедрили новый формфактор платы, позволяющий использовать устройство в системных блоках уменьшенного размера.



Аппаратный модуль доверенной загрузки для IBM-совместимых ПК (автономных и в локальной сети), обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа

ОКБ САПР (<http://www.okbsapr.ru>) является родоначальником отечественных МДЗ. Первый сертификат соответствия Гостехкомиссии России компания получила более 15 лет назад – в декабре 1994 года.

Выпускаемые в настоящее время ОКБ САПР модули доверенной загрузки носят общее наименование «Аккорд-АМДЗ» и реализуются в пяти модификациях:

«Аккорд-5MX» – для шин стандарта PCI, PCI-X;

«Аккорд-5.5» – для шин PCI, PCI-X;

«Аккорд-5.5E» – для шин PCI Express;

«Аккорд-5.5MP» – для стандарта mini-PCI (см. рис. 1);

«Аккорд-5.5ME» – для стандарта mini-PCI Express.

Комплекс «Аккорд-АМДЗ» включает аппаратные и программные средства. В базовый комплект поставки аппаратных средств входят контроллер, два идентификатора iButton DS1992 и считывающее устройство.

Другие компоненты МДЗ (устройства блокировки каналов FDD, HDD (IDE), USB-портов, устройства отключения питания ATX, EATX и др.) поставляются дополнительно по требованию заказчиков.

Программное обеспечение «Аккорд-АМДЗ» размещается в энергонезависимой памяти контроллеров.

«Аккорд-АМДЗ» обеспечивает доверенную загрузку операционных систем, поддерживающих файловые системы FAT 12, FAT 16, FAT 32, NTFS, HPFS, EXT2FS, EXT3FS, FreeBSD, Sol86FS, QNXFS, MINIX. В список операционных систем входят MS DOS, Windows 9x/ME/NT/2000/XP/2003/Vista, QNX, OS/2, UNIX, LINUX, BSD и др. Для ОС семейства Windows дополнительно реализована функция контроля целостности и неизменности реестра.

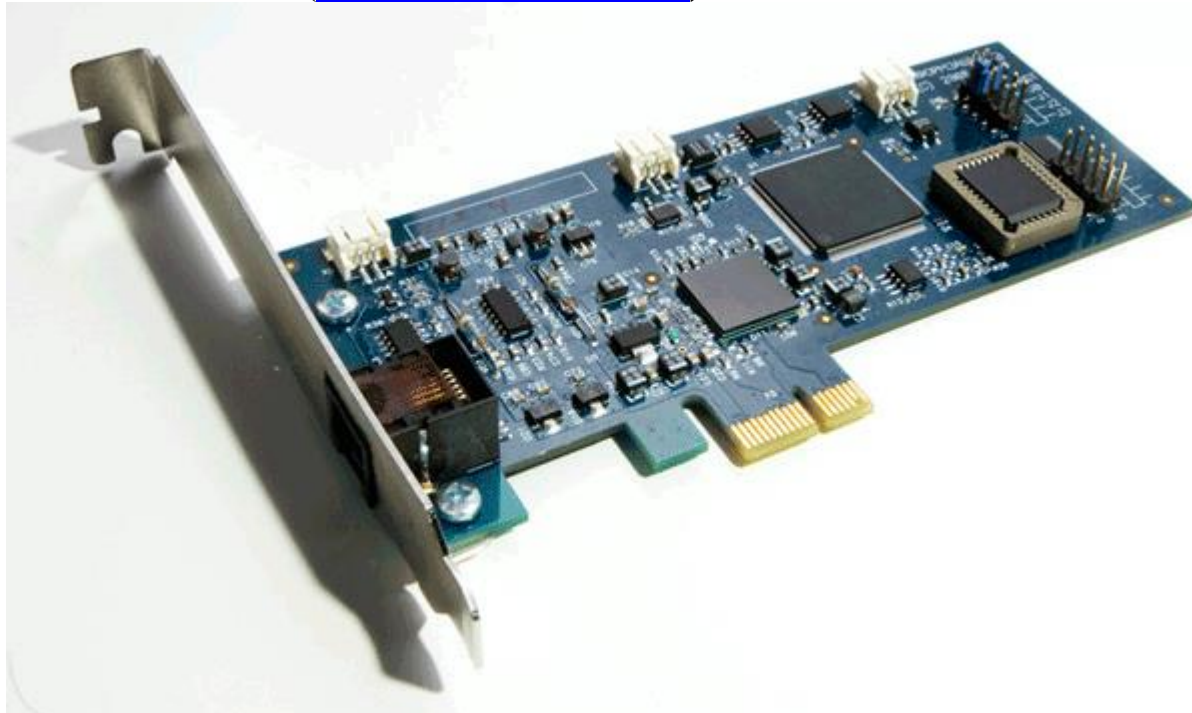
Для идентификации пользователей разработчики «Аккорд-АМДЗ» предлагают применять идентификаторы iButton, персональное средство криптографической защиты информации «ШИПКА» и другие устройства, тип которых уточняется при заказе средства защиты. Аутентификация осуществляется по паролю (длиной до 12 символов), вводимому пользователем с клавиатуры. В «Аккорд-АМДЗ» поддерживается регистрация до 126 пользователей.

Помимо традиционного контроля целостности файлов и служебных областей жестких дисков «Аккорд-АМДЗ» поддерживает проверку неизменности аппаратной части компьютера и ветвей реестра операционных систем семейства Windows.

В МДЗ «Аккорд-5.5» дополнительно внедрены аппаратно реализованные криптографические алгоритмы защиты информации: шифрование (ГОСТ Р 28147-89), хэширование (ГОСТ Р 34.11-94, MD5, SHA-1), выработка и проверка электронной цифровой подписи (ГОСТ Р 34.10-2001), защитных кодов аутентификации (на основе ГОСТ Р 31.11-94).

Контроллеры «Аккорд-АМДЗ» могут использоваться совместно со специальным программным обеспечением, предназначенным для реализации алгоритмов разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам. Также контроллеры функционируют совместно с изделием «Средство криптографической защиты информации «КриптоПро CSP».

НИП «Информзащита» (<http://www.infosec.ru>) ПАК семейства «Соболь»
«Код Безопасности» (<http://www.securitycode.ru>)



обеспечивает доверенную загрузку более 20 операционных систем компьютеров с 32- и 64-разрядной архитектурой, поддерживающих файловые системы FAT 16, FAT 32, NTFS, UFS, EXT2, EXT3 (Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2, Windows 7, VMware ESX, MCBC 3.0, Linux XP 2008 Secure Edition и др)

НИП «Информзащита» (<http://www.infosec.ru>) создало свой первый МДЗ в 1999 году. Он получил название «Электронный замок «Соболь». С 2009 года разработку МДЗ осуществляет компания «Код Безопасности» (<http://www.securitycode.ru>), входящая в группу компаний «Информзащита».

В настоящее время «Код Безопасности» серийно выпускает следующие типы МДЗ:

- программно-аппаратные комплексы (ПАК) семейства «Соболь» версий 2.1 и 3.0;
- изделия Secret Net Touch Memory Card PCI 2, Secret Net Card – упрощенные варианты ПАК «Соболь», созданные для блокировки загрузки ОС с внешних носителей и поддержки реализуемой системой Secret Net процедуры идентификации и аутентификации пользователей с помощью идентификаторов iButton.

Новая версия ПАК «Соболь 3.0» выпускается в двух вариантах:

- для шины стандарта PCI Express (PCI-E) версии 1.0a и выше (см. рис. 2);
- для шины стандарта PCI версий 2.0/2.1/2.2/2.3 с напряжением питания 5 В или 3,3 В.

Комплекс «Соболь 3.0» обеспечивает доверенную загрузку более 20 операционных систем компьютеров с 32- и 64-разрядной архитектурой, поддерживающих файловые системы FAT 16, FAT 32, NTFS, UFS, EXT2, EXT3. В их число входят Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2, Windows 7, Windows Vista/Vista x64 Edition, Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/Server 2003 R2 x64 Edition, VMware ESX, MCBC 3.0, Linux XP 2008 Secure Edition и др.

Помимо основных функций МДЗ (идентификация и аутентификация пользователей, блокировка загрузки ОС с внешних носителей, контроль целостности, регистрация событий безопасности) в ПАК «Соболь» реализован ряд дополнительных возможностей:

- механизм сторожевого таймера;
- использование случайных паролей;
- контроль работоспособности основных компонентов комплекса;
- программная инициализация комплекса, реализуемая без вскрытия системного блока компьютера.

Расчет контрольных сумм при реализации механизма контроля целостности осуществляется в соответствии с алгоритмом ГОСТ Р 28147-89 в режиме вычисления имитовставки.

Механизм идентификации и аутентификации, реализованный в ПАК «Соболь 3.0», дает возможность использования нескольких типов идентификаторов:

- eToken PRO;
- iKey 2032;
- Rutoken S;
- Rutoken RF S;
- iButton.

В зависимости от типа предъявляемого идентификатора в комплексе поддерживаются и усиленный двухфакторный способы аутентификации. Аутентификация пользователя осуществляется по паролю (длиной до 16 символов), вводимому с клавиатуры.

В ПАК «Соболь 3.0» поддерживается совместная работа с системами защиты семейства Secret Net, АПКШ «Континент», средствами защиты информации Security Code vGate for VMware Infrastructure, Security Studio Honeypot Manager, «Континент-АП» и «КриптоПро CSP».

В базовый комплект поставки ПАК «Соболь 2.1» входят плата для шины PCI, идентификаторы iButton DS1992 (2 шт.) с контактным устройством, кабель для механизма сторожевого таймера, компакт-диск с эксплуатационной документацией и программным обеспечением. В комплект поставки ПАК «Соболь 3.0» помимо iButton могут входить USB-идентификаторы.

Электронные идентификаторы

предназначены для безопасной аутентификации пользователя при доступе к защищаемым ресурсам рабочей станции, а так же для безопасного хранения ключей шифрования, цифровых сертификатов пользователей и любой другой информации ограниченного доступа

Развитие и совершенствование МДЗ осуществлялось практически в ногу с развитием компьютерной техники и с изменением угроз информационной безопасности. На компьютерном рынке появлялись новые типы компьютеров, новые материнские платы, новые идентификаторы, следом за ними совершенствовалась аппаратная часть МДЗ, увеличивалось количество типов поддерживаемых идентификаторов.

Данное средство предназначено для безопасной аутентификации пользователя при доступе к защищаемым ресурсам рабочей станции, а так же для безопасного хранения ключей шифрования, цифровых сертификатов пользователей и любой другой информации ограниченного доступа.

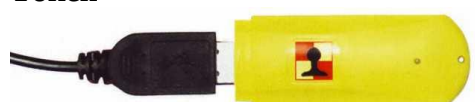
ЭИ обладают следующими возможностями:

- аутентификация пользователей при доступе к базам данных, серверам, Web-ресурсам
- защита электронной почты с помощью цифровой подписи и шифрования
- защита при взаимодействии банк-клиент
- электронная торговля
- защита виртуальных частных сетей (VPN)
- защита рабочих станций
- хранение паролей, ключей шифрования, цифровых сертификатов пользователей

Идентификаторы

- **eToken PRO**
- **iKey 2032**
- **Rutoken S**
- **Rutoken RF S**
- **iButton**
- **ШИПКА**

Token



Смарт-карты



iButton



Электронный идентификатор - это компактное устройство в виде USB-брелока, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

ЭИ с успехом заменяет любые парольные системы защиты, ведь теперь не нужно запоминать множество логинов и сложных паролей, все они надежно хранятся в памяти ЭИ. Все что должен сделать пользователь - подключить ЭИ (к USB-порту) и набрать PIN-код. Таким образом, осуществляется двухфакторная аутентификация, когда доступ к информации можно получить, только обладая уникальным предметом (ЭИ) и зная некоторую уникальную комбинацию символов (PIN-код).

Token выступает удачной альтернативой другим аппаратным носителям ключевой информации: смарт-картам, i-button, не говоря уже о дискетах. Действительно, token - это аналог смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель), данные надежно хранятся в энергонезависимой памяти токена объемом до 128 Кб, прочный корпус Rutoken устойчив к внешним воздействиям. Основу token составляет микроконтроллер, который выполняет криптографическое преобразование данных, и память, в которой хранятся данные пользователя (пароли, сертификаты, ключи шифрования и т. д.).

Электронные идентификаторы обычно используются в комплексе с соответствующими программно-аппаратными средствами. Token поддерживает основные промышленные стандарты (см. технические характеристики), что позволяет без труда использовать токены в уже существующих системах безопасности информации.

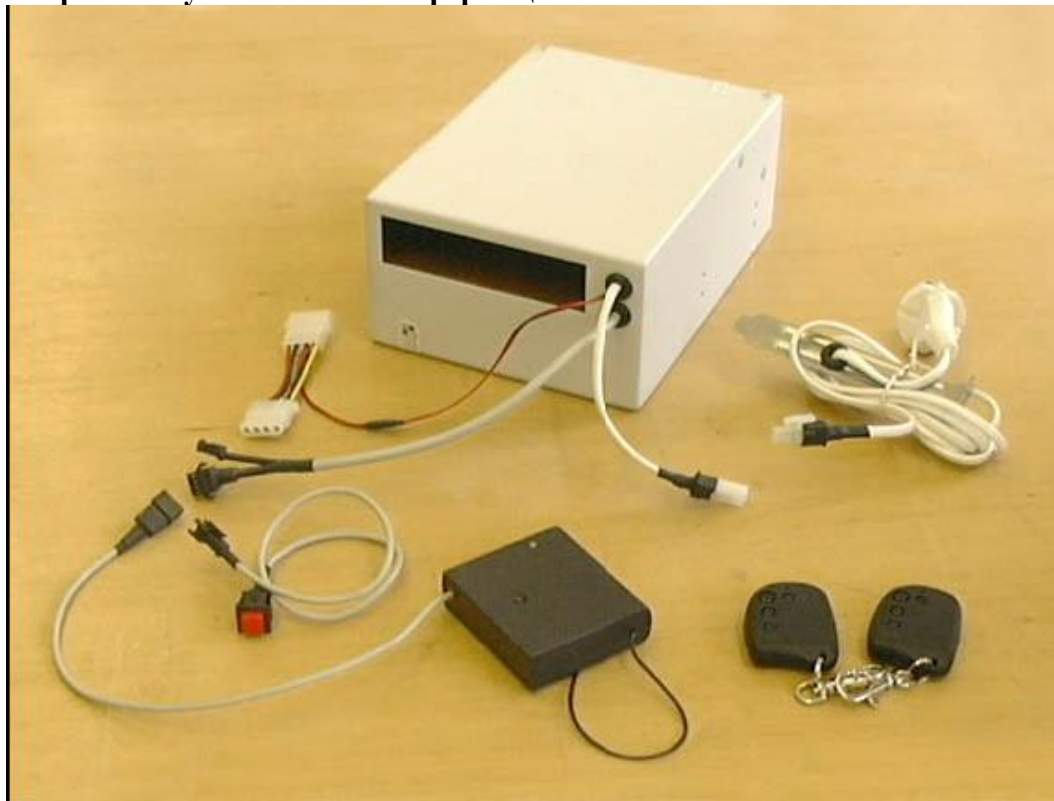
Главным отличием Rutoken от зарубежных аналогов является аппаратно реализованный российский стандарт шифрования - ГОСТ 28147-89.

Утилизатор для жестких дисков компьютеров "Стек-НС1в"



для быстрого (экстренного) уничтожения информации, записанной на накопителях на жестких магнитных дисках с продольным и вертикальным типами записи

Устройство уничтожения информации на магнитных носителях 2С-994В



Для экстренного гарантированного уничтожения информации с накопителя на жестком магнитном диске при возникновении опасности ее хищения по команде пользователя

Специальные устройства поиска средств негласного получения информации

«УЛАН-2» - универсальный анализатор проводных линий (сертификат ФСТЭК России № 922)



предназначен для обнаружения фактов несанкционированного подключения к различным проводным коммуникациям, таким как телефонные линии, электрические сети переменного тока, компьютерные сети, линии охранной сигнализации и т.п.

Прибор "УЛАН-2" (пятое поколение) предназначен для обнаружения фактов несанкционированного подключения к различным проводным коммуникациям, таким как телефонные линии, электрические сети переменного тока, компьютерные сети, линии охранной сигнализации и т.п.

Анализатор способен не только выявить и идентифицировать обнаруженные устройства, но и, используя метод импульсной локации, с высокой точностью измерить расстояние до места несанкционированного подключения.

"УЛАН-2" ПОЗВОЛЯЕТ ОБНАРУЖИТЬ СЛЕДУЮЩИЕ ВИДЫ НЕГЛАСНЫХ ПОДКЛЮЧЕНИЙ И СИГНАЛОВ:

В телефонных линиях (без отключения от АТС и без наличия предварительной информации):

последовательные подключения с эквивалентным сопротивлением более 30 Ом;
параллельные подключения в режиме с током потребления более 0,1 мА;
высокочастотные сигналы в линии в диапазоне 0,02÷30 МГц с эффективным напряжением более 10 мВ при симметричном и несимметричном подключениях;
низкочастотные сигналы в диапазоне 20÷20000 Гц с эффективным напряжением более 1 мВ.

В линиях электросети переменного тока под напряжением:

"сторожевые устройства" с током потребления более 0,1 мА;

высокочастотные сигналы в диапазоне 0,02÷30 МГц с эффективным напряжением более 10 мВ.

В обесточенных линиях:

параллельные подключения с активным сопротивлением до 100 МОм;

последовательные подключения с активным сопротивлением более 1 Ом;

наличие реактивных элементов с емкостью более 10 пФ и индуктивностью более 10 мГн (без учета собственных параметров).

В любых линиях (в том числе без отключения от напряжения), при наличии предварительно полученной рефлектограммы:

последовательные подключения с эквивалентным сопротивлением более 1 Ом;

параллельные подключения с эквивалентной емкостью более 5 пФ;

параллельные ответвления любой протяженности;

восстановленные нарушения целостности линии (разрыв с последующей скруткой);

нарушения линии, связанные с установкой бесконтактных магнитных съемников.

Кроме указанного, прибор "УЛАН-2" позволяет:

производить измерения напряжения постоянного и переменного токов в проверяемой линии;

производить измерения сопротивления, емкости и индуктивности в обесточенных линиях;

производить измерение сопротивления шлейфа телефонной линии;

прослушивать, записывать и обрабатывать аудио сигналы в проверяемой линии;

выводить на экран встроенного 17" TFT дисплея следующую графическую информацию о проверяемой линии: вольт-амперную характеристику, импульсную переходную характеристику, нагрузочную характеристику телефонной линии, амплитудно-частотную характеристику линии, параметрическую зависимость выходного тока от входного гармонического напряжения (т.н. фигуры Лиссажу), импульсные рефлектограммы линий;

хранить числовые и графические результаты измерений на встроенном жестком диске;

совместно с прибором "УП-7" прослеживать трассу прокладки проверяемой линии в стенах и строительных конструкциях.

"КОРДОН" - АНАЛИЗАТОР ЭЛЕКТРОМАГНИТНОГО ПОЛЯ



Анализатор поля позволяет выявлять закладные устройства, внедренные в выделенные помещения и на объекты информатизации и использующие для передачи информации радиоканал.

Анализатор электромагнитного поля "КОРДОН" предназначен для выявления и локализации маломощных источников электромагнитного излучения в диапазоне от 50 МГц до 8000 МГц.

Анализатор поля позволяет выявлять закладные устройства, внедренные в выделенные помещения и на объекты информатизации и использующие для передачи информации радиоканал.

Работа анализатора основана на интегральном методе измерения уровня электромагнитного поля в точке его расположения. Прибор позволяет идентифицировать сигналы устройств сотовой и телефонных систем связи стандартов GSM-900, GSM-1800 (DCS), DECT, а также беспроводных систем связи Bluetooth и Wi-Fi (диапазон 2,4 ГГц).

Анализатор электромагнитного поля "КОРДОН" позволяет не только обнаружить излучение радиопередатчика, негласно установленного в выделенном помещении, но и измерить частоту его сигнала, а также оценить мощность электромагнитного излучения в точке приема

NR- μ нелинейный радиолокатор



Нелинейные локаторы предназначены для поиска электронных устройств, содержащих полупроводниковые компоненты.

Прибор применяется для обследования ограждающих конструкций, мебели, предметов интерьера, с целью выявления электронных устройств негласного получения информации, которые могут находиться как в рабочем, так и полностью отключенном состоянии.

При облучении внешним СВЧ сигналом, электронные устройства, содержащие полупроводниковые компоненты (диоды, транзисторы, микросхемы), переизлучают сигнал на удвоенной и утроенной частотах зондирующего сигнала, который принимается и анализируется детектором нелинейных переходов.

Одновременный прием второй и третьей гармоник зондирующего сигнала, визуальная и звуковая индикация уровней отраженных сигналов, а также режим анализа огибающей, позволяют оператору отличить сигналы, отраженные от электронных устройств, от сигналов естественных (коррозийных) нелинейных отражателей.

Высокий энергетический потенциал прибора (отношение мощности передатчика к чувствительности приемника ~ 146 дБ), обеспечивает эффективный поиск электронных устройств в массивных стенах, в том числе железобетонных, а также позволяет обнаруживать закладные устройства за армирующей сеткой.

Прибор обеспечивает возможность работы в условиях помех от сигналов сотовой связи стандарта GSM-1800.

«ВОРОН» ПРИБОР ОБНАРУЖЕНИЯ СКРЫТЫХ ВИДЕОКАМЕР



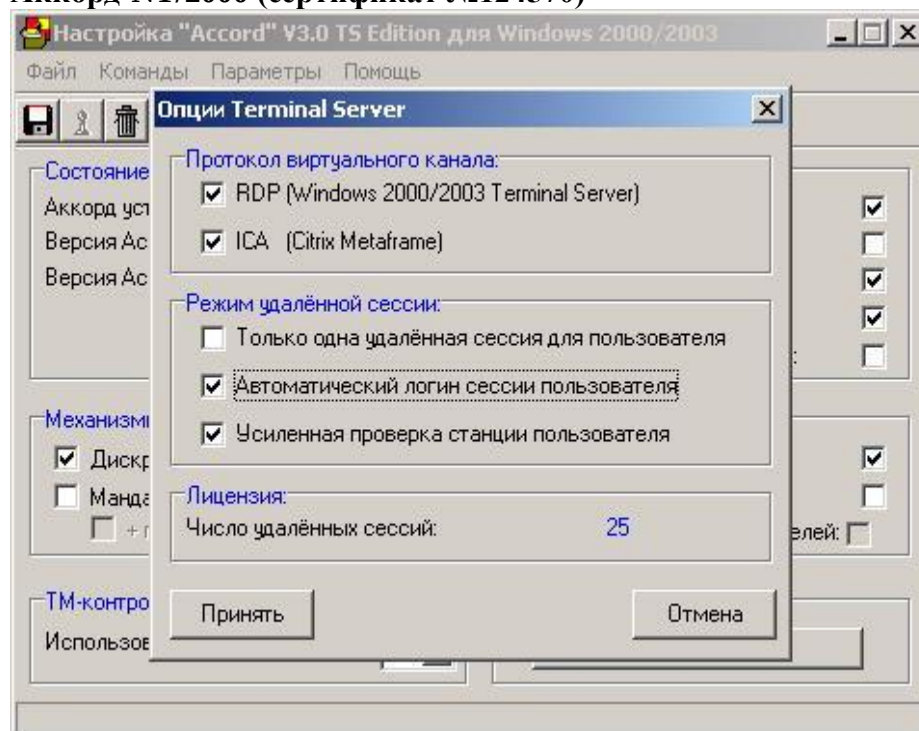
Предназначен для быстрого обнаружения и определения местоположения скрытых (камуфлированных в различные предметы интерьера и одежды) микровидеокамер, в том числе с объективами типа "Pin-hole".

Предназначен для быстрого обнаружения и определения местоположения скрытых (камуфлированных в различные предметы интерьера и одежды) микровидеокамер, в том числе с объективами типа "Pin-hole". Принцип обнаружения видеокамер основан на эффекте световозвращения или "обратного блика", когда луч от источника света, находящегося на оптической оси видеокамеры, отражается объективом и фотоприемником видеокамеры, как зеркалом, и направляется обратно на источник света. Поэтому, в случае обнаружения скрытой цели, в поле зрения прибора наблюдается яркое точечное пятно красного цвета (отражение от объектива видеокамеры).

Дальность обнаружения объективов скрытых видеокамер типа Pin-Hole (о 1 мм) составляет от 1 до 20 метров в зависимости от условий применения. "ВОРОН" использует светодиодную подсветку целей, что гарантирует безопасность эксплуатации и отсутствие вредного воздействия на человека (в отличие от лазерной подсветки).

Работа прибора в оптическом, а не радиочастотном диапазоне, позволяет обнаруживать любые оптические устройства (в том числе видеокамеры), независимо от их состояния (включено/выключено) и типа передачи информации (по радиоканалу или кабелю).

Аккорд-NT/2000 (сертификат №124570)



Программно-аппаратный комплекс средств защиты информации предназначен для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам. Комплекс работает на всей ветви операционных систем (ОС) Microsoft Windows

ПАК СЗИ Аккорд-МТ/2000 V3.0 предназначен для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам. Комплекс работает на всей ветви операционных систем (ОС) Microsoft NT +, на терминальных серверах, построенных на базе ОС Windows 2000 Advanced / Server и на базе серверов семейства Windows 2003, а также ПО Citrix Metaframe XP и XenApp 5, работающем на этих ОС.

ПАК СЗИ НСД Аккорд включает в себя Аккорд-АМДЗ, обеспечивающий доверенную загрузку ОС, и ПО разграничения доступа, которое обеспечивает:

- создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
- запрет запуска неразрешенных программ;
- разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа;
- разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа;
- автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса;
- усиленную аутентификацию терминальных станций с помощью контроллера Аккорд или ПСКЗИ ШИПКА;
- идентификацию/аутентификацию пользователей, подключающихся к терминальному серверу (с использованием ТМ-идентификатора или ПСКЗИ ШИПКА);
- опциональную автоматическую идентификацию в системе Windows и на терминальном сервере пользователей, аутентифицированных защитными механизмами контроллера АМДЗ (избегая повторной идентификации пользователей, можно гарантировать, что ОС будет загружена под именем того же пользователя, который был аутентифицирован в контроллере АМДЗ, и к терминальному серверу подключится тот же самый пользователь);
- управление терминальными сессиями;

контроль целостности файлов, ключей реестра, контейнеров при запуске сессии пользователя, а также проверку контрольных сумм процессов при их запуске и проверку данных с указанным интервалом времени;
контроль доступа к USB-устройствам;
маркировку и учет документов, выводимых на печать (любые документы из любых приложений на любое устройство печати - принтеры с любым размером бумаги, плоттеры и т. д.).

Аккорд-РАУ (распределенный аудит и управление)



Объединяет АРМ администратора безопасности информации и пользовательские терминалы, оснащенные СЗИ семейства АККОРД.

Может выполнять следующие функции:

- Оперативное наблюдение
- Оперативное управление
- Удаленное администрирование

По мере роста объема и сложности автоматизированных систем выполнение функций, возложенных на администратора безопасности информации - организация применения средств защиты и управление ими, контроль за соблюдением пользователями требований безопасности информационных ресурсов АС, - становится задачей все более сложной и трудоемкой.

Для автоматизации управления защитой информации в АС предназначена подсистема «Аккорд-РАУ». Она объединяет Автоматизированное рабочее место администратора безопасности информации (АРМ АБИ) и пользовательские терминалы, оснащенные СЗИ семейства АККОРД.

Система управления защитой информации может быть надежной только в том случае, если она построена на базе защищенного обмена данными, в противном случае, она лишь увеличивает уязвимость АС.

Подсистема Аккорд-РАУ построена на основе комплекса Аккорд-AsXNet, обеспечивающего защищенный обмен данными по сети, и ПО АРМ АБИ.

Использование ПК с внедренными средствами защиты не требует изменения существующего программного обеспечения.

С помощью АРМ администратор безопасности информации может выполнять следующие функции:

Оперативное наблюдение

В рамках оперативного наблюдения за работой пользователя можно:

получать информацию о том, кто работает на данной станции, о версии ОС, под управлением которой идет работа, о списке задач, которые выполняются на этой станции в текущий момент времени;

просматривать все события подсистемы разграничения доступа со всех станций в одном окне;

при необходимости детального анализа работы одной станции, получать все поступающие события в отдельное окно;

выбирать для просмотра только те рабочие станции или только те события, которые в данный момент представляют особенный интерес;

оперативно изменять уровень детальности журнала на рабочих станциях;

просматривать экран выбранной рабочей станции;

просматривать диски рабочих станций (до уровня файлов).

Оперативное управление

Оперативное управление работой пользователя - это возможность:

посылать пользователю сообщения;

обмениваться с пользователем файлами;

включать пользователю Screensaver, который может быть разблокирован только ТМ-идентификатором АБИ;

управлять «мышью» и клавиатурой рабочих станций;

перегружать рабочие станции.

Удаленное администрирование

Централизованный сбор журналов регистрации

Работа со списком зарегистрированных рабочих станций

«СГУ-2» можно использовать для уничтожения информации с грифами конфиденциально, секретно и совершенно секретно.

Защита информации
www.cobra.ru

СПИРАН
СЕРВИС-ЦЕНТР
ПО ЗАЩИТЕ ИТ, Д. 30

НИО ПИБ
(812) 336-43-40
(812) 336-15-30

АУРА

Дает возможность построения автоматизированных систем отвечающих классу 1Б, 1В, 1Г, 1Д и информационных систем по обработке персональных данных по классам К1, К2, К3, К4.

СТРАЖ NT 3.0 (сертификат №2145)



Предназначена для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах и информационных системах персональных данных. Функционирует в среде 32-разрядных операционных систем MS Windows.

Организация работы с конфиденциальными документами.

Источник - users.g.com.ua

Установление порядка секретного делопроизводства.

Во время работы по защите коммерческой тайны необходимо обратить особое внимание на документы фирмы, поскольку большинство коммерческих структур в нашей стране основные объемы коммерческой информации, в том числе конфиденциальной, хранят в документах. Руководитель фирмы должен упорядочить соответствующим образом процессы фиксации секретной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено настолько, чтобы оно становилось экономически невыгодным для похитителя.

При работе с документами, содержащими охраняемую фирмой информацию, надо соблюдать определенные правила. Это дает весомые гарантии надежной охраны коммерческих секретов и ставит заслон на пути утечки информации.

Эти правила сводятся к следующему:

- 1) строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;
- 2) точное установление того, кто конкретно из руководства и служащих фирмы организует и контролирует секретное делопроизводство фирмы, наделение их соответствующими полномочиями;
- 3) разработка инструкции (памятки) по работе с секретными документами, ознакомление с ней соответствующих работников фирмы;
- 4) контроль за принятием соответствующими служащими письменных обязательств о сохранении коммерческой тайны фирмы;
- 5) введение системы материального и иного стимулирования служащих фирмы, имеющих доступ к ее секретам;
- 6) внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;
- 7) личный контроль со стороны руководителя фирмы службы внутренней безопасности и секретного делопроизводства.

Вероятность утечки секретной информации из документов особенно велика в процессе их пересылки. Очевидно, что у коммерческих структур нет возможностей пользоваться услугами военнизированной фельдсвязи. По этой причине доставку секретных документов и ценностей надо организовать собственными силами, с привлечением охранников фирмы, или обращаться в те фирмы, которые такие услуги оказывают за плату.

Служащие фирмы, отвечающие за сохранность, использование и своевременное уничтожение секретных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но радикальным способом - хорошей платой за работу. В процессе хранения и пересылки секретных документов фирмы могут быть применены средства защиты и сигнализации о несанкционированном доступе к ним.

Одна из новинок - невидимое светочувствительное покрытие, наносимое на документы, которое может проявляться под воздействием света, указывая тем самым на факт несанкционированного ознакомления с документами или их фотографирования.

Используют в этих целях и электронику. На Всесоюзном семинаре по вопросам защиты коммерческой информации, состоявшемся летом 1991 г. в Москве, на стенде фирмы "Альянс" демонстрировалось несложное электронное устройство размером с пачку сигарет, изготовленное в одной из стран Юго-Восточной Азии. Устройство называется "Хоум детектив" (Домашний детектив), стоит всего 10 долларов США и реагирует на свет. Стоит включить устройство и в течение 20 сек. поместить его где-то в сейфе, под бумагами на рабочем столе, в его ящиках и в вашем распоряжении надежный электронный сторож. Он срабатывает при попадании слабого луча света и

подаст пронзительный звуковой сигнал. По желанию заказчика фирма снабжает "Хоум детектив" радиопередатчиком, включающим на значительном расстоянии иные защитные системы и внешнюю сигнализацию.

Специалистам по вопросам защиты коммерческой информации известны и иные технологии и системы охраны конфиденциальных документов фирмы от несанкционированного к ней доступа или возможной утечки из них охраняемых сведений. За информацией по данному вопросу следует обращаться в организации и службы, которые специально занимаются данной проблемой. Методы ведения секретного делопроизводства. Для ведения секретного делопроизводства должны привлекаться люди, прошедшие специальную проверку, и в честности которых нет никаких сомнений. Кроме того, эти люди должны быть соответствующим образом подготовлены и обучены, т.к. профессиональные недочеты и отступление от правил в их работе могут слишком дорого стоить фирме.

Помещения, в которых ведется работа с секретными документами, должны хорошо охраняться, а доступ в эти помещения должен быть закрыт для посторонних лиц. Помещения, в которых секретные документы хранятся, должны иметь прочные перекрытия и стены, усиленную металлическую дверь, прочные оконные рамы с двойными стеклами и решеткой, плотные шторы, не позволяющие вести просмотр помещения со стороны улицы. Хранилище секретных документов должно быть оборудовано охранной и пожарной сигнализацией и тщательно охраняться силами внутренней охраны. Доступ в хранилище должен быть строго ограничен. Не рекомендуется располагать такое помещение на первом и последнем этажах здания, т.к. это упрощает несанкционированный к нему доступ. Секретные документы хранятся в сейфах или несгораемых металлических шкафах с надежными замками и запорами.

Существуют различные приемы ведения секретного делопроизводства, которые направлены на предотвращение утечки содержащихся в документах коммерческих секретов. Например, документы, содержащие коммерческую тайну, подразделяются по степени секретности отображенной в них информации и снабжаются соответствующим грифом секретности. В Вооруженных Силах страны, к примеру, существуют следующие грифы секретности для документов: "СЕКРЕТНО", "СОВЕРШЕННО СЕКРЕТНО" и "ОСОБОЙ ВАЖНОСТИ". Кроме того имеется гриф "ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ" (ДСП), который выставляется на документах, не являющихся секретными, но содержащих информацию, разглашение которой было бы нежелательно.

Практика ведения секретного делопроизводства коммерческих структур показывает, что для надлежащего разделения информации по степени секретности, содержащейся в документах, вполне достаточно введение трех грифов : "ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ", "СЕКРЕТНО" и "СОВЕРШЕННО СЕКРЕТНО" (или им аналогичных, например: "СЛУЖЕБНАЯ ИНФОРМАЦИЯ", "КОНФИДЕНЦИАЛЬНО" и "СТРОГО КОНФИДЕНЦИАЛЬНО").

Рассмотрим методику ведения секретного делопроизводства на основе именно этих трех грифов. Прежде всего, следует отметить, что секретный документ (т.е. с грифами "СЕКРЕТНО" и "СОВ.СЕКРЕТНО") уже по внешнему виду должен отличаться от несекретного.

На обложке каждого такого документа должны содержаться следующие сведения:

1. В правом верхнем углу ставится гриф секретности (для этого предлагается изготовить штампы соответствующих грифов).

2. Под ним проставляется инвентарный номер данного документа, который фиксируется в КНИГЕ ЛИЦЕВЫХ СЧЕТОВ.

3. Если документ имеет гриф "СОВЕРШЕННО СЕКРЕТНО", рекомендуется проводить красную черту тушью из правого верхнего угла обложки в левый нижний для придания данному документу более значимого вида.

На титульном листе секретного документа обязательно дублируются гриф секретности и инвентарный номер, имеющиеся на обложке. Это делается на случай, если обложка документа вдруг оторвется.

Листы секретного документа нумеруются и прошиваются прочной ниткой, концы которой заклеиваются папиросной бумагой с оттиснутой на ней печатью "ДЛЯ ДОКУМЕНТОВ" (такую печать рекомендуется специально изготовить для того, чтобы постоянно не прибегать к основной Гербовой печати фирмы).

На последнем листе документа необходимо сделать следующую надпись:

В данном документе пронумеровано и прошнуровано _____ листов.
_____ (подпись ответственного лица)

Бывают случаи, когда в специальную папку вкладываются отдельные секретные листы, прошнуровать которые не представляется возможным. В этом случае в папку вкладывается (вклеивается) реестр, в котором учитываются все имеющиеся в папке секретные листы. Каждый листок получает гриф секретности и свой инвентарный номер, который отмечается в реестре по форме:

| инвент. № гриф секрет. название дата и подпись изъятия |

Сама такая папка получает гриф не ниже наиболее секретного в ней листка и собственный инвентарный номер, который учитывается в книге Лицевых счетов.

Черновики секретных документов фирмы должны готовиться в тетрадях с пронумерованными листами. После подготовки документов "набело" черновики должны уничтожаться уполномоченными на то служащими. Число копий секретных документов фирмы должно строго учитываться, а копировальные машины - снабжаться счетчиком копий и ключом, запускающим машины в действие. Копировальная бумага и красящая лента пишущих машин - предмет особых забот, так как с них можно снять секретную информацию. Поэтому использованная копировальная бумага и лента уничтожаются под контролем ответственных лиц.

Все секретные и сов.секретные документы обязательно учитываются в книге Лицевых счетов. Книга состоит из следующих разделов:

	инв.	№	название	гриф сек.	кол-во	листов	дата
получения	подпись	дата	изъятия	подпись			

Если в фирме имеется несколько филиалов, то в каждом из них заводится своя книга Лицевых счетов, а в главной Секретной части фирмы - Лицевые счета на каждый из филиалов. В итоге получается, что в фирме имеется одна Главная книга Лицевых счетов и по паре дополнительных на каждый филиал.

Книга Лицевых счетов на филиал, имеющаяся в Главной секретной части фирмы должна быть **СОВЕРШЕННО ЭДЕНТИЧНА** книге Лицевых счетов, остающаяся в данном филиале. Благодаря этому появляется возможность максимально четко контролировать перемещения секретных документов между филиалом и штаб-квартирой фирмы. Книга Лицевых счетов, как правило, имеет гриф "СЕКРЕТНО". Это связано с тем, что только упоминание где-либо или фиксация только названия сов. секретных документов уже само по себе содержит секретную информацию. Книга Лицевых счетов на филиал учитывается в Главной книге Лицевых счетов, а Главная книга - сама в себе под инв. N 1. Документы с грифом "ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ" также могут учитываться в специальной книге по принципу, изложенному выше, но не вместе с секретными и сов. секретными документами.

Руководство фирмы может издавать секретные приказы, которые касаются определенного контингента сотрудников и не должны быть известны всем остальным. Для выделения таких приказов от несекретных рекомендуется перед его номером ставить "О" в случае, если приказ секретный, и "ОО" - если приказ сов. секретный (например: N O14; N OO56-P). Учет таких приказов производится по правилам, установленным для документов с соответствующими грифами секретности. Этот же принцип можно использовать и для выделения секретных договоров от несекретных.

Иногда на практике коммерческим структурам приходится сталкиваться с необходимостью засекречивания не только документов, но и каких-либо изделий. Учет и работа с секретными изделиями строится по тому же принципу, что и с секретными документами с той лишь разницей, что необходимо предусмотреть систему опломбирования изделия так, чтобы не допустить несанкционированное проникновение внутрь изделия и ознакомление с его внутренней структурой. Пломбы рекомендуется применять также в отношении сейфов и дверей секретной части по окончании рабочего дня. Секретные документы выдаются только лицам, имеющим право на работу с этими документами. Внутри фирмы целесообразно ввести допуски на работу с секретными документами.

Например, в армии допуск N 3 соответствует праву на работу с документами с грифом "СЕКРЕТНО", допуск N 2 - документами с грифом "СОВЕРШЕННО СЕКРЕТНО", допуск N 1 - документами с грифом "ОСОБОЙ ВАЖНОСТИ". Работа с документами ДСП не требует специального допуска. Работник с допуском N 3 не имеет право пользоваться сов. секретными и особой важности документами, а работник с допуском N 2 не допущен к документам особой важности.

Система допусков позволяет максимально ограничить круг лиц, знакомых с секретами фирмы. Номер допуска определяется сроком службы в фирме данного сотрудника и степенью доверия к нему со стороны руководства. Все секретные документы выдаются только под роспись. Целесообразно на каждый документ завести карточку по форме:

гриф _____	кол-во листов _____	инвентарный N _____
(название документа) _____		
дата выдачи _____	подпись _____	дата возврата _____
подпись _____		

Рядовым работникам фирмы секретные документы выдаются только на время рабочего дня. В конце рабочего дня все секретные документы должны быть возвращены в Секретную часть (хранилище) фирмы.

Рассекречивание документов происходит либо по команде руководства фирмы, либо по истечении определенного срока путем понижения степени секретности и присвоения более низкого грифа. Установление контроля за публикациями.

Даже тщательно охраняемые тайны фирмы могут стать известны конкурентам из обычных публикаций для широкой публики, если пустить это дело на самотек. Поэтому один из служащих фирмы обязательно должен быть наделен самыми широкими властными полномочиями для того, чтобы заниматься предварительной цензурой готовящихся брошюр, рекламных объявлений, пресс-релизов и иных материалов для симпозиумов, выставок, конгрессов, а также выступлений, научных и иных публикаций сотрудников фирмы.

Интересы охраны секретов фирмы в подавляющем числе случаев находятся в трудно разрешимом противоречии с личными амбициями, самолюбием, академической независимостью сотрудников фирмы, желающих профессионально самоутвердиться в ученом мире, среди своих коллег, в общественном или групповом мнении. Не менее легок для разрешения конфликт между стремлением сохранить коммерческие тайны фирмы и желанием использовать в рекламных целях некоторые наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Сотрудник, осуществляющий цензуру открытых публикаций рекламного, научного и популяризаторского характера, готовящихся персоналом фирмы или по ее заказам, должен руководствоваться простым, но достаточно эффективным правилом. Суть его в том, чтобы В МАКСИМАЛЬНО ВОЗМОЖНОЙ СТЕПЕНИ РАЗДРОБИТЬ, РАЗОБЩИТЬ ПО ВРЕМЕНИ, В ПРОСТРАНСТВЕ И ПО АВТОРАМ ТУ СТРОГО ОХРАНЯЕМУЮ КОММЕРЧЕСКУЮ ИНФОРМАЦИЮ, без которой невозможно опубликование упомянутых выше работ. Конечно, все это затрудняет осуществление

персоналом фирмы научно-исследовательских и опытно-конструкторских работ, но зато существенно препятствует сбору секретной информации о фирме конкурентами и недоброжелателями. Этот барьер преодолим лишь посредством очень больших затрат.

Организация конфиденциального делопроизводства

В. Панкратьев

Источник - daily.sec.ru

Организации конфиденциального делопроизводства в информационной безопасности уделяется, как правило, наименьшее внимание, хотя получение конфиденциальной информации через пробелы в делопроизводстве является наиболее простым и малозатратным способом получения информации.

Составные части делопроизводства:

- бумажное делопроизводство;
- электронное делопроизводство;
- системы взаимодействия и сопряжения бумажного и электронного делопроизводства.

При ведении конфиденциального делопроизводства необходимо соблюдать следующие правила:

- присвоение и снятие грифа конфиденциальности должно осуществляться руководством компании;
- обязательная регистрация и учет всех конфиденциальных документов, а также передача их исполнителю под расписку в реестре;
- контроль не только документов, содержащих конфиденциальную информацию, но и бумаг с печатями, штампами, бланками, особенно бланков строгой отчетности, содержащих уникальный номер, зарегистрированных установленным способом и имеющих специальный режим использования;
- организационное выделение конфиденциального делопроизводства из обычного;
- гриф конфиденциальности документа присваивается по наивысшей степени конфиденциальности сведений, в нем изложенных;
- создание конфиденциальных документов производится в изолированных, специально оборудованных помещениях, прием и выдача документов производится через специальное окно, не выходящее в общий коридор или барьер, ограничивающий доступ к рабочим местам лиц, создающих конфиденциальные документы;
- уничтожение конфиденциальных документов, в том числе черновиков, в машинках для уничтожения бумаг (шредерах) в присутствии нескольких человек и с проставлением соответствующих пометок в журналах уничтожения конфиденциальных документов. При большом количестве документов возможно их сжигание;
- запрещение выноса из контролируемой территории конфиденциальных документов;
- к работе с конфиденциальными документами допускаются только лица, заключившие соответствующие договора о нераспространении коммерческой тайны;
- хранение конфиденциальных документов только в сейфах;
- в делах или в архивах конфиденциальные документы должны храниться отдельно от открытых, по завершении оформления дел на последнем листе делается запись о количестве пронумерованных в нем листов, заверенная соответствующей подписью и печатью;
- включать в документы только минимально необходимую конфиденциальную информацию;
- рассылка конфиденциальных документов должна быть обоснованной и сведена к минимуму;
- система учета (ручная или компьютерная) конфиденциальных документов должна предоставлять необходимые удобства поиска и контроля за местонахождением каждого конфиденциального документа;
- организационно исключить необоснованное ознакомление с документами лиц, не имеющих нужных полномочий;

- отправку конфиденциальных документов производить только заказными или ценными письмами, по каналам специальной связи или осуществлять доставку корреспонденции нарочным из числа сотрудников, допущенных к работе с такими документами;
- контроль за использованием копировально-множительной техники, а также блокирование систем ввода-вывода информации на компьютерах, обрабатывающих конфиденциальную информацию;
- организация периодической проверки делопроизводства.

Порядок создания бумажного делопроизводства

1 этап - создание Секретариата (подразделения, отвечающего за делопроизводство) или введение в штат должности, в чьи функциональные обязанности будет входить обеспечение делопроизводства организации.

2 этап - закупка необходимых принадлежностей для функционирования делопроизводства (сейфы, печати, оборудование помещений и т.д.).

3 этап - создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.).

4 этап - доведение нормативных документов до сотрудников в рамках функциональных обязанностей.

5 этап - создание механизмов контроля за соблюдением делопроизводства.

6 этап - создание механизма ответственности за нарушение правил делопроизводства.

Делопроизводство должно быть организовано в соответствии с ГОСТами, применяемыми в Российской Федерации. Основа - ГОСТ 6.30-97 <Унифицированные системы документации. Система организационно-распорядительной документации. Требования к оформлению документов>.

Порядок создания конфиденциального бумажного делопроизводства

1 этап - создание обычного бумажного делопроизводства.

2 этап - определение перечня сведений конфиденциального характера и документов, содержащих конфиденциальные сведения. Разделение сведений на несколько групп по степени конфиденциальности (например: строго конфиденциальные, конфиденциальные, для служебного пользования).

3 этап - утверждение перечня сведений конфиденциального характера у руководства, а также определение порядка и сроков переутверждения данного перечня, а также снижение и снятие грифа конфиденциальности.

4 этап - определение правил конфиденциального бумажного делопроизводства на основе общего бумажного делопроизводства.

5 этап - определение порядка допуска сотрудников к сведениям конфиденциального характера.

6 этап - заключение договоров о нераспространении конфиденциальных сведений между сотрудниками, которые будут допущены к работе с конфиденциальной информацией и руководством организации.

7 этап - создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.).

8 этап - доведение нормативных документов до сотрудников в рамках функциональных обязанностей.

9 этап - создание механизмов контроля за соблюдением конфиденциального делопроизводства.

10 этап - создание механизма ответственности за нарушение правил конфиденциального делопроизводства.

Составные части бумажного делопроизводства:

Делопроизводство, связанное со стандартными, но специфическими задачами:

- бухгалтерия;
- учредительные документы;

- судебно-процессуальные документы;
- договорные документы и т.д.

Делопроизводство, связанное с текущей деятельностью:

Внешнее делопроизводство:

- доставка входящей корреспонденции (в бумажном виде, в виде факса и т.д.);
- отправление исходящей корреспонденции (в бумажном виде, в виде факса и т.д.);

Внутреннее делопроизводство:

- хранение документов;
 - хранение документов у сотрудников;
 - хранение документов в Секретариате.
 - создание документов у исполнителя;
 - издание нормативных документов руководством организации (приказы, распоряжения и т.д.);
 - регистрация документа в Секретариате;
 - движение документа внутри организации. Создание реестровой системы передачи документов;
 - размножение документов (снятие копий);
 - контроль за исполнением документов;
 - создание архивов документов. Экспертиза ценности документов.
- Возможность использования в работе документов, определенных в архив;
- уничтожение документов.

Необходимые нормативные документы для функционирования делопроизводства, в том числе конфиденциального:

Нормативно-правовые документы организации с внесенными изменениями и дополнениями, связанными с сохранностью конфиденциальной информации:

- Устав организации;
- "Коллективный договор";
- правила внутреннего трудового распорядка для сотрудников;
- трудовой договор;
- заключаемые договора.

Договор между руководством организации и сотрудником о сохранении конфиденциальной информации.

Инструкция по обеспечению сохранности конфиденциальной информации в организации.

Примерный план инструкции:

- общие положения;
- определение информации и обозначение документов, содержащих конфиденциальную информацию, и сроков ее действия;
- организация работы с конфиденциальными документами;
- порядок сохранности документов, дел и изданий, содержащих конфиденциальную информацию;
- порядок допуска к сведениям, составляющим конфиденциальную информацию;
- контроль за выполнением требований внутри объектного режима при работе со сведениями содержащими конфиденциальную информацию;
- обязанности сотрудников организации, работающих со сведениями представляющими конфиденциальную информацию, и их ответственность за ее разглашение.

Инструкция по организации делопроизводства. Инструкция должна состоять из следующих разделов:

- общие положения;
- правила составления и оформления документов;

- составление и оформление основных видов документов;
- организация документооборота;
- порядок движения и обработки входящих документов;
- порядок движения и обработки исходящих документов;
- порядок движения и обработки внутренних документов;
- регистрация документов;
- контроль исполнения документов;
- систематизация документов;
- разработка номенклатуры дел;
- формирование дел;
- подготовка документов к архивному хранению;
- экспертиза ценности документов;
- описание документов постоянного и временного сроков хранения;
- обеспечение сохранности дел;
- передача дел в архив;
- приложения:
 - примерный перечень документов, не подлежащих регистрации;
 - перечень документов, на которых ставится печать;
 - перечень документов, подлежащих утверждению;
 - перечень документов, подлежащих согласованию;
 - форма регистрационно-контрольной карточки;
 - перечень документов, подлежащих контролю за исполнением, с указанием сроков хранения;
 - акт о выделении к уничтожению документов с истекшими сроками хранения;
 - внутренняя опись документов дела;
 - опись дел, передаваемых на архивное хранение.

Инструкция по конфиденциальному делопроизводству, определяющая:

- порядок выноса-вноса конфиденциальных документов применительно к охраняемой территории;
- порядок работы с конфиденциальными документами вне служебных помещений;
- порядок изготовления и использования бланков организации, печатей и штампов;
- порядок использования бланков строгой отчетности (бланков организации, подготавливаемых за подписью первых лиц организации);
- порядок передачи конфиденциальных документов в случае ухода в отпуск, командировку или увольнение с работы;
- порядок подготовки конфиденциальных документов, его согласование, в том числе с юристами, финансистами, корректорами, а также порядок подписи конфиденциальных документов;
- порядок пересылки конфиденциальных документов вне контролируемых помещений.

Положение о Секретариате (подразделении отвечающего за бумажное и электронное делопроизводство).

Должностные обязанности сотрудников Секретариата по обеспечению делопроизводства.

Корпоративное конфиденциальное электронное делопроизводство должно состоять из следующих взаимосвязанных систем:

- системы электронного конфиденциального документооборота;
- системы защиты информации, циркулирующей в системе электронного конфиденциального документооборота;
- системы электронного конфиденциального информационного хранилища;

- системы сопряжения конфиденциального электронного и бумажного документооборота.

Система электронного конфиденциального документооборота должна предусматривать следующие возможности:

- возможность создания электронных документов с помощью текстовых редакторов, включая создание электронных документов по типовым формам;
- возможность создания составных электронных документов, состоящих из нескольких разных по формату файлов;
- возможность создания электронных документов с помощью сканирования документа на бумажном носителе;
- возможность создания электронных документов с помощью иных электронных данных, полученных с помощью:
 - электронной почты;
 - корпоративной компьютерной сети;
 - устройств ввода компьютерной информации (дисководы и т.д.).
- работу с электронными документами различных форматов (текстовых, графических и т.д.).
- создание регистрационной карточки электронного документа, связи регистрационной карточки с электронным документом и присвоение необходимых реквизитов, среди которых:
 - дата создания, получения, исполнения;
 - регистрационный номер;
 - фамилия, имя, отчество исполнителя, адресата;
 - права доступа;
 - степень конфиденциальности;
 - количество листов и т.д.
- разделения документов по степени конфиденциальности, присвоение каждому документу грифа конфиденциальности и разграничение права пользователей работы с конфиденциальными документами по мандатному принципу.
- получения и отправления электронных документов (документооборот) по корпоративной компьютерной сети, а также по электронной почте.
- работы с взаимосвязанными документами, поддержание возможности установления ссылок между учетными карточками или документами, связанных тематически, отменяющих или дополняющих друг друга (например с помощью гиперссылок с возможностью просмотра цепочки взаимосвязанных документов).
- контроля передвижения электронных документов по сети и контроля ознакомления с электронными документами, а также контроля за копированием, редактированием и размножением электронных документов.
- осуществления контрольных функций (контроля исполнения резолюций, поручений, сроков исполнения и т.д.), а также возможность сигнального режима, как составной части контроля.
 - поиска электронных документов по:
 - реквизитам;
 - ключевым словам;
 - содержанию;
 - дате создания;
 - контрольным срокам;
 - исполнителю и т.д.
 - анализа электронных документов по:
 - тематике;
 - проблематике;
 - исполнителям;
 - резолюциям;
 - дате создания и т.д.

- дублирования (архивирования) электронных документов с заданной периодичностью, а также ведение систематизированных электронных архивов документов, их образов, учетных карточек с возможностью поиска и анализа.

- разделение конфиденциального и открытого электронного делопроизводства.

Система конфиденциального электронного информационного хранилища должна предусматривать возможность:

- систематизирования поступающих в хранилище документов различных видов и форм и упорядочения работы с ними;

- гарантированно сохранять документы в массивах хранилища, освободив от этой функции сотрудников;

- отслеживать движение документов, выдаваемых сотрудникам, контролировать и обеспечивать их возврат (физические документы) и уничтожение выданных электронных копий;

- обеспечивать эффективный поиск нужных документов в хранилище по идентификационным признакам;

- организовать малозатратную технологию выдачи документов сотрудникам и возврат документов в хранилище;

- уменьшить количество документов, одновременно находящихся у исполнителя за счет оперативного их получения из хранилища;

- упростить работу с документами, находящимися в хранилище, и сократить временные затраты на их подборку и анализ за счет дружественного интерфейса в интерактивном режиме;

- обеспечить режим безопасности документов в процессе их хранения, передачи в хранилище или получения из хранилища за счет использования современных технологий и средств информационной безопасности, а также разграничение доступа пользователей.

Система защиты конфиденциального электронного делопроизводства должна состоять из следующих взаимосвязанных блоков:

- блок технических (программных) средств защиты электронного делопроизводства;

- блок технических средств защиты электронного делопроизводства, связанных с нейтрализацией побочных электромагнитных излучений и наводок;

- блок методов защиты электронного делопроизводства, связанных с человеческим фактором и решением кадровых вопросов;

- блок организационных методов защиты электронного делопроизводства.

Блок технических (программных) средств защиты электронного делопроизводства должен быть многорубежный. Наиболее эффективной является система, состоящая из 3 рубежей:

1 рубеж - системы защиты информации, предусмотренные программным обеспечением, на которой работает компьютерная сеть (средства защиты Windows, Office и т.д.);

2 рубеж - системы защиты информации, встроенные в саму систему электронного делопроизводства;

3 рубеж - системы защиты информации, дополнительно установленные в компьютерной сети на сервере и на рабочих местах пользователя

Блок технических (программных) средств защиты электронного делопроизводства должен предусматривать:

- криптографическую защиту компьютерной информации на магнитных носителях (жестких дисках, дискетах, Zip, CD-ROM и т.д.), в том числе создание защищенных <цифровых сейфов> пользователей на сервере;

- защиту информации (в том числе криптографическими методами) при пересылке по корпоративной компьютерной сети;

- защиту информации (в том числе криптографическими методами) при передаче по электронной почте;
- защиту компьютерной информации от несанкционированного доступа;
- защиту компьютерной сети при работе в глобальной информационной сети Интернет (в идеальном случае для работы с Интернетом, а также с электронной почтой необходим отдельный компьютер, работающий в автономном режиме);
 - мандатный принцип доступа пользователей к информационным ресурсам электронного делопроизводства, включающий в себя:
 - контроль и защиту электронного документа от просмотра;
 - контроль и защиту электронного документа от редактирования и отмена защиты от редактирования;
 - контроль и защиту электронного документа от копирования и распечатывания на принтерах;
 - разделение пользователей на группы и наделение каждой группы возможности работы только с электронными документами определенного грифа конфиденциальности
 - контроль целостности и достоверности электронного документа, а также подтверждение авторства исполнителя с помощью электронной цифровой подписи;
 - защиту от вредоносных программ (вирусов);
 - парольную защиту на включение машины, на обращение к жесткому диску и/или на открытие файлов прикладных программ с периодическим изменением используемых паролей.

Системы сопряжения электронного и бумажного делопроизводства состоят из:

- системы перевода бумажного документа в электронный документ;
- системы перевода электронного документа в бумажный документ;
- системы электронного контроля за бумажным документооборотом;
- системы параллельного хождения одного и того же документа в электронном и бумажном виде.

Представляется целесообразным хождение документа внутри организации осуществлять в электронном виде. Полученные в бумажном виде документы извне сканируются и дальнейшая работа с ними происходит в электронном виде. Полученные извне электронные документы обрабатываются в организации в электронном виде. Перед отправкой исходящие документы (письма, факсы) преобразуются из электронного в бумажное представление и их отправка производятся обычными способами. При необходимости возможна отправка документа и в электронном виде.

Об авторе: Панкратьев Вячеслав Вячеславович, преподаватель курса "Корпоративная безопасность" в:

- Институте бизнеса и делового администрирования Академии народного хозяйства при Правительстве РФ;
- Высшей школе международного бизнеса Академии народного хозяйства при Правительстве РФ;
- Высшей школе корпоративного управления Академии народного хозяйства при Правительстве РФ;
- Центре коммерциализации технологий Академии народного хозяйства при Правительстве Российской Федерации;
- Центре международного бизнеса и регионального развития Академии народного хозяйства при Правительстве Российской Федерации;
- Академии народного хозяйства при Правительстве РФ (факультет академических программ обучения);
- Академии народного хозяйства при Правительстве РФ (факультет финансового и банковского дела);
- Академии народного хозяйства при Правительстве РФ (факультет государственного управления);

- Высшей коммерческой школе Министерства экономического развития и торговли РФ;
- Высшей школе бизнеса Московского государственного университета;
- Классической бизнес-школе (до 2000 года)

Данный материал является частью выпускаемого автором методического пособия по корпоративной безопасности. По вопросам заказа полного текста методического пособия, а также по вопросам преподавания и консультаций с автором можно связаться по E-mail: kotakkel2@mtu-net.ru.

3.4. Защита от компьютерных вирусов.

Работу на компьютере в условиях сегодняшней действительности можно характеризовать как угодно, только не определением «скучно-будничная». Расслабиться нам не дают как всевозможные проблемы, «подбрасываемые» прикладными программами либо операционной системой, так и компьютерные вирусы, огромная армия которых угрожает результатам нашего труда. Наряду с ростом числа пользователей в мире непрерывно растёт и число людей, развлекающихся созданием и распространением всяческой «электронной заразы». Спасти от нее можно, либо вообще не получая на компьютер информацию в электронной форме, либо используя специальные программы, предназначенные для борьбы с вирусами.

Сергей Потресов

Если быть объективными, то распространению разной вирусной пакости способствуем и мы с вами причём в большинстве случаев об этом даже не дозревая: происходит это просто через обмен файлами, которые, как оказывается, уже были заражены.

Кто и зачем создаёт многочисленные компьютерные вирусы? Сегодня — все кому не лень. Несколько лет назад для написания мало-мальски грамотного вируса требовались определённая квалификация и навыки, «вирусописатели» собой весьма гордились и даже пытались создавать своего рода закрытые «клубы для посвящённых». Сейчас существует достаточно много всякого рода «сервисных» программ, позволяющих создавать новые вирусы-клоны на основе уже существующих, и ещё больше оказывается желающих эти-ми программами воспользоваться. На вопрос «зачем - ответить труднее: зачем на чистой свежеекрашенной поверхности пишут разные, не всегда приличные слова (и самый безобидный вариант — «Здесь был Вася!»)? Иногда вирусы создают из идеологических соображений: так, определённую известность получил вирус, без ведома пользователя добавлявший в каждой напечатанный документ фразу «А также я требую прекратить испытания ядерного оружия в Тихоокеанском регионе!». Однако морально-этические аспекты проблемы выходят за рамки данного материала. Нас интересует более прозаический вопрос: как уберечь свою машину от электронной напасти?

Что такое компьютерный вирус?

Распространившаяся среди многих пользователей компьютеров «вирусофобия» зачастую принимает самые неожиданные формы вплоть до боязни включить компьютер вообще. Заявляем с полной ответственностью: человеку компьютерный вирус (программа) не передаётся, и в этом смысле пользователю ничто не угрожает, разве что нервный срыв или подскочившее давление из-за погубленных результатов многомесячного труда.

Компьютерный вирус, как правило, представляет собой некую программу, способную самостоятельно размножаться и которая в большинстве случаев снабжена соответствующими механизмами для распространения своих копий на другие компьютеры через Интернет или по локальной сети. В качестве «довеска» вирус часто (но не всегда!) несет в себе определённые деструктивные функции, причём разные его модификации могут совершать самые разнообразные действия на заражённом компьютере. Иногда вирус просто в бешеном темпе размножается, рассылая себя по всем электронным адресам, какие только сможет обнаружить в компьютере «жертвы». При всей кажущейся безобидности таких действий последствия могут оказаться катастрофическими из-за возросшей в сотни раз нагрузки на сеть и почтовые серверы. К сожалению, намного чаще компьютерный вирус производит те или иные разрушительные действия: портит или стирает документы, разрушает программы, выводит из строя операционную систему. Отдельные особо «злобные» разновидности даже выводят из строя аппаратную часть компьютера, принося тем самым значительные убытки.

Чаще всего программа-вирус существует в виде файла, который требуется

запустить, или некой добавки к документу, который необходимо открыть. Некоторые последние «модели» вирусов физически (т. е. в виде файлов) как бы не существуют: в компьютер передаются по сети определенные данные, которые из-за ошибок в программном обеспечении (так называемых дыр в защите) загружаются в оперативную память и начинают исполняться, как обычная программа, со своим «центром управления» в оперативной памяти компьютера. При этом не создается никаких файлов и на жесткий диск ничего не записывается.

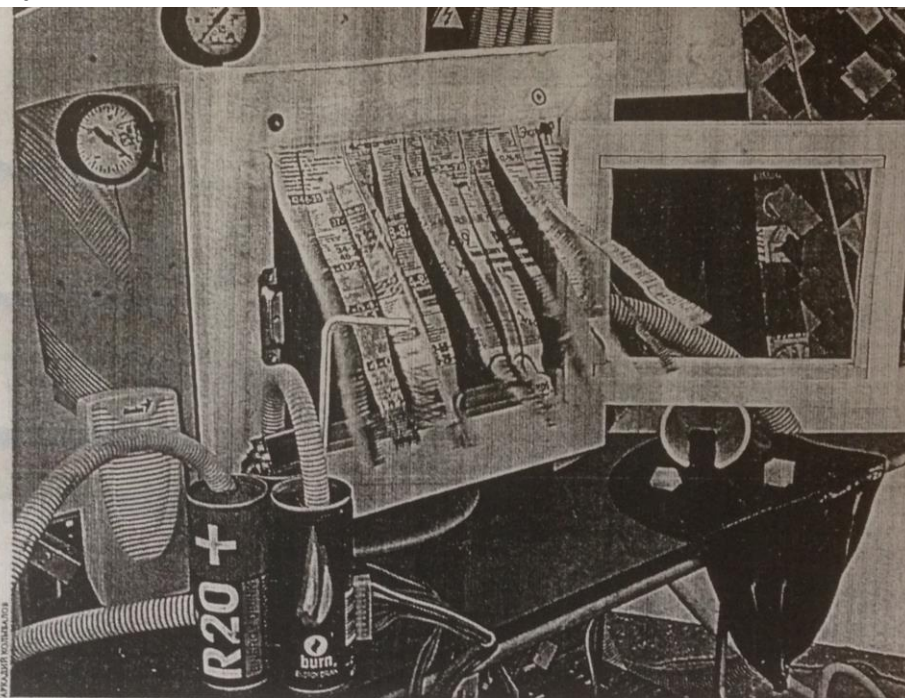
Антон Благовещенский

Если раньше вредоносные программы для компьютера были просто результатом шалостей ленивых программистов, то теперь это серьезный криминальный бизнес, в котором может быть замешан любой пользователь ПК.

Сравнительно недавно, в середине и конце 90-х годов, так называемые компьютерные вирусы в большинстве своем создавали студенты или изыскивающие от безделья программисты, решившие попробовать свои силы. В те времена вирус представлял собой программу, которая уничтожала файлы на компьютере, тормозила его работу и вообще мешала жить.

Но времена изменились. Компьютеры стали значительно «умнее» и многократно увеличили свои вычислительные способности. Доступом в Интернет обзавелись не только «избранные», но и вполне обычные люди — выходить в Сеть на приемлемой скорости могут примерно 50 млн человек в России. Появились электронные деньги, многие интернет-магазины начали принимать к оплате банковские карты.

Так что нет ничего удивительного в том, что и вредоносные программы претерпели серьезные изменения. Теперь они занимаются тем, что крадут конфиденциальную информацию (имена, пароли, данные о пластиковых картах) и «заражают» пользовательский компьютер, превращая его в инструмент для совершения киберпреступлений. Одни внедряются на компьютер и воруют персональные данные, другие превращают ПК в «компьютер-зомби», который незаметно для владельца веером рассылает рек-



сы именно с его помощью. Обычно они проникают в компьютер посредством электронной почты, через зараженные сайты или вместе с загруженными из Сети программами. Кроме того, недоработки («дыры») в установленных на компьютер программах также могут использоваться для того, чтобы поселить злонамеренную утилиту в недрах ПК. Наконец, не стоит забывать и о том, что USB-накопители, или флешки, пришедшие на смену компакт-дискам, также могут быть заражены.

Пользователь вводит эти данные, не подозревая, что сайт — поддельный и предназначен для кражи паролей. Поэтому стоит внимательно проверять, правильно ли написан адрес сайта.

Кроме того, при щелчке по ссылке, которая пришла по электронной почте, может открыться не сайт-подделка, а зараженный сайт, с которого на компьютер без ведома пользователя загружается программа, которая может украсть пароль и передать его своему «хозяину», или же вредоносный вирус, использующий ресурсы ком-

Вирус не муха. В форточку не выгонишь, dustom не возьмешь. Нужны тонкие технологии.

иболее свежие версии программ. Особенно это касается сложных продуктов известных разработчиков — например, Microsoft Windows и Office (update.microsoft.com).

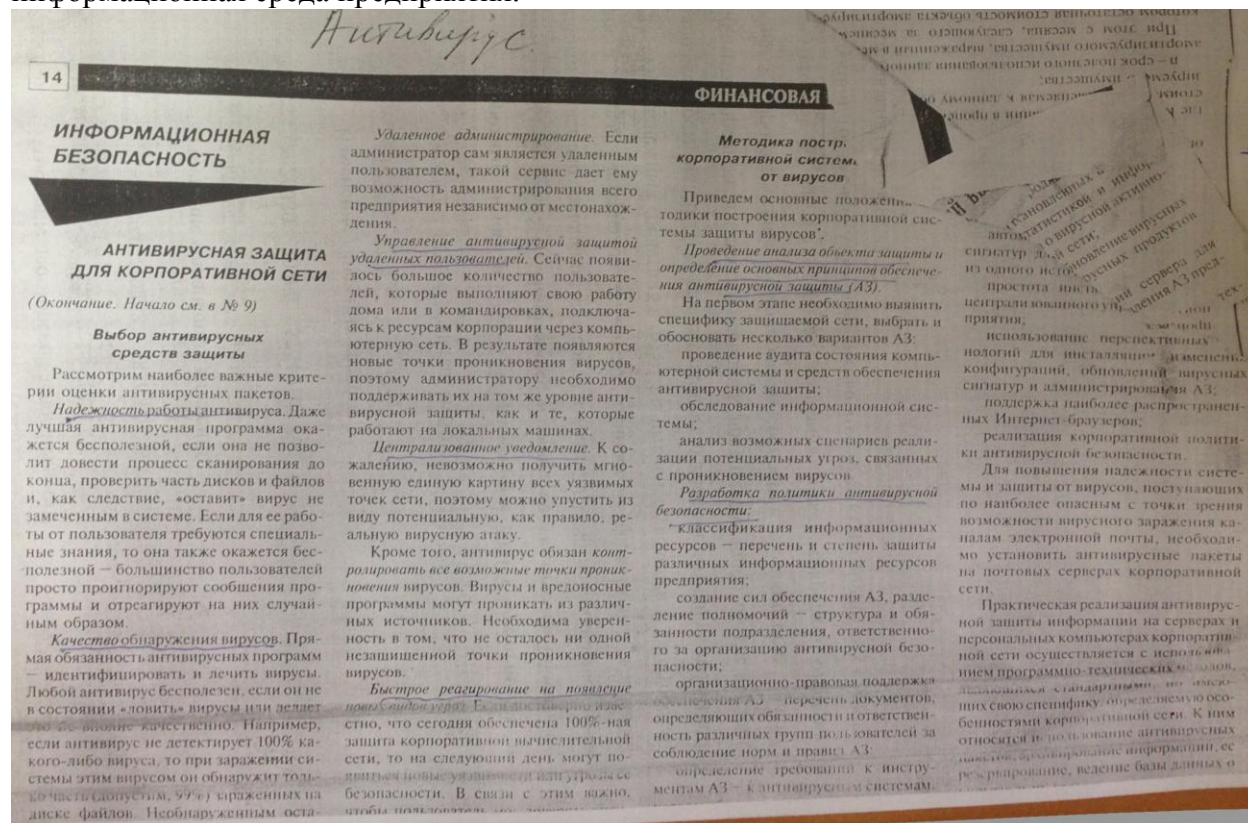
Подведем итог, атаки и воздействия на вычислительную технику существовали всегда. Стоило только появиться первым компьютерам, которые начали обрабатывать конфиденциальную информацию, как они сразу же привлекли внимание «плохих парней», выбравших их в качестве мишени для своих неблагоприятных дел. Соответственно возникла потребность в обнаружении и нейтрализации таких атак. Но все подвержено эволюции и в настоящее время существует множество различных программ для обеспечения информационной безопасности, о которых рассказано далее.

Основными тенденциями в развитии вредоносных программ, выявленными в прошлые годы, являлись преобладание троянских программ над «червями» и увеличение в новых «зловредах» доли программ, ориентированных на нанесение финансового ущерба пользователям. Рост числа всех новых вредоносных программ по сравнению с 2005 г. составил 41%.

В настоящее время эффективное построение системы антивирусной защиты является одной из приоритетных проблем комплексной безопасности корпоративных информационных ресурсов предприятия.

Установка антивирусных пакетов на серверах и компьютерах сети позволяет

значительно снизить риск вирусного заражения, но не исключает его полностью в силу ряда случайных факторов: ошибок пользователей, неправильных настроек, несвоевременности обновления антивирусных баз пакета и т.д. Следовательно, чем больше будет выделено ресурсов, чем профессиональнее будут специалисты, по антивирусной защите, тем меньше будет размер риска, которому подвергается информационная среда предприятия.



Начиналось все в самом конце далеких уже 70-х. когда специалист по компьютерной безопасности Джеймс Андерсон задумался о возможных способах обнаружения действий, нарушающих политику безопасности. И такой способ был найден - анализ журналов регистрации в поисках следов несанкционированной активности. Собственно, уже тогда выявилось отличие систем обнаружения атак от средств защиты, построенных на применении моделей разграничения доступа.

В этих моделях доступ к чему-либо разрешается после прохождения процедуры установления подлинности (аутентификации). Стоит вам предъявить пароль, неважно как и откуда полученный, — и система разграничения доступа пропустит вас ко всем ресурсам (разумеется, в рамках прав того пользователя, чей пароль используется). А дальше вы можете творить все что угодно. Принцип работы систем обнаружения иной. Им абсолютно все равно, кто выполняет несанкционированные действия: рядовой пользователь или администратор. В этом их преимущество перед другими защитными технологиями — авторизация, аутентификация, контроля доступа, межсетевое экранирование и т.п.

Предложенный Андерсоном подход оказался не утопией, а мощным инструментом в борьбе со злоумышленниками. Требование наличия и использования журналов регистрации всех событий вошло во все существующие стандарты информационной безопасности — в «Оранжевую книгу» (1985), в руководящие документы почившей ныне в базе Гостехкомиссии России (1992), в Общих критериях (1996) и ISO 17799 (1999). Первый прототип системы, использующей идеи Андерсона, появился в 1983-1985 годах, после чего такие системы посыпались как из рога изобилия. Особняком стоят системы обнаружения мошенничества (fraud detection), которые появились в то же время и...

Наиболее популярные антивирусные программы

Антивирусная программа (антивирус) - программа которая пытается

обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы с зараженного компьютера, а также служит для профилактики - предотвращения заражения файлов вирусами.

Первые антивирусные программы появились практически сразу после появления первых вирусов. Сейчас разработкой антивирусных программ занимаются крупные компании. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

Практически все современные антивирусы не ограничиваются защитой только от вирусов, а детектируют так же троянские программы и некоторые другие.

В основу практически всех антивирусов входит:

- * ядро;
- * сканер;
- * монитор активности;
- * модуль обновления.

Принцип работы практически всех антивирусов следующий:

- * Найти и удалить инфицированный файл;
- * Заблокировать доступ к инфицированному файлу;
- * Отправить файл в карантин (т.е. недопустить дальнейшего распространения вируса);
- * Попыаться "вылечить" файл, удалив вирус из тела файла;
- * В случае невозможности лечения-удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Для того, чтобы антивирусная программа постоянно успешно работала, *ф* необходимо базу сигнатур вирусов периодически загружать (обычно, через Интернет).

Для успешной защиты компьютера от вирусов желательно поставить Один "антивирус" и Один "firewall" (сейчас уже есть антивирусные программы которые предоставляют комплексную защиту - совмещая в себе и то и другое), если поставить больше то они не смогут работать вместе и это будет вызывать "зависание" компьютера и постоянное торможение, что только ухудшит защиту.

На сегодняшний день список антивирусных программ весьма огромен. Они различаются как по своим функциональным возможностям, так и по цене. Существуют конечно и бесплатные версии антивирусных программ.

Далее представлен список наиболее популярных антивирусных программ на сегодняшний день:

Антивирус Касперского - продукт для защиты вашего ПК, чья эффективность проверена миллионами пользователей во всем мире. Программа включает в себя основные инструменты для защиты ПК.

Страница разработчика: www.kaspersky.ru

ESET NOD32 обеспечивает обнаружение и блокировку вирусов, троянских программ, червей, шпионских программ, рекламного ПО, фишинг-атак, руткитов и других интернет-угроз, представляющих опасность для компаний. Несмотря на минимальную потребность в ресурсах, данное решение обеспечивает непревзойденный уровень проактивной защиты, практически не снижая производительность компьютера.

Страница разработчика: www.eset.com

Symantec Norton Anti-Virus

Разработанная компанией Symantec программа Norton AntiVirus является наиболее популярным антивирусным средством в мире. Эта программа автоматически удаляет вирусы, интернет-червей и троянские компоненты, не создавая помех работе пользователя. Norton AntiVirus позволяет противостоять угрозам самых современных spyware- и adware-программ и блокирует работу таких программ еще до того момента, как пользователь перенаправляется на другой сайт.

Страница разработчика: www.symantec.com

Dr. Web

Антивирус Dr.Web проверит всю Windows память даже зараженного компьютера. Доктор Веб проводит полную антивирусную проверку Windows-памяти компьютера и способен остановить вирусный процесс. Важным показателем качества работы антивирусной программы является не только ее способность находить вирусы, но и лечить их, не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное "здоровое" состояние.

Страница разработчика: www.drweb.ru

Trend Micro Internet Security позволяет очень просто защитить ваш компьютер, ваши приватные персональные данные и вашу онлайн-активность. Продукт обеспечивает защиту как от существующих вирусов, программ-шпионов и кражи данных, так и от будущих веб-угроз. Пользуйтесь электронной почтой, интернет-магазинами, онлайн-банкингом, обменивайтесь цифровыми фотографиями и не беспокойтесь о безопасности вашей приватной информации.

Страница разработчика: www.ru.trendmicro.com

Avast! Professional Edition вобрал в себя все высокопроизводительные технологии для обеспечения одной цели: предоставить вам наивысший уровень защиты от компьютерных вирусов. Данный продукт представляет собой идеальное решение для рабочих станций на базе Windows. Новая версия ядра антивируса avast! обеспечивает высокий уровень обнаружения вкупе с высокой эффективностью, что гарантирует 100%-ое обнаружение вирусов "In-the-Wild" и высокий уровень обнаружения троянов с минимальным числом ложных срабатываний. Механизм антивирусного ядра сертифицирован ICSA, постоянно принимает участие в тестах VirusBulletin и получает награды VB100%. Внешний вид пользовательского интерфейса отображается с помощью так называемых скинов, поэтому у вас есть возможность настроить внешний вид панели продуктов avast! по своему желанию.

Страница разработчика: www.avast.ru

BitDefender Antivirus - мощная антивирусная программа с разнообразными возможностями, позволяющими оптимально защитить персональный компьютер. BitDefender Antivirus защищает от компьютерных вирусов с применением технологий ICSA Labs, Virus Bulletin, Checkmark, CheckVir и TUV. Модуль B-HAVE подражает действительному (виртуальному) "компьютеру в компьютере". Эта BitDefender-технология представляет новый уровень безопасности, обнаруживая и обезвреживая даже редкие вирусы, или вирусный код, для которого еще не вышли новые базы записей вирусов.

Страница разработчика: www.bitdefender.com

Panda Antivirus является самым простым и интуитивно понятным в использовании решением безопасности для домашнего ПК. После установки программы пользователь может забыть о вирусах, программах-шпионах, руткитах, хакерах, онлайн-мошенниках и больше не беспокоиться о сохранности конфиденциальной информации.

Panda Antivirus имеет простые настройки, легкий и понятный интерфейс, автоматическое обновление (после установки сразу будет искать обновления), осуществляет контроль на уровне TCP/IP. Panda Antivirus является достаточно надежным антивирусом подойдет в первую очередь для домашнего пользования
Страница разработчика: <http://www.viruslab.ru/>

McAfee VirusScan

Продукт McAfee VirusScan осуществляет сканирование файловых серверов[^] и рабочих станций по расписанию и по запросу пользователя, способен обнаруживать и обезвреживать вирусы-трояны и программы-черви. Кроме того, системные администраторы получают возможность присваивать программам и процессам ту или иную степень приоритетности, в соответствии с которой они и будут сканироваться антивирусом, что позволяет экономить ресурсы корпоративных сетей.

Страница разработчика: www.mcafee.com

Avira AntiVir

Популярный антивирус германской сборки. Эту программу всегда отличали качество работы и быстрая реакция на появление новых вирусов. Она включает в себя резидентный монитор, сканер и программу обновления. AntiVir может постоянно следить за файлами и архивами, которые могут быть потенциальными переносчиками вирусов. Отыскиваются также и макросы, которые внедряются в офисные документы. Программа нетребовательна к ресурсам и показывает хорошие результаты в работе по скорости и качеству поиска.

Страница разработчика: www.free-av.com

Проактивная защита основана на контроле и анализе поведения всех программ, установленных на компьютере, может обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. *Таким образом, компьютер защищен не только от уже и местных вирусов, но и от новых, еще не исследованных.*

Анти-Шпион отслеживает нежелательные действия на компьютере и блокирует их выполнение. Например, компонент блокирует показ баннеров и всплывающих окон, мешающих пользователю при работе с веб-ресурсами, блокирует работу программ, пытающихся осуществить несанкционированный пользователем звонок (если соединение с Интернет осуществлено через телефонную линию), анализирует веб-страницы на предмет фишинг-мошенничества.

Анти-Хакер компонент предназначенный для защиты компьютера при работе в интернете и других сетях. Он контролирует все сетевые соединения, обнаруживает сетевые атаки и обеспечивает невидимость компьютера в сети.

Для поиска вирусов в состав антивируса включены три задачи :

1) Критические области проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты исполняемые при старте системы, загрузочные секторы дисков, системные каталоги Windows. Цель задачи - быстрое обнаружение не в системе активных вирусов, без запуска полной проверки компьютера.

2) Мой компьютер поиск вирусов с тщательной проверкой всех подключенных дисков, памяти файлов.

3) Объекты автозапуска проверка объектов, загрузка которых осуществляется при старте операционной системы, а так же оперативной памяти и загрузочных секторов дисков.

Так же предусмотрена возможность создавать другие задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска в каталоге МОИ ДОКУМЕНТЫ

Разработчики антивирусных программ – www.comss.ru

- Comodo Group – США,
- Dr. Web – Россия (www.drweb.com),
- Eset NOD32 – Словакия (www.esethod32.ru),
- McAfee – США,
- Outpost – Россия,
- Panda Software – Испания,
- Symantec – США,
- Trend Micro – Япония,
- Антивирус Касперского – Россия (www.kaspersky.ru).

Обзор и сравнение антивирусных программ

В данной статье приводится обзор и сравнение функциональных возможностей антивирусных программ (антивирусов) для защиты корпоративных рабочих станций и серверов (Endpoint Protection). Стоит сразу подчеркнуть, что корпоративный антивирус от домашней версии является наличие серверного компонента, предназначенного для

централизованного управления политикой безопасности в организации. За счет серверного компонента, как правило, осуществляется установка, настройка и управление многочисленными клиентами, установленными на рабочих станциях и серверах предприятия.

Описание функциональных возможностей программ взяты с официальных сайтов компаний производителей. Результаты сравнения и тестирования взяты из ежегодного отчета независимой аналитической компании PassMark Software, являющейся ведущим агентством в области тестирования производительности программного и аппаратного^ обеспечения. А так же приведены результаты ежегодного отчета «Endpoint Protection» программ компании Gartner, специализирующейся на исследованиях рынка информационных технологий.

Антивирусные программы для защиты конечных систем уровня предприятия (Enterprise Endpoint Security)

- * Kaspersky Endpoint Security (версия 10.2.1.23)
- * McAfee VirusScan Enterprise (8.8 Scan Engine 5600.1067)
- * Sophos EndUser Protection (версия Endpoint Security and Control 10.0)
- * Symantec Endpoint Protection (версия 12.1.5013.5000)
- * Trend Micro OfficeScan (версия 10.6.3)
- * Microsoft System Center 2012 Endpoint Protection (версия 4.3.220.0)

Сравнение функциональных характеристик антивирусных программ

Рассмотрим общие результаты *сравнения антивирусных программ* для защиты информации. Для удобства сравнение представлено в виде сводной таблицы, которая в относительных величинах показывает оценку общих свойств каждого из представленных решений.

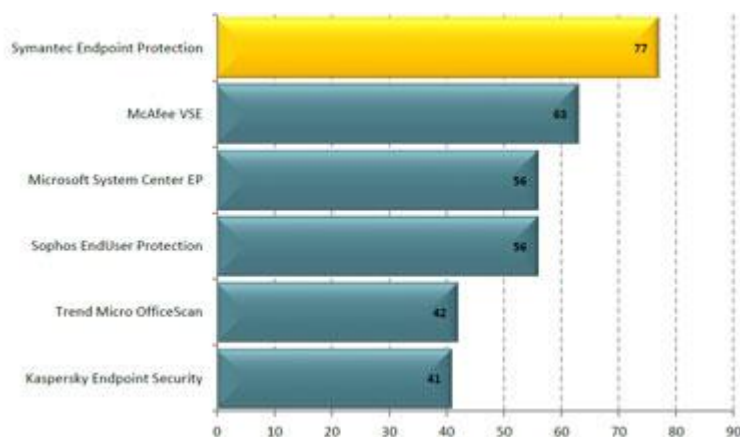
Наименование	Symantec	Kaspersky	McAfee	Microsoft	Sophos	Trend Micro
Установка и настройка	★★★★★	★★★★★	★★★★★	★	★★★★★	★★★★★
Миграция	★★★★★	★★★★★	★★★★★	★	★★★★★	★★★★★
Управление политикой безопасности	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★
Установка клиента	★★★★★	★★★★★	★★★★★	★	★★★★★	★★★★★
Дизайн интерфейса	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Удаленное управление	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Обновление	★★★★★	★★★★★	★★★	★	★★★★★	★★★★★
Эффективность	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Производительность	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★

Сравнение производительности антивирусных программ

Приведем результаты некоторых тестов, демонстрирующих влияние антивирусных средств защиты информации на производительность рабочих станций (ноутбук, компьютер или сервер).

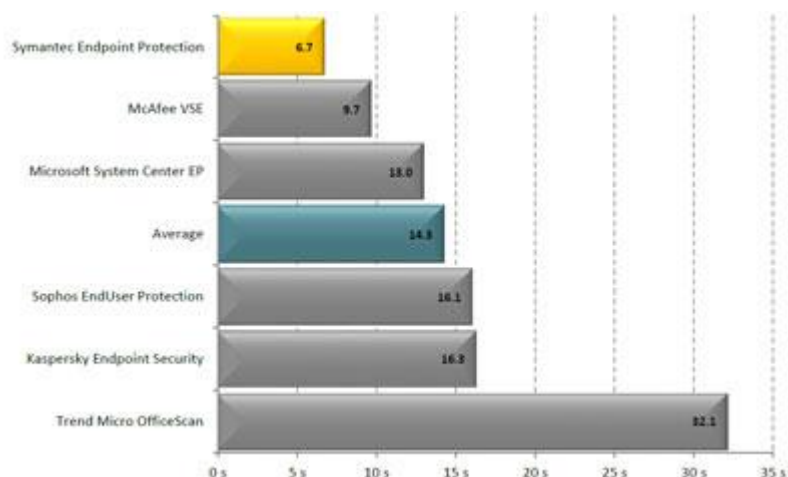
Общий результат тестирования

Все тесты были проведены в одинаково равных условиях. В качестве тестовой рабочей станции был использован HP Pavilion P6-2300A (CPU Intel Core i5 750 2.66GHz / видеокарта 1GB nVIDIA GeForce GT 620M / RAM 6GB DDR3 / HDD Hitachi HDS721010CLA630 / сетевая карта 1GB/s) с операционной системой Microsoft Windows 7 Ultimate SP1 (64-bit).



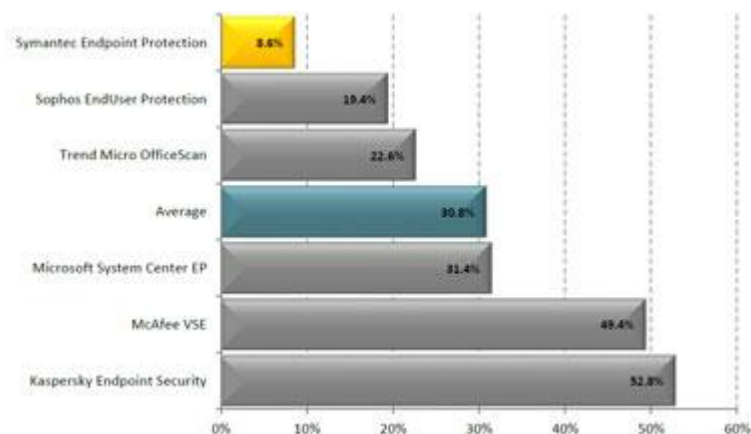
Тест - Влияние антивируса на копирование, перемещение и удаление файлов

В процессе защиты системы антивирусу необходимо контролировать любую активность на рабочей станции. Большинство задач связано с перемещением, копированием или удалением файлов. В это время программа анализирует каждый файл на предмет безопасности. Поэтому при выборе средств защиты крайне важно учитывать время, необходимое для выполнения этих действий. На графике приведено время (в секундах) необходимое для копирования, перемещения и удаления набора файлов (различных форматов) между каталогами.



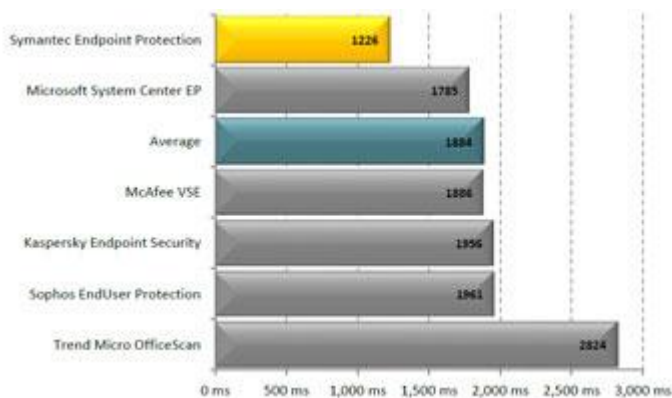
Тест – Загрузка процессора во время сканирования

Сравнение результатов доли загрузки процессора во время сканирования антивирусом набора мультимедийных документов, системных файлов и документов Microsoft Office, общим объемом 5,42 ГБ.



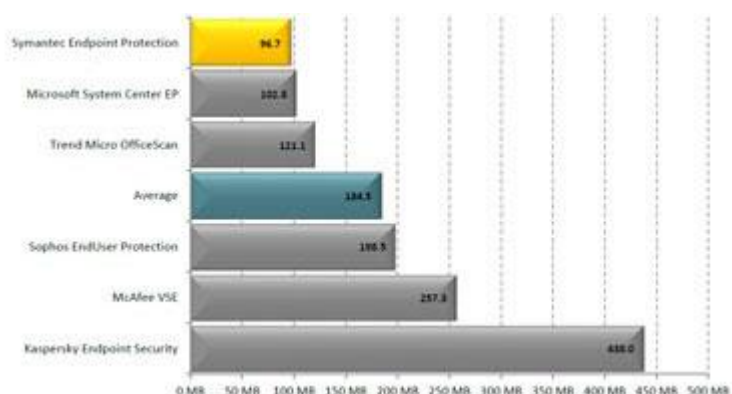
Тест - Время запуска веб браузера

На графике представлены результаты сравнения времени запуска веб браузера (Internet Explorer). Решение с наименьшим временем загрузки считается более эффективным.



Тест – Использование оперативной памяти при сканировании

Сравнение средних значений загрузки оперативной памяти системы в процессе сканирования системы на вирусы. Среднее значение было рассчитано на основании десяти замеров, сделанных с пяти секундным интервалом при сканировании новых файлов (ранее не сканированных).



Оценка разработчиков антивирусных программ

Для оценки поставщиков программ защиты конечных систем принято использовать «магический квадрант» международной компании Gartner, представляющий собой поле поделенной на 4 части. Каждый поставщик оценивается по 2-м критериям: виденье и способность реализации.

При этом, «полнота видения» откладывается на оси абсцисс, «способность реализации» на оси ординат. Каждый поставщик, таким образом, оказывается в одном из четырех квадрантов плоскости: Лидеры – «leaders», претенденты – «challengers», провидцы – «visionaries», нишевые игроки – «niche players».



Для многих существующих производителей, попадание даже в квадрант «нишевых игроков» является большим достижением и признанием другими конкурентами.

...и простую установку софта.

Что насобирали пираты?

Начинать нужно с отказа от эмуляции пиратской версии windows. Мало того что это отпозаконно, да еще при и нестабильности Windows заботе пиратские версии стабильны вдвойне. К тому в «левой» операционной системе могут возникнуть проблемы с обновлением, которое надо проводить регулярно. Так что устанавливайте только лицензионную опера-

ционную систему. После этого можно переходить и к возведению «стен» защиты. Вредоносное программное обеспечение может проникнуть в ваш компьютер через съемные диски и флэшки, электронную почту, веб-сайты и, разумеется, напрямую с соседнего компьютера. Защититься от этого можно, используя специальные антивирусные приложения.

Программа-вакцина



Среди антивирусных программ существуют коммерческие приложения – ESET NOD32 (примерно 1200 рублей), Panda (примерно 1600 рублей), Dr. Web (примерно 1000 рублей), Symantec (примерно 1500 руб-

лей). Антивирус Касперского (примерно 1200 рублей), а также бесплатные антивирусы, например Avast. В Сети не прекращаются споры о том, какой антивирус лучше. Мы выбрали ESET NOD32 – он более прост в настройке, чем его «коллеги», не сильно загружает компьютер, и его можно настроить на обновление в «Нижегородском кольце». И не пытайтесь использовать пиратские программы, производители которых периодически блокируют ключи, в результате пользователи остаются без обновления и с неактивным антивирусом. Не помогайте пиратам!

Следующий этап строительства «крепости» для компьютера – установка брандмауэра Outpost Firewall Pro (от 1000 рублей). Он защитит вашу систему от сетевых атак, шпионского программного обеспечения и кражи данных. Эта программа

является файерволом, через который проходят пакеты из Интернета. Она блокирует или разрешает доступ к локальной сети установленных приложений. Установка этой или подобной программы – такая же необходимость, как и установка антивируса.

Ищем шпионов

Еще стоит установить приложение – «антитроян» для поиска и удаления программ-шпионов (spyware), рекламных вставок (adware), программ – похитителей данных (hackers) и прочего вредоносного программного обеспечения. На помощь придут такие программы, как Ad-aware, Agnitum Tauscan, Spybot-Search & Destroy. Установка и использование этих программ проходит без особых хлопот даже у начинающего пользователя.

Всё в одном

Если вы не хотите устанавливать много программ у себя на компьютере, то можно пользоваться комплексной «броней» – ESET NOD32 Smart Security, Kaspersky Internet Security 2010, Norton Internet Security 2010, Panda Internet Security 2010 не только защитят от вирусов, программ-шпионов, троянов, червей, ботов и руткиотов, но и будут контролировать небезопасные сайты. Кроме того, они имеют встроенный брандмауэр (файервол). Кстати, при установке одной из этих программ Outpost Firewall Pro уже не требуется.

Секретные коды

Пользователю ПК нужно запомнить десятки паролей и логинов для доступа к веб-сайтам и электронной почте. Освободить вашу память поможет бесплатная программа KeePass, простой в управлении менеджер паролей. С помощью него вы сможете создавать коды любой длины, хранить пароли и логины в зашифрованном виде. Вам нужно запомнить только один пароль к этой программе. Но даже если вы установили все указанные прило-

жения на компьютер, это не даст вам 100%-ной защищенности от вредоносных программ. Остается человеческий фактор – вы сами должны помнить о безопасности. Скачав архив, сперва проверьте его с помощью антивируса и только потом открывайте. Старайтесь не посещать подозрительные сайты, проверяйте антивирусом флэшку, перед тем как на нее зайти. Регулярно проводите полную проверку системы на наличие вирусов и шпионских программ.

Заметаем следы

Для удаления «мусора», который остается после посещения веб-страниц, можно использовать бесплатную утилиту CCleaner. Она удалит:

- cookies;
- историю посещения сайтов;
- временные файлы;
- ActiveX-элементы.

Кроме этого, CCleaner поддерживает очистку системного реестра от записей о неиспользуемых расширениях, обновлениях и уже удаленных программах.

Сергей ЗОРИН, Наталья ХАЛЕЗОВА

Есть и бесплатные антивирусы. Они создаются известными компаниями, однако не содержат многих «удобств», присущих платным версиям, или показывают пользователю рекламные картинки – баннеры. Тем не менее бесплатные антивирусы также неплохо справляются со своей задачей. Например, чешская компания AVG предлагает всем желающим загрузить свой бесплатный продукт со страницы free.avg.com.

Если вы подозреваете, что ПК заражен (например, он «тормозит» и отправляет в Интернет какие-то данные, хотя вы ничего не делаете), однако не можете позволить себе покупку антивируса, можно воспользоваться бесплатными программами от крупных фирм. У «Лаборатории Касперского» такая утилита называется Kaspersky Virus Removal Tool (www.kaspersky.ru/removaltools). Компания «Доктор Веб» выпускает утилиту Dr.Web CureIt! (www.freedrweb.com/cureit/).

Что нужно сделать, чтобы не стать жертвой вируса. Установить на компьютер антивирус (хотя бы бесплатный). Следить за обновлениями для операционной системы. Посещать только проверенные интернет-сайты, приглядываясь к адресу в строке браузера (создатели сайтов-подделок могут просто переставить местами буквы: odnoklassinki.ru). Здоровья вашему компьютеру!

СРЕДСТВО ОТ СЛУЧАЙНЫХ СВЯЗЕЙ В КОРПОРАТИВНЫХ СЕТЯХ:

- А. Ночной клуб,
- Б. Прием наркотиков,
- В. Антивирусные программы.

Электронная цифровая подпись и особенности ее применения.

И в суму его пустую суют грамоту другую.

А.С. Пушкин

С давних времен от человека к человеку пересылались различные послания. Иногда это были подложные письма от подставного адресата.

Проблема сокрытия информации встала перед человечеством едва ли не тогда же, когда появилась сама информация и возникла необходимость в ее передаче. Тайнописи Древнего мира, замысловатые шифры старых и не очень старых спецслужб — всем этим наука криптография занималась давно, пока XX век не внес и сюда свои решительные коррективы. Бурное развитие электронных технологий породило невиданный доселе информационный бум, превратив кабинетную науку о древних письменах в практическое руководство по защите самого дорогого на мировом рынке товара - информации.

Чтобы этого избежать, ставились на бумаге признаки подлинности: подписи, печати и пр., что в полной мере не гарантировало от несанкционированного доступа к содержанию письма.

Первый алгоритм симметричного шифрования был, как считается, изобретен еще Юлием Цезарем. Новейшие достижения в этой области, в частности, описание алгоритмов, победивших в последнем конкурсе, проведенном в США на лучший алгоритм шифрования.

Система шифрования Цезаря. Эта система известна с 50 г. до н.э. и названа именем римского императора Гая Юлия Цезаря, который использовал ее при ведении переписки [46].

Система заключается в том, что каждая буква исходного текста заменяется на букву, определяемую смещением от исходной на некое фиксированное число. При достижении конца алфавита выполняется переход к его началу (и наоборот - при отрицательных смещениях). Пример:

М = УВАЖАЕМАЯ...

C = ФГБЗБЖНБА...

В примере показан самый простой вариант - каждая буква заменяется на следующую букву алфавита, т. е. фиксированное число $k = 1$. В данном случае это число и есть ключ шифрования, достаточно знать его, чтобы получить исходный текст общения.

Система Цезаря является примером алгоритма шифрования простой заменой.

При *шифровании заменой (подстановкой)* символы открытого текста заменяются символами того же или другого алфавита по заранее установленному правилу [46]. Частным случаем шифрования заменой является *шифр простой замены*, где каждый символ исходного текста заменяется символами того же алфавита одинаково по всему тексту.

Пример замены при использовании различных алфавитов:

М = УВАЖАЕМАЯ...

$$C = \odot_0 \leftrightarrow \updownarrow \leftrightarrow \Psi \Delta \leftrightarrow \Sigma \dots$$

Несомненно, во времена Цезаря само использование шифрования можно считать революционным, однако на сегодняшний день абсолютно невозможно считать данный шифр хоть сколько-нибудь стойким против атак криптоаналитика. Раскрыть ключ шифрования можно:

- простым перебором возможных вариантов ключей. Полагая, что количество букв в алфавите 33, получаем всего 33 возможных варианта, перебрать которые даже без компьютера не представляет никакой сложности. Криптоатака, осуществляемая путем перебора возможных вариантов ключей, называется *атакой по методу грубой силы* (в англоязычной литературе используется термин *brute-force attack*);
- анализом частоты появления букв в шифртексте. Даже взяв за пример приведенный текст и

предположив, что это начало сообщения, легко получить исходное слово «Уважаемая», проанализировав частоту появления символа «Б» в шифртексте. С двухалфавитной заменой несколько сложнее, но вскрываемо аналогичным образом (символ ↔).

Очень хороший пример двухалфавитной замены и криптоанализа такого шифра лап в «Пляшущих человечках» А. Конан Дойля.

Шифрующие таблицы. Такие таблицы появились существенно позже: они известны с конца XIV века [46]. Рассмотрим пример зашифрования того же текста с помощью шифрующей таблицы размером 3 x 3.

У	В	А
Ж	А	Е
М	А	Я

М = УВАЖАЕМАЯ...

С = УЖМВАААЕЯ...

Шифрование производится следующим образом: исходный текст записывается в строки таблицы, шифртекст считывается по столбцам.

Ключом в данном случае является размер таблицы - 3x3 и порядок записи исходного текста - по вертикали или горизонтали (что важно для «неквадратных» таблиц).

Как видим, за 14 веков криптография шагнула далеко вперед - данный алгоритм существенно сильнее системы Цезаря хотя бы в том, что теоретически количество ключей в нем не ограничено. Однако стоит признать, что использование таблиц большого размера, как минимум, неудобно, поэтому криптоаналитик тех времен вполне мог исходить из предположения, что количество ключей все же не безгранично (сложно представить заполнение средневековым дипломатом таблицы, скажем, 100x100). Это значит, что л гак методом грубой силы вполне применима и в данном случае.

Таблица также не скрывает частоты появления символов исходного текста, да и самих символов, однако это знание не так полезно при криптоанализе, как в предыдущем случае, где достаточно сделать лишь одно верное предположение о соответствии символа шифртекста определенному символу открытого текста.

Данный алгоритм шифрования является примером *шифрования перестановкой*.

При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста [46].

На примере известных простых шифров мы рассмотрели шифрование перестановкой и заменой. Существуют и другие типы шифров [46].

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой *гаммой шифра*.

Основные определения

Прежде чем дать определение собственно термину «шифрование», приведем еще несколько основных понятий:

Криптография - наука о защите информации.

Криптоанализ - противоположная криптографии наука о противодействии криптографическим методам.

Криптология - наука, объединяющая в себе криптографию и криптоанализ.

Шифрование - это основной криптографический метод защиты информации, обеспечивающий ее конфиденциальность. Будет рассмотрено в данной книге наиболее подробно.

Шифрование информации - это процесс преобразования открытой информации в зашифрованную и наоборот. Первая часть процесса называется *зашифрованием*, вторая - *расшифрованием* [42].

Формула зашифрования:

$$C = E(M),$$

M (message) - открытая информация, в литературе также называется «исходный текст» или «открытый текст»;

C (cipher text) - полученный в результате зашифрования шифртекст (в литературе также называется словом «криптограмма»);

E (encryption) - функция зашифрования, выполняющая криптографические преобразования над исходным текстом;

$k1$ (key) - параметр функции E , называемый «ключом шифрования».

В стандарте ГОСТ 28147-89 (отечественный алгоритм симметричного шифрования) [8] понятие «ключ» определено следующим образом: «Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований».

В настоящее время пользователь, получив послание в электронном виде, должен быть уверен, что:

- достоверно установлен автор сообщения;
- послание не было искажено;
- обеспечена его конфиденциальность, т.е. с ним не знакомились посторонние лица.

Для обеспечения авторства и исключения возможности внесения искажений в текст документа используются различные механизмы шифрования (криптографии). Криптография - это наука об обеспеченности секретности и/или аутентичности (подлинности) передаваемых сообщений. Шифрование производится программными и аппаратными средствами.

Защита информации методом криптографического преобразования заключается в приведении ее к неявному виду путем преобразования составных частей информации с помощью специальных алгоритмов либо аппаратных средств и кодов ключей. Ключ - это изменяемая часть криптографической системы, хранящаяся в тайне и определяющая, какое шифрующее преобразование из возможных выполняется в данном случае. Для преобразования используется некоторый алгоритм или устройство, реализующее заданный алгоритм. Само же управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа.

Различают:

- симметричное шифрование (для шифрования и расшифрования используется один и тот же ключ);
- шифрование на открытом ключе - асимметричное шифрование (для шифрования данных используется один ключ, а для расшифрования - другой);
- необратимое шифрование (используется при шифровании паролей, зашифрованный текст записывается в память, далее сравниваются зашифрованные строки текста, при этом данные не могут быть воспроизведены).

В качестве паролей большинство исследователей не рекомендуют использовать:

- свои имя, фамилию, а также имена и фамилии близких родственников;
- свои номера телефонов;
- номерной знак своего автомобиля;
- пароли, содержащие одинаковые буквы;
- комбинации букв на клавиатуре (например, qwerty);
- даты рождения, свою, друзей, коллег по работе, близких родственников;
- слова: user, master, guru, got и т. д.

К алгоритму шифрования, предназначенному для массового применения в вычислительных системах, предъявляется следующая система требований [65, с. 205]:

- зашифрованный текст должен поддаваться только чтению при наличии ключа шифрования;

- число операций, необходимых для определения использованного ключа шифрования по фрагменту зашифрованного текста и соответствующему ему открытому тексту, должно быть не меньше общего числа возможных ключей;
- знание алгоритма шифрования не должно влиять на надежность защиты.

Шифрование может быть симметричным и асимметричным. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования - другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

При использовании симметричного шифрования порядок работы следующий. Исходный текст документа кодируется с применением специальных алгоритмов и некоего секретного (закрытого) ключа, превращаясь в строку символов, которая фактически и представляет собой цифровую подпись под документом. Электронная цифровая подпись (ЭЦП) добавляется к исходному тексту документа, и сформированный файл пересылается получателю. Для этого владелец ЭЦП вставляет дискету с закрытым ключом в дисковод и нажимает указателем мыши на соответствующую кнопку, что и означает подписание документа электронной подписью. Процесс проверки кода аутентификации у получателя, т.е. правильности ЭЦП, выполняется аналогичным образом. При этом проверяется не только подпись, но и текст, т.к. кодирование производилось с использованием всех символов исходного текста документа. Как видим, при симметричной ЭЦП и у отправителя, и у получателя имеется один и тот же ключ и одинаковые права подписывать цифровой подписью и проверять полученные сообщения. Преимущества этой системы заключаются в ее простоте и относительно невысокой стоимости. Условиями применения симметричной ЭЦП является взаимное доверие владельцев закрытого ключа, исключающее отказ от своей подписи под документом, изготовление подложных данных и пр., т.е. ЭЦП должна быть неотречаемой. К тому же при рассылке неопределенному кругу лиц получить принципиально не может иметь заранее ключ. Если у Вас 50 корреспондентов, то Вам придется хранить 50 секретных ключей, по одному для каждого.

Названные проблемы позволяет решить криптография с открытым ключом, использующая асимметричные алгоритмы шифрования.

Криптография с открытым ключом основана на концепции ключевой пары. Каждая половина пары (один ключ) шифрует информацию таким образом, что ее может расшифровать только другая половина (второй ключ). Одна часть ключевой пары - личный ключ, известна только ее владельцу. Другая половина — открытый ключ, распространяется среди всех его корреспондентов, но связана только с этим владельцем. Ключевые пары обладают уникальной особенностью: данные, зашифрованные любым из ключей пары, могут быть расшифрованы только другим ключом из этой пары. Другими словами, нет никакой разницы, личный или открытый ключ используется для шифрования послания; получатель сможет применить для расшифровки вторую половину пары.

Ключи можно использовать и для обеспечения конфиденциальности послания, и для аутентификации его автора. В первом случае для шифрования послания отправитель использует открытый ключ получателя, и таким образом оно останется зашифрованным, пока получатель не расшифрует его личным ключом. Во втором случае, отправитель шифрует послание личным ключом, к которому только он сам имеет доступ.

Шифрование посланий открытым ключом принципиально не слишком отличается от симметричного шифрования с использованием секретного ключа, но все же имеет ряд преимуществ. Например, открытая часть ключевой пары может свободно распространяться без опасений, что это помешает использовать личный ключ. Не нужно рассылать копию своего открытого ключа всем корреспондентам; они смогут получить его на сервере вашей компании или у вашего провайдера.

Другое преимущество криптографии с открытым ключом в том, что она позволяет аутентифицировать отправителя послания. Поскольку вы - единственный, кто имеет возможность зашифровать какую-либо информацию вашим личным ключом, всякий, кто использует ваш открытый ключ для расшифровки послания, может быть уверен, что оно от вас. Таким образом, шифрование электронного документа вашим личным ключом схоже с подписью на бумажном документе. Но не забывайте: нет никаких гарантий, что помимо получателя ваше послание не прочтет кто-то еще. Использование криптографических алгоритмов с открытым ключом для шифрования посланий - это достаточно медленный вычислительный процесс, поэтому специалисты по криптографии придумали способ быстро генерировать короткое, уникальное представление вашего послания, называемое дайджестом послания. Дайджест можно зашифровать, а затем использовать как вашу цифровую подпись.

Чтобы использовать систему криптографии с открытым ключом, необходимо сгенерировать открытый и личный ключи. Обычно это делается программой, которая будет использовать ключ (такой, как ваш Web-браузер или программа электронной почты). После того, как ключевая пара сгенерирована, вы должны хранить свой личный ключ в тайне от посторонних. Затем вам нужно распространить открытый ключ среди своих корреспондентов. Можете использовать для этого электронную почту, но вдруг вы забудете внести кого-то в список или у вас появятся новые корреспонденты: Кроме того, такой подход не обеспечит аутентификации: кто-то может сгенерировать ключевую пару и, назвавшись вами, разослать открытый ключ корреспондентам. После этого ничто не мешает ему отправлять сообщения от вашего имени.

Самый лучший и надежный способ распространения открытых ключей - воспользоваться услугами сертификационных центров. Сертификационный центр выступает как хранилище цифровых сертификатов. Он принимает ваш открытый ключ вместе с доказательствами вашей личности (какими - зависит от класса сертификата). После этого ваши корреспонденты могут обращаться в сертификационный центр за подтверждением вашего открытого ключа. Цифровые сертификаты выступают в роли электронного варианта удостоверения личности и, будучи общепринятым методом распространения открытых ключей, позволяют вашим корреспондентам убедиться, что вы на самом деле тот. За кого себя выдаете.

Нет системы шифрования, идеально подходящей для всех ситуаций. В таблице проведено сравнение преимуществ и недостатков каждого типа шифрования.

Преимущества и недостатки криптографических систем

Тип шифрования	Преимущества	Недостатки
Шифрование с симметричным ключом	- быстрота; - легко реализовать аппаратно	- оба ключа одинаковы; - трудно распространять ключи; - не поддерживает цифровые подписи
Шифрование с открытым ключом	- использовать два разных ключа; - относительно просто распространять ключи; - обеспечивает целостность и невозможность отказа от авторства (за счет цифровой подписи)	- работает медленно; - требует больших вычислительных мощностей

Известно, что алгоритмы защиты информации (прежде всего шифрования) можно реализовать как программным, так и аппаратным методом. Рассмотрим аппаратные шифраторы: почему они считаются более надежными и обеспечивающими лучшую защиту.

Аппаратный шифратор по виду и, по сути, представляет собой обычное

компьютерное «железо», чаще всего это плата расширения, вставляемая в разъем системной платы ПК.

Производители аппаратных шифраторов обычно стараются насытить их различными дополнительными возможностями, среди которых:

1. Генерация случайных чисел. Это нужно, прежде всего, для получения криптографических ключей.

2. Контроль входа на компьютер. При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами). Работа будет разрешена только после того, как устройство опознает предъявленные ключи и сочтет их «своими». В противном случае придется разбирать системный блок и вынимать оттуда шифратор, чтобы загрузиться (однако, как известно, информация на ПК тоже может быть зашифрована).

3. Контроль целостности файлов операционной системы. Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные. Шифратор хранит в себе список всех важных файлов с заранее рассчитанными для каждого контрольными суммами, и если при следующей загрузке не совпадает эталонная сумма хотя бы одного из них, компьютер будет заблокирован.

Плата со всеми перечисленными возможностями называется устройством криптографической защиты данных - УКЗД.

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность операционной системы, называют также «электронным замком». Понятно, что последним не обойтись без программного обеспечения - необходима утилита, с помощью которой формируются ключи для пользователей и ведется их список для распознавания «свой/чужой». Требуется приложение для выбора важных файлов и расчета их контрольных сумм. Эти программы обычно доступны только администратору по безопасности, который должен предварительно настроить все УКЗД для пользователей, а в случае возникновения проблем разбираться в их причинах.

Структура шифраторов

Для выполнения функций УКЗД должно состоять из:

1. Блока управления - основной модуль шифратора, который «заведует» работой всех остальных. Обычно реализуется на базе микроконтроллера.

2. Контроллер системной шины ПК. Через него осуществляется основной обмен данными между УКЗД и компьютером.

3. Энергозависимое запоминающее устройство (ЗУ) - должно быть достаточно емким (несколько мегабайт) и допускать большое число треков записи. Здесь размещается программное обеспечение микроконтроллера, которое выполняется при инициализации устройства (т.е. когда шифратор перехватывает управление при загрузке компьютера).

4. Память журнала. Также представляет собой энергозависимое ЗУ.

5. Шифропроцессор - это специализированная микросхема или микросхема программируемой логики. Собственно, он и шифрует данные.

6. Генератор случайных чисел. Обычно представляет собой такое устройство, дающее статистически случайный и непредсказуемый сигнал - белый шум.

7. Блок ввода ключевой информации. Обеспечивает защищенный прием ключей с ключевого носителя, через него также вводится идентификационная информация о пользователе, необходимая для решения вопроса «свой/чужой».

8. Блок коммутаторов. Помимо перечисленных выше основных функций, УКЗД может по велению администратора безопасности ограничивать возможность работы с внешними устройствами: дисковыми, CD-ROM и т.д.

Современные алгоритмы шифрования являются комплексными, т.е. используют в определенной последовательности несколько типов преобразований.

Наиболее известными алгоритмами шифрования являются следующие:

- отечественный стандарт шифрования ГОСТ 28147-89;
- стандарт шифрования США AES (RIJNDAEL);

- бывший стандарт шифрования США DES;
- наиболее широко используемый алгоритм асимметричного шифрования

RSA:

Современные алгоритмы симметричного шифрования подразумевают выполнение над шифруемыми данными определенных криптографических преобразований, которые повторяются несколько раз (раундов), в то время как асимметричное шифрование основано на использовании однонаправленных функций.

Симметричное шифрование выполняется с существенно более высокой скоростью, чем асимметричное, однако ключи симметричного шифрования необходимо передавать «из рук в руки» или по доверенным каналам связи, что ограничивает и усложняет применение этого типа шифрования. Открытые ключи асимметричного шифрования могут быть переданы по открытым каналам связи, например, через Интернет, что гораздо более удобно, чем использование симметричного шифрования, однако существует риск подмены открытого ключа при его передаче или хранении. Для минимизации недостатков различных методов шифрования используется комплексное шифрование, в котором поочередно применяются симметричное и асимметричное шифрование.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Назначение и использование

Электронная цифровая подпись (ЭЦП) предназначена для решения следующих задач по защите информации:

- обеспечение целостности данных;
- подтверждение авторства данных.

Рассмотрим схему использования ЭЦП неким пользователем i (рис. 3.1) [42]:

- Предварительный этап:
- пользователь i генерирует пару ключей: секретный ключ K_{si} и открытый ключ K_{pi} . Открытый ключ вычисляется из парного ему секретного ключа (аналогично алгоритмам асимметричного шифрования);
- открытый ключ K_{pi} рассылается остальным пользователям (или делается доступным, например, на разделяемом ресурсе).
- Использование:
- пользователь i подписывает сообщение с помощью своего секретного ключа K_{si} ;
- остальные пользователи могут проверить подпись сообщения с помощью открытого ключа пользователя i - K_{pi} .

Секретный ключ ЭЦП является тем самым уникальным элементом, без которого нельзя подделать ЭЦП его владельца, поэтому, необходимо исключить возможность несанкционированного доступа к секретному ключу. Секретный ключ ЭЦП, аналогично ключу симметричного шифрования и секретному ключу асимметричного шифрования, рекомендуется хранить на персональном ключевом носителе.

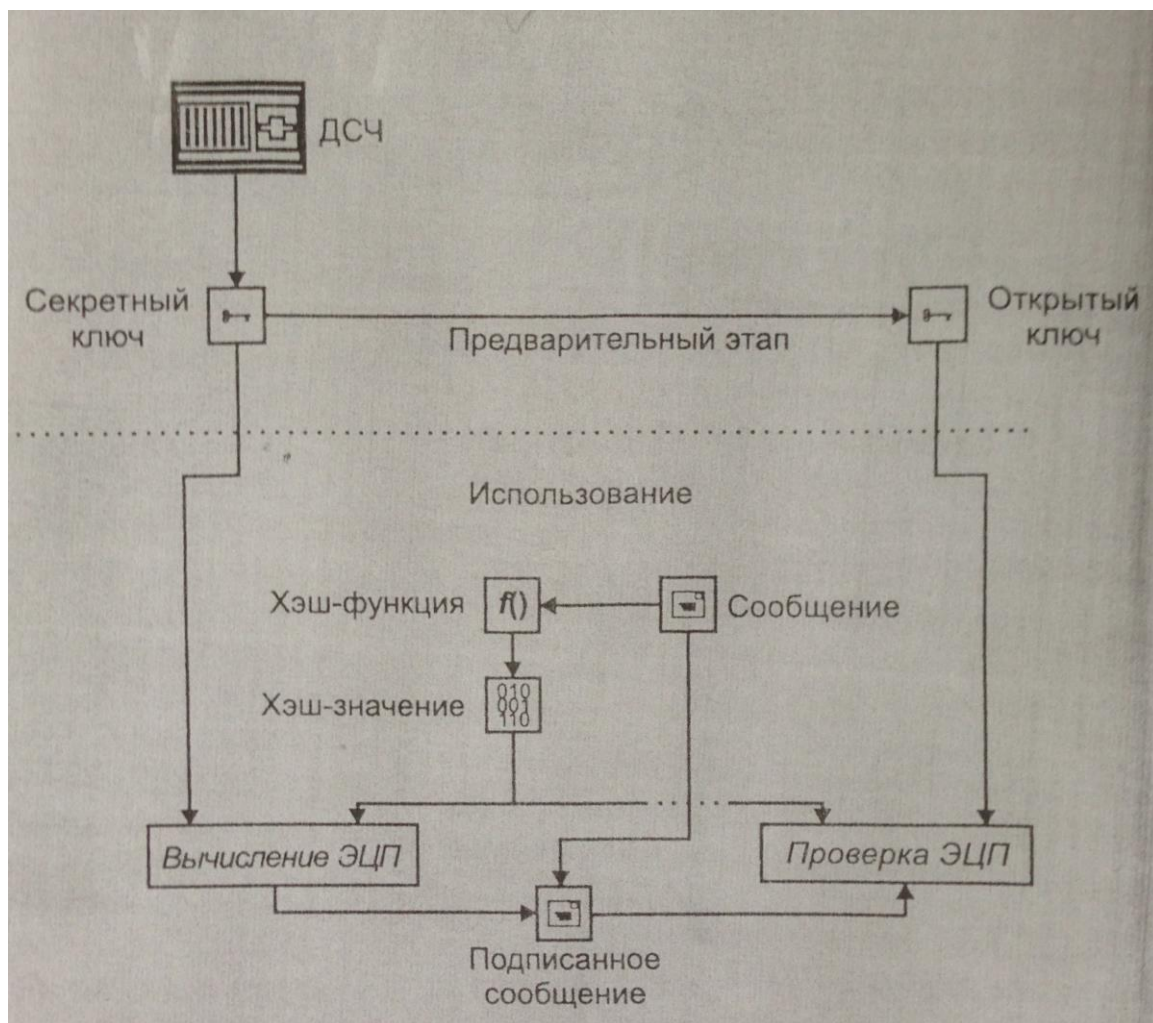


Рис. 3.1. Схема использования ЭЦП.

При компрометации секретного ключа ЭЦП его владельцу необходимо оповестить всех потенциальных адресатов о том, что соответствующий данному секретному ключу открытый ключ больше не является действительным, поскольку злоумышленник, владеющий секретным ключом, сможет подписать любую информацию подписью законного владельца ключа.

Побочное, но не менее важное назначение электронной подписи - подтверждение авторства сообщения. Обычно в файлы ключей ЭЦП записывается различная дополнительная информация (помимо собственно ключа), по-разному интерпретируемая различными криптосистемами, например: ФИО владельца ключа, его место работы, срок действия ключа и т.п. Информация из секретного ключа и, прежде всего информация о его владельце, обычно копируется в подпись сообщения или документа. Это и позволяет установить автора сообщения (не нужно запоминать, кто именно прислал тот открытый ключ, проверка которым показала, что ЭЦП верна, - а открытых ключей в реальной работе может быть несколько сотен или тысяч). Причем корректно реализованные средства работы с ЭЦП включают в расчет собственно электронной подписи сообщения и информацию об авторе, чтобы не было возможности ее изменить. А результат проверки ЭЦП обычно выводится на экран в понятном для восприятия виде, например:

«Подпись файла Compromat.bmp верна (Автор: Иванов Василий Семенович)»

ОРГАНИЗАЦИЯ ЮРИДИЧЕСКИ ЗНАЧИМОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Признание равнозначности ЭЦП собственноручной подписи

Условия признания равнозначности электронной цифровой подписи и собственноручной подписи (статья 4 ФЗ-1) следующие:

1. Сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

2. Подтверждена подлинность электронной цифровой подписи в электронном документе;

Статья 3 Закона «Об ЭЦП» говорит: *«Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе».*

3. Электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Организовать рабочие места для применения электронной цифровой подписи предлагается на основе комплекта продуктов «КриптоТри». На рабочем месте пользователя устанавливаются о СКЗИ «КриптоПро CSP» - сертифицированное средство криптографической защиты информации от компании «КРИПТО-ПРО», реализующее функции создания и проверки ЭЦП, шифрования и создания ключей ЭЦП и шифрования о программное средство «КриптоАРМ» от компании «Цифровые технологии», использующее функции криптопровайдера и реализующее пользовательский графический интерфейс, посредством которого обеспечивается управление (создание и/или проверка) ЭЦП и шифрование данных

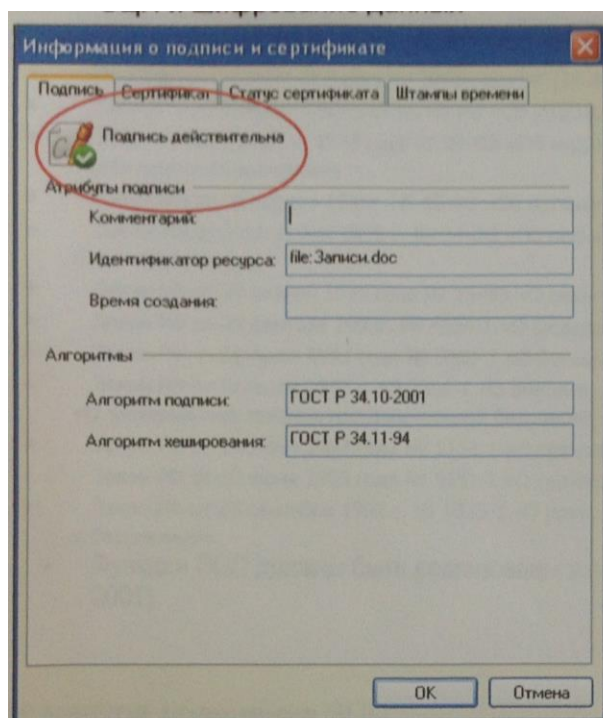


Рисунок 1 «КриптоАРМ». Результат проверки математической корректности подписи

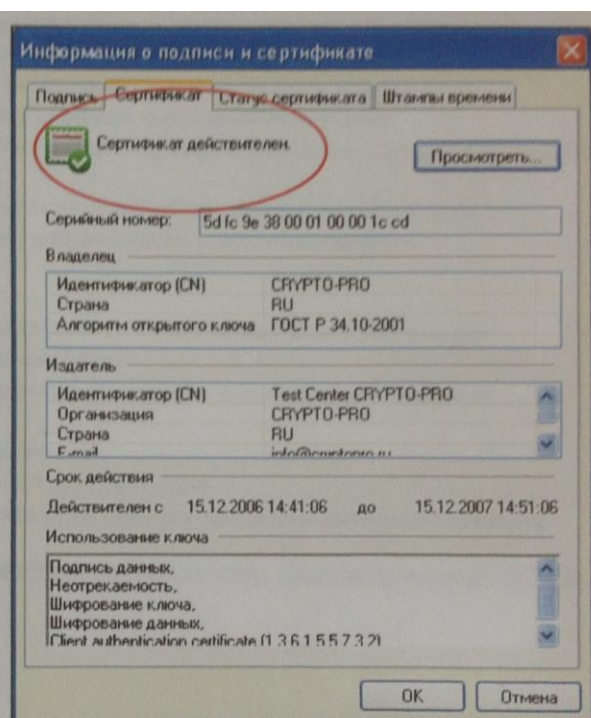


Рисунок 3 «КриптоАРМ». Результат проверки статуса сертификата подписи

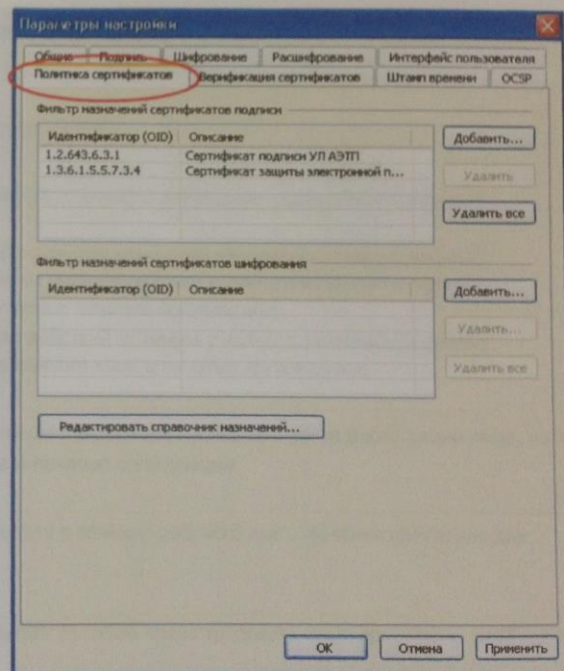
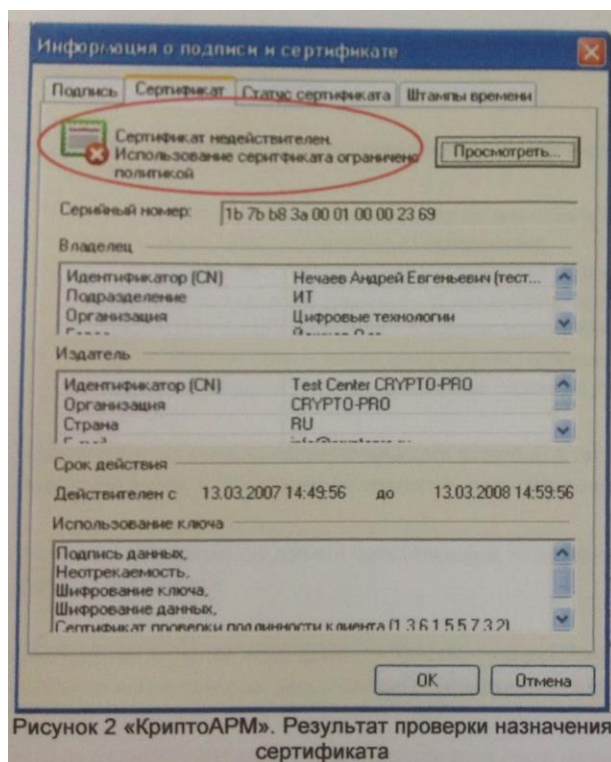


Рисунок 2 «КриптоАРМ». Результат проверки назначения сертификата

Рисунок 4 «КриптоАРМ». Настройка назначения сертификатов подписи и шифрования

Решение организационных и юридических вопросов

Правовые основы применения ЭЦП

- Федеральный закон от 28 марта 2002 г № 32-ФЗ «О внесении изменения и дополнения в Федеральный закон «О бухгалтерском учете».
- Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».
- Федеральный закон от 28 декабря 2001 г. № 180-ФЗ «О внесении изменения в статью 80 части первой Налогового кодекса Российской Федерации» дополняет Налоговый кодекс положениями, касающимися пересылки налоговой декларации в налоговую инспекцию в электронном виде по каналам связи («бесбумажная» технология).
- Федеральный закон от 8 августа 2001 года № 128-ФЗ «О лицензировании отдельных видов деятельности».
- Закон РФ от 4 июля 1995 года № 85-ФЗ «Об участии в международном информационном обмене».
- Закон РФ от 1 апреля 1995 года № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования».
- Закон РФ от 03 апреля 1995г. № 40-ФЗ «Об органах Федеральной службы безопасности в Российской Федерации».
- Закон РФ от 20 февраля 1995 г. N 9 24-ФЗ «Об информации, информатизации и защите информации» (с комментариями).
- Закон РФ от 20 января 1995 года № 15-ФЗ «О связи».
- Закон РФ от 24 декабря 1993г. № 4524-1 «О федеральных органах правительственной связи и информации».
- Закон РФ от 21 июля 1993 года № 5485-1 «О Государственной тайне».
- Закон РФ от 01 июля 1993 г. № 5306-1 «О внесении изменений и дополнений в Закон Российской Федерации «О федеральных органах государственной безопасности».
- Закон РФ от 10 июня 1993 года № 5154-1 «О стандартизации».
- Закон РФ от 10 июня 1993 года N? 5151-1 «О сертификации продуктов и услуг».

- Функции ЭЦП должны быть реализованы в соответствии с требованиями законодательства (ГОСТ 34.10- 2001).

Процедура получения ЭЦП

В течение рабочего дня после получения регистрационной карты ответственный сотрудник аккредитованного Ассоциацией

Удостоверяющего Центра связывается с организацией для выставления счета на ЭЦП и оформления договора.

Перечень документов, необходимых для получения ЭЦП:

1. Выписка из Ы ИОЛ (срок действия выписки зависит от УЦ, осуществляющего услуги по выпуску ЭЦП) — оригинал или нотариально заверенная копия;

2. Документ, подтверждающий полномочия лица, на имя которого выдается ЭЦП:

- для единоличного исполнительного органа — копия приказа (протокола) о назначении, заверенная подписью уполномоченного лица и печатью организации;

- для сотрудника — копия приказа о приеме на работу, заверенная подписью уполномоченного лица и печатью организации, копия доверенности на осуществление действий от имени участника размещения заказа с правом использования ЭЦП, заверенная подписью уполномоченного лица и печатью организации;

- для представителя — копия доверенности на осуществление действий от имени участника размещения заказа с правом использования ЭЦП, заверенная подписью уполномоченного лица и печатью организации;

3. Копия 2-й и 3-й страниц общегражданского паспорта, а также страницы с указанием последнего места регистрации лица, на имя которого выдается ЭЦП, заверенная подписью уполномоченного лица и печатью организации.

4. Полученный сертификат должен был» отправлен по адресу cert@aetr.ru в течение рабочего дня с момента получения для регистрации в реестре.

Примечание: В случае необходимости Удостоверяющий Центр оставляет за собой право требовать иные документы, необходимые для полной идентификации пользователя Удостоверяющего центра.

Компоненты, используемые на рабочем месте клиентов и необходимые для построения системы юридически значимого документооборота в электронных торговых площадках:

- MS Internet Explorer — используется с целью предоставления пользователю веб-интерфейса для доступа к данным.

- ЭЦП Framework — компонент предоставляет возможность активного взаимодействия с клиентом посредством MS Internet Explorer (через веб-интерфейс сайта) для реализации механизмов создания подписи документов и форм,

ее просмотра и проверки; шифрования и расшифрования документов и форм. Использует для работы COM-интерфейсы, поставляемые «КриптоАРМ SDK*».

«КриптоАРМ SDK», идущее в составе «КриптоАРМ Стандарт», предоставляет COM-интерфейсы для:

- шифрования и формирования электронной цифровой подписи форм и документов; — online-проверки статуса сертификатов (OCSP-ответы Службы актуальных статусов);

- работы со Службой штампов времени (TSP);

- взаимодействия с Удостоверяющим центром для первичной сертификации и последующего управления жизненным циклом сертификата;

- поддержки нового формата электронной цифровой подписи — CAdES (усовершенствованная подпись с расширенными доказательствами ее подлинности).

При выполнении перечисленных операций «КриптоАРМ SDK» использует функции сертифицированных СКЗИ. Сертифицированное СКЗИ — средство криптографической защиты информации предназначенное для авторизации и обеспечения контроля подлинности электронных документов при обмене ими между пользователями с применением электронной цифровой подписи; обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты и др. Поставщик сертифицированных криптографических алгоритмов — криптопровайдер КриптоПро CSP (от компании «Крипто-Про»). Сертифицированный отчуждаемый носитель. Он представляет собой носитель закрытых ключей, реализованный в виде usb-брелка и предназначенный для хранения контейнеров закрытых ключей, защищенных пин-кодом. Поддерживаются сертифицированные токены производства ruToken и eToken.

www.securitycode.ru

Назначение

Secret Net является сертифицированным средством защиты информации от несанкционированного доступа и позволяет привести автоматизированные системы в соответствие требованиям регулирующих документов:

- №152-ФЗ («О персональных данных»);
- №98-ФЗ («О коммерческой тайне»);
- №5485-1 -ФЗ («О государственной тайне»);
- СТО БР ИББС (Стандарт Банка России).

Возможности

- Аутентификация пользователей.
- Разграничение доступа пользователей к информации и ресурсам автоматизированной системы.
- Доверенная информационная среда.
- Контроль утечек и каналов распространения конфиденциальной информации.
- Контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации.
- Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.
- Масштабируемая система защиты, возможность применения Secret Net (сетевой вариант) в организации с большим количеством филиалов.
- Защита терминальной инфраструктуры и поддержка технологий виртуализации рабочих столов (VDI).

Варианты развертывания Secret Net

- Автономный режим - предназначен для защиты небольшого количества (до 20-25) рабочих станций и серверов. При этом каждая машина администрируется локально.
- Сетевой режим (с централизованным управлением) - предназначен для развертывания в доменной сети с Active Directory. Данный вариант имеет средства централизованного управления и позволяет применить политики безопасности в масштабах организации. Сетевой вариант Secret Net может быть успешно развернут в сложной доменной сети (domain tree/forest).

Дополнительно

- Плата аппаратной поддержки Secret Net Card

Архитектура

Компоненты Secret Net 7 (сетевой режим):

- Secret Net 7 - Клиент;
- Secret Net 7 - Сервер безопасности;
- Secret Net 7 - Программа управления.

Клиент

Клиент Secret Net 7 устанавливается на всех защищаемых компьютерах. Он следит за соблюдением настроенной политики безопасности на рабочих станциях и серверах, обеспечивает регистрацию событий безопасности и передачу журналов на сервер безопасности, а также прием от него оперативных команд и их выполнение.

Сервер безопасности

Сервер безопасности является основным элементом в сетевой структуре системы Secret Net 7. Этот компонент обеспечивает взаимодействие объектов управления, реализует функции контроля и управления, а также осуществляет обработку, хранение и передачу информации.

Программа оперативного управления («Монитор»)

В состав СЗИ Secret Net 7 включена программа оперативного управления, заменяющая средства оперативного управления предыдущих версий СЗИ.

Программа оперативного управления предназначена для конфигурирования сетевой структуры, централизованного управления защищаемыми компьютерами и для работы с записями журналов, поступивших на хранение в базу данных сервера безопасности. Программа устанавливается на рабочих местах администраторов. При работе программа взаимодействует с сервером безопасности, который обрабатывает все управляющие команды администратора.

Дополнительно лицензируемый компонент - механизм защиты дисков

Дополнительно может использоваться и лицензироваться модуль блокировки НСД к жесткому диску, который осуществляет сокрытие данных на диске при загрузке компьютера с внешних носителей.

Ранее приобретенная лицензия на СЗИ Security Studio 6 - Trusted Boot Loader может использоваться для активации этого механизма в Secret Net 7.

Системные требования

Компонент «Клиент» (компонент, реализующий защитные механизмы СЗИ): автономный режим, сетевой режим

Операционная система	Windows 8/8.1; Windows 7 SP1; Windows Vista SP2; Windows XP Professional SP3/XP Professional x64 Edition SP2; Windows Server 2012/Server 2012 R2; Windows Server 2008 SP2/Server 2008 R2 SP1; Windows Server 2003 SP2/Server 2003 R2 SP2
Процессор Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное пространство)	150 МБ
Дополнительное ПО	Internet Explorer 6 или выше

Компонент «Сервер безопасности»

Операционная система	Windows Server 2012/2012 R2; Windows Server 2008 SP2/Server 2008 R2 SP1; Windows Server 2003 SP2/Server 2003 R2 SP2
Процессор Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное пространство)	150 ГБ
Дополнительное ПО	IIS (из состава соответствующей ОС). СУБД Oracle/MS SQL, компонент «Клиент» - для сервера безопасности

Компонент «Программа управления» (устанавливается на рабочее место администратора)

Операционная система	Windows 8/8.1; Windows 7 SP1; Windows Vista SP2; Windows XP Professional SP3/XP Professional x64 Edition SP2; Windows Server 2012/Server 2012 R2; Windows Server 2008 SP2/Server 2008 R2 SP1; Windows Server 2003 SP2/Server 2003 R2 SP2.
Процессор Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное пространство)	2 ГБ
Дополнительное ПО	Internet Explorer 6 или выше; компонент «Клиент»

Системные ограничения:

1. Система Secret Net 7 несовместима с редакциями ОС Windows, в которых отсутствует возможность подключения к домену и управление средствами групповых политик (например, Windows XP Home Edition, Windows Vista Home Basic, Windows 7 Home Premium и др.).

2. Для корректного функционирования системы требуется установка русского языка в региональных настройках ОС Windows.

Продукты

Средства криптографической защиты информации (СКЗИ) Верба-W, Верба-OW

Новые возможности библиотек "Верба-OW" версии 6.1

- реализована возможность формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с требованиями ГОСТ Р. 34.1Q- 2001 (алгоритм, основанный на эллиптических кривых);
- в библиотеку добавлена функция генерации ключей (verba_key_gen);
- обеспечена возможность проверки ЭЦП ГОСТ Р 34.10-94 под сообщением в формате PKCS#7 с использованием сертификата открытого ключа в формате X.509, сформированного СКЗИ "КриптоПро CSP".

Комплектность

СКЗИ "Верба-OW" версии 6.1 может поставляться в следующих комплектациях:

- **Комплектация № 1:** Программная реализация библиотеки шифрования и электронной цифровой подписи ОС Windows (сертификат по уровню ИКСГ).
- **Комплектация № 2:** Аппаратно-программная реализация библиотеки шифрования и электронной цифровой подписи ОС Windows (сертификат по уровню "КС2").
- **Комплектация № 3:** Программная реализация библиотеки электронной цифровой подписи ОС Windows (сертификат по уровню "КС1").
- **Комплектация № 4:** Аппаратно-программная реализация библиотеки электронной цифровой подписи ОС Windows (сертификат по уровню "КС 2").

Динамические библиотеки СКЗИ (5.1)

Динамические библиотеки СКЗИ "ВЕРБА-W" f"ВЕРБА-OW") предназначены для встраивания в прикладное программное обеспечение, в результате чего к функциям ПО добавляются возможности шифрования файлов и областей оперативной памяти, формирования и проверки электронной цифровой подписи в соответствии с российскими стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ 28147-89.

СКЗИ "ВЕРБА-W" использует симметричные ключи шифрования и асимметричные ключи для подписи. СКЗИ "ВЕРБА-OW" использует принцип открытого распределения ключей шифрования и электронно-цифровой подписи.

Для формирования ключей шифрования и электронно-цифровой подписи используются:

- для СКЗИ "ВЕРБА-W" - Автоматизированное рабочее место администратора безопасности (АРМ АБ-С) и ключевые блокноты типа ДСРФ;
- для СКЗИ "ВЕРБА-OW" - АРМ АБ-О.

Основные функции библиотеки WSIGN, WSIGN(O)

К основным возможностям библиотеки WSIGN(O) относятся:

- формирование электронной цифровой подписи файла/блока памяти;
- проверку ЭЦП файла/блока памяти;
- удаление подписи;
- выработка значения хэш-функции файла/блока памяти.

Библиотеки WBOTH, WBOTH(O)

Библиотеки WBOTH(O) содержат функции библиотек WSIGN(O) и дополнительно реализуют функции шифрования, к основным из которых относятся:

- зашифрование/расшифрование файлов/блоков памяти;
- одновременное зашифрование файлов/блоков памяти в адрес множества абонентов;
- получение имитовставки для файла/блока памяти;
- формирование случайного числа заданной длины..

Управление справочниками открытых ключей

Библиотеки предоставляют возможность формирования и администрирования справочников открытых ключей шифрования и ЭЦП соответственно, и обеспечивают выполнение следующих функций при работе со справочниками:

- добавление и удаление открытого ключа;
- получение атрибутов открытого ключа по идентификатору и наоборот;
- контроль целостности справочника открытых ключей;
- контроль целостности открытого ключа.

Применение библиотек СКЗИ

Криптографические библиотеки в первую очередь предназначены для встраивания в прикладное программное обеспечение заказчика. Для этих целей в комплект поставки включается подробное описание функций и рекомендаций по построению защищенных систем. Вместе с тем МО ПНИЭИ и компании-партнеры успешно поставляют на рынок большое количество приложений, использующих СКЗИ "Верба-W" и "Верба-OW".

В их число входят: АРМ шифрования и ЭЦП (Файловый Криптоменеджер), защищенная электронная Интернет-почта "Курьер", система защиты HTTP-протокола "Корвет", Криптографический Сервер с системой управления ключами, защищенная электронная почта X.400, текстовый процессор Лексикон, система документооборота БОСС- Референт.

МО ПНИЭИ и дилеры поставили около 20 000 копий программных библиотек и продуктов их использующих. В числе крупнейших заказчиков: ФАПСИ, Банк России, Пенсионный Фонд России, ФСФС, ДКК, РТС. ММВБ, НДЦ и другие государственные, финансовые и банковские структуры.

Развитие систем с использованием СКЗИ

Используя СКЗИ "Верба-OW", МО ПНИЭИ совместно с ООО "Валидата" разработало первую версию нового программного комплекса - Систему управления сертификатами VCERT PKI, реализующего Инфраструктуру Открытых Ключей (Public Key Infrastructure). VCERT PKI основана на международных рекомендациях X.509, RFC-2459, PKCS, использует российские криптографические стандарты. Средства разработчика VCERT PKI включают развитый инструментарий разработчика.

Технические характеристики

В 2000 г. длина открытого ключа шифрования и подписи увеличена до 1024 бит. При обработке информации на ПЭВМ СКЗИ "Верба-W" и "Верба-OW" обеспечивают следующие показатели (без учета времени обращения к устройствам ввода-вывода):

Операции	Intel Celeron 266 МГц<
Шифрование/расшифрование	2,0 МБайт/с
Вычисление хэш-функции	1,9 МБайт/с
Формирование ЭЦП	0,01 с
Проверка ЭЦП	0,04 с

3.6. Защита информации в Интернете

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску, безопасность Вашей локальной сети и конфиденциальность, содержащейся в ней информации.

Internet - глобальная компьютерная сеть, охватывающая весь мир. Сегодня Internet имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям во всем мире, одна с другой.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи распределенного доступа к ресурсам. Около двух лет назад были созданы оболочки, поддерживающие функции сетевого поиска и доступа к распределенным информационным ресурсам, электронным архивам.

Internet, служившая когда-то исключительно исследовательским и учебным группам, чьи интересы простирались вплоть до доступа к суперкомпьютерам, становится все более популярной в деловом мире.

Компании соблазняют быстрота, дешевая глобальная связь, удобство для проведения совместных работ, доступные программы, уникальная база данных сети Internet. Они рассматривают глобальную сеть как дополнение к своим собственным локальной сетям.

При низкой стоимости услуг (часто это только фиксированная ежемесячная плата за используемые линии или телефон) пользователи могут получить доступ к коммерческим и некоммерческим информационным службам США, Канады, Австралии и многих европейских стран. В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до прогноза погоды на завтра.

Вместе с тем, интерактивный характер общения с сетью, особенно в WWW, приводит к появлению дистанционных торговых служб, где можно ознакомиться с предложением товаров, посмотреть их фотографии на экране компьютера - и тут же заказать товар, заполнив соответствующую экранную форму. Подобные службы дополняются средствами дистанционной оплаты товара - по той же Сети, с использованием в начале обычных пластиковых карточек, а затем и специально разработанной для Internet механизмов расчета.

Разработка средств электронных расчетов для Сети финансируется банками, некоторые из которых создают службы расчетов, целиком ориентированные на Internet.

Сеть Internet в принципе применима для самых разных областей работы банка - от взаимодействия с клиентом до обмена информацией с другими банками.

Первым этапом работы в Internet для любой финансовой организации обычно становится использование World Wide Web для опубликования рекламной и прочей информации. Сегодня примерно 300 финансовых организаций применяют WWW как средство рекламы

Второй этап - представление клиентам базового доступа в банк. Клиенты получают возможность просмотреть относящуюся к ним финансовую информацию, при этом они ничего не могут с ней сделать

Взаимодействие с клиентом - третий этап. Благодаря такому взаимодействию, клиент получит не только доступ к финансовой информации, но и сможет внести коррективы в информацию и провести различные расчеты. При такой реализации системы на базе Internet могут придти на смену специализированным системам «банк-клиент» или, по крайней мере, взять на себя часть их функций. На Западе уже есть примеры так называемых «виртуальных» банков, которые вообще не имеют обычных филиалов, и ведут все дела с клиентами через Internet.

Помимо удешевления транзакций Интернет - банкинг позволяет:

✓ привлечь новых клиентов. Теперь это могут быть жители других штатов, удаленных на тысячи километров от ближайшего отделения банка;

✓ удержать старых клиентов. Переезжая на новое место, клиент отрывается от старого банка, если он управляет счетом по телефону или модему. Благодаря Интернету создается впечатление, что ничего не произошло - банк остался на месте, поэтому подавляющее большинство клиентов остаются со своим старым банком и после переезда;

✓ поощрять наиболее выгодных клиентов. Если клиент управляет счетом по Интернету, все его действия можно зафиксировать, восстановить карту его предпочтений и в соответствии с этим строить индивидуальную политику банка.

Поскольку Интернет-банкинг выгоден, то создаются новые банки, работающие только в Интернете, не имеющие не собственных зданий, ни филиалов, ни банкоматов. Он может предложить своим клиентам более выгодные, чем в обычных банках, условия, например, меньшие проценты по кредиту или более высокие выплаты по депозитным сертификатам.

Чисто сетевые банки так же надежны, как и любой американский банк, потому что надежность банка определяется гарантиями государства, которое страхует вклады до 100000 долларов в любом американском банке.

Использование средств Интернета становится привлекательным для клиентов налоговых органов, страховых компаний и др.

Однако чем проще доступ в Сеть, тем сложнее обеспечить ее информационную безопасность, так как пользователь может даже и не узнать, что у него были скопированы файлы и программы, не говоря уже о возможности их порчи и корректировки.

Платой за пользование Internet является всеобщее снижение информационной безопасности.

Безопасность данных является одной из главных проблем в Internet. Появляются сведения о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных или получают доступ в архивам коммерческих данных.

В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т.п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана, а priori.

Платой за пользование Internet являются следующие информационные угрозы:

- организация внешних атак на корпоративную сеть;
- несанкционированный доступ к сети организации со стороны рабочих станций, удаленных и передающих серверов, включенных в сеть Internet;
- потеря информации в каналах связи Internet в результате заражения вредоносными программами, некомпетентности сотрудников, отказа канала связи, стихийных бедствий;
- несанкционированный программно-аппаратный доступ к информации, находящейся в канале связи Internet;
- несанкционированный доступ к информации через электромагнитные излучения каналов связи и средств передачи информации Internet;
- несанкционированный доступ к информации, размещенной на удаленных и передающих серверах Internet;
- сбор и мониторинг сетевой информации в интересах третьих лиц;

- переизбыток ненужной и вредоносной информации в системе.

Из всего вышеперечисленного следует, что если ваш компьютер или корпоративная сеть является носителем ценной информации необходимо серьезно подумать перед подключением ее в Internet. И перед выполнением следующих рекомендаций выполнить по возможности все рекомендации по средствам защиты перечисленные выше. Провести тщательный анализ и изъятие конфиденциальной информации из подключаемой сети или персонального компьютера. Проконсультироваться со специалистами, занимающимися информационной безопасностью, и выполнить нижеизложенные рекомендации до подключения к Internet. Итак, пути решения:

- При работе в сети Internet на первое место выходит "межсетевой экран" или брандмауэр. Брандмауэр - неотъемлемая часть системы защиты, без которой невозможна разработка ее политики. Брандмауэр позволяет значительно снизить число эффективных внешних атак на корпоративную сеть или персональный компьютер, несанкционированный доступ к сети организации со стороны рабочих станций, удаленных и передающих серверов, включенных в сеть Internet, снизить вероятность сбора и мониторинга сетевой информации в интересах третьих лиц, блокировать доступ ненужной и вредоносной информации в систему;

- использование VPN технологии, алгоритмов криптографирования (электронной подписи, сжатия с паролем, шифрования), позволяет снизить потери от несанкционированного программно-аппаратного доступа к информации, находящейся в канале связи Internet, доступ к информации через электромагнитные излучения каналов связи и средств передачи информации Internet, также доступа к информации, размещенной на удаленных и передающих серверах Internet, сбор и мониторинг информации в интересах третьих лиц;

- дублирование канала Internet и сжатие информации позволяет повысить надежность системы в случае отказа или перегрузки канала связи и в случае стихийных бедствий;

- использование антивирусных средств, не без оснований, считается необходимым условием при подключении к Internet, позволяет значительно снизить потери информации в результате заражения вредоносными программами;

- использование автоматизированных средств проверки сети на возможные уязвимости в системе защиты и аудита безопасности корпоративных серверов позволяет установить источники угроз и значительно снизить вероятность эффективных атак на корпоративную сеть или персональный компьютер;

- использование Proxu и анонимных серверов позволяет оставаться условно анонимным при действиях в Internet и снизить риски, связанные со сбором и мониторинг сетевой информации в интересах третьих лиц, потоком ненужной и вредоносной информации в систему;

- использование систем ограничения доступа сотрудников к сетевым ресурсам Internet, использование маршрутизаторов и надежных поставщиков сетевых услуг, кратковременного канала связи позволяют сократить сбор и мониторинг сетевой информации в интересах третьих лиц, поток ненужной и вредоносной информации в систему.

Одним из наиболее распространенных механизмов защиты является применение межсетевых экранов - **брандмауэров (firewalls)**.

Стоит отметить, что вследствие непрофессионализма администраторов и недостатков некоторых типов брандмауэров порядка 30% взломов совершается после установки защитных систем.

Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем. Экран (firewall) - это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Экран выполняет свои функции, контролируя все информационные потоки

между этими двумя множествами информационных систем, работая как некоторая "информационная мембрана". В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа, в частности, фиксировать все "незаконные" попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.

Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия "внутри" и "снаружи", и задача экрана состоит в защите внутренней сети от "потенциально враждебного" окружения. Важнейшим примером потенциально враждебной внешней сети является Internet.

Рассмотрим более подробно, какие проблемы возникают при построении экранирующих систем. При этом мы будем рассматривать не только проблему безопасного подключения к Internet, но и разграничение доступа внутри корпоративной сети организации.

Первое, очевидное требование к таким системам, это обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

Во-вторых, экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации и, кроме того, для обеспечения простой реконфигурации системы при изменении структуры сети.

В-третьих, экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий.

В-четвертых, экранирующая система должна работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в "пиковых" режимах. Это необходимо для того, чтобы firewall нельзя было, образно говоря, "забросать" большим количеством вызовов, которые привели бы к нарушению ее работы.

Пятое. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку она является ключом к конфиденциальной информации в организации.

Шестое. В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности.

Седьмое. Система Firewall должна иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им, тем не менее, требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна уметь надежно распознавать таких пользователей и предоставлять им необходимый доступ к информации.

СТРУКТУРА СИСТЕМЫ SOLSTICE FIREWALL- 1 Классическим примером, на котором хотелось бы проиллюстрировать все вышеизложенные принципы, является программный комплекс Solstice FireWall-1 компании Sun Microsystems. Данный пакет неоднократно отмечался наградами на выставках и конкурсах. Он обладает многими полезными особенностями, выделяющими его среди продуктов аналогичного назначения.

Рассмотрим основные компоненты Solstice FireWall- 1 и функции, которые они реализуют.

Центральным для системы Fire Wall- 1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети. Следует

отметить, что продуманность и удобство графического интерфейса модуля управления отмечалось во многих независимых обзорах, посвященных продуктам данного класса.

Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

- Определить объекты, участвующие в процессе обработки информации. Здесь имеются в виду пользователи и группы пользователей, компьютеры и их группы, маршрутизаторы и различные подсети локальной сети организации.

- Описать сетевые протоколы и сервисы, с которыми будут работать приложения. Впрочем, обычно достаточным оказывается набор более чем из 40 описаний, поставляемых с системой FireWall-1.

- Далее, с помощью введенных понятий описывается политика разграничения доступа в следующих терминах: "Группе пользователей А разрешен доступ к ресурсу Б с помощью сервиса или протокола С, но об этом необходимо сделать пометку в регистрационном журнале". Совокупность таких записей компилируется в исполнимую форму блоком управления и далее передается на исполнение в модули фильтрации.

Модули фильтрации могут располагаться на компьютерах - шлюзах или выделенных серверах - или в маршрутизаторах как часть конфигурационной информации. В настоящее время поддерживаются следующие два типа маршрутизаторов: Cisco IOS 9.x, 10.x, а также BayNetworks (Wellfleet) OS v.8.

Модули фильтрации просматривают все пакеты, поступающие на сетевые интерфейсы, и, в зависимости от заданных правил, пропускают или отбрасывают эти пакеты, с соответствующей записью в регистрационном журнале. Следует отметить, что эти модули, работая непосредственно с драйверами сетевых интерфейсов, обрабатывают весь поток данных, располагая полной информацией о передаваемых пакетах.

Система Solstice FireWall-1 имеет собственный встроенный объектно - ориентированный язык программирования, применяемый для описания поведения модулей - Фильтров системы. Собственно говоря, результатом работы графического интерфейса администратора системы является сгенерированный сценарий работы именно на этом внутреннем языке. Он не сложен для понимания, что допускает непосредственное программирование на нем. Однако на практике данная возможность почти не используется, поскольку графический интерфейс системы и так позволяет сделать практически все, что нужно.

FireWall-1 полностью прозрачен для конечных пользователей. Еще одним замечательным свойством системы Solstice FireWall-1 является очень высокая скорость работы. Фактически модули системы работают на сетевых скоростях передачи информации, что обусловлено компиляцией сгенерированных сценариев работы перед подключением их непосредственно в процесс фильтрации.

Компания Sun Microsystems приводит такие данные об эффективности работы Solstice FireWall-1. Модули фильтрации на Internet-шлюзе, сконфигурированные типичным для многих организаций образом, работая на скоростях обычного Ethernet в 10 Мб/сек, забирают на себя не более 10% вычислительной мощности процессора SPARCstation 5,85 МГц или компьютера 486DX2-50 с операционной системой Solaris/x86.

Solstice FireWall-1 - эффективное средство защиты корпоративных сетей и их сегментов от внешних угроз, а также от несанкционированных взаимодействий локальных пользователей с внешними системами.

Solstice FireWall-1 обеспечивает высокоуровневую поддержку политики безопасности организации по отношению ко всем протоколам семейства TCP/IP. Solstice FireWall-1 характеризуется прозрачностью для легальных пользователей и высокой эффективностью.

По совокупности технических и стоимостных характеристик Solstice FireWall-1 занимает лидирующую позицию среди межсетевых экранов.

Рассмотрим 2 способа ограничения доступа в WWW серверах:

- Ограничить доступ по IP адресам клиентских машин;
- ввести идентификатор получателя с паролем для данного вида документов.

Такого рода ввод ограничений стал использоваться достаточно часто, т.к. многие стремятся в Internet, чтобы использовать его коммуникации для доставки своей информации потребителю. С помощью такого рода механизмов по разграничению прав доступа удобно производить саморассылку информации, на получение которой существует договор.

Ограничения по IP адресам

Доступ к приватным документам можно разрешить, либо наоборот запретить используя IP адреса конкретных машин или сеток, например:

123.456.78.9

123.456.79.

В этом случае доступ будет разрешен (или запрещен в зависимости от контекста) для машины с IP адресом 123.456.78.9 и для всех машин подсети 123.456.79.

Ограничения по идентификатору получателя

Доступ к приватным документам можно разрешить, либо наоборот запретить используя присвоенное имя и пароль конкретному пользователю, причем пароль в явном виде нигде не хранится. Рассмотрим такой пример: Агентство печати предоставляет свою продукцию, только своим подписчикам, которые заключили договор и оплатили подписку. WWW Сервер находится в сети Internet и общедоступен.

Выберем Вестник предоставляемый конкретному подписчику. На клиентском месте подписчик получает сообщение.

Если он правильно написал свое имя и пароль, то он допускается до документа, в противном случае - получает сообщение Authorization failed. Retry? **Защита электронной почты: PEM, S/MIME и PGP**

Для защиты электронной почты в Интернете есть множество различных протоколов, но лишь один или два из них используются достаточно широко. PEM (Privacy Enhanced Mail) - это стандарт Интернета для защиты электронной почты с использованием открытых или симметричных ключей. Он применяется все реже, поскольку не предназначен для обработки нового, поддерживаемого MIME, формата электронных посланий и, кроме того, требует жесткой иерархии сертификационных центров для выдачи ключей. S/MIME - новый стандарт. Он задействует многие криптографические алгоритмы, запатентованные и лицензированные компанией RSAData Security Inc. S/MIME использует цифровые сертификаты, и следовательно, при обеспечении аутентификации полагается на сертификационный центр (корпоративный или глобальный).

Еще одно популярное приложение, разработанное для защиты посланий и файлов - PGP (Pretty Good Privacy). Вероятно, это самое распространенное приложение защиты электронной почты в Интернете, использующее различные стандарты шифрования. Приложения шифрования-расшифровки PGP выпускаются для всех основных операционных систем, и послания можно шифровать до использования программы отправки электронной почты. Некоторые почтовые программы, такие как Eudora Pro фирмы Qualcomm и OnNet от FTP Software, позволяют подключать специальные PGP-модули для обработки зашифрованной почты. PGP построена на принципе паутины доверия (web of trust) и позволяет пользователям распространять свои ключи без посредничества сертификационных центров.

В настоящее время есть два основных набора инструментов, призванных упростить для разработчиков задачу внедрения криптографических методов защиты в приложения для персональных компьютеров - это CryptoAPI от Microsoft и CDSA (Common Data Security Architecture) от Intel.

Microsoft разрабатывает интегрированную систему безопасности Интернета -

Internet Security Framework - совместимую с Microsoft Windows 95 и Microsoft Windows NT. Важный компонент этой интегрированной системы - CryptoAPI. Этот интерфейс прикладного программирования (API) действует на уровне операционной системы и предоставляет разработчикам в среде Windows средства вызова криптографических функций (таких как алгоритмы шифрования) через стандартизированный интерфейс.

Поскольку CryptoAPI имеет модульную структуру, он позволяет разработчикам в зависимости от их потребностей заменять один криптографический алгоритм другим. CryptoAPI также обладает средствами для обработки цифровых сертификатов.

CDSA от Intel предлагает практически те же самые функциональные возможности, что и CryptoAPI, но этот набор инструментов с самого начала предназначался для многоплатформенного использования, а не только для WindowsV. Некоторые компании (в том числе Netscape, Datakey, VASCO Data Security и Verisign) уже включили поддержку CDSA в свои продукты.

Корпоративные сети часто связывают офисы, разбросанные по городу, региону, стране или всему миру. В настоящее время ведутся работы по защите на сетевом уровне IP-сетей (именно такие сети формируют Интернет), что позволит компаниям создавать свои собственные виртуальные частные сети (virtual private networks, VPN) и использовать Интернет как альтернативу дорогим арендованным линиям.

Ведущие поставщики брандмауэров и маршрутизаторов выступили с инициативой: предложили технологию S/WAN (Secure Wide Area Networks). Они взяли на себя внедрение и тестирование протоколов, предлагаемых Рабочей группой инженеров Интернета (Internet Engineering Task Force, IETF) для защиты IP-пакетов. Эти протоколы обеспечивают аутентификацию и шифрование пакетов, а также методы обмена и управления ключами для шифрования и аутентификации. Протоколы S/WAN помогут достичь совместимости между маршрутизаторами и брандмауэрами различных производителей, что позволит географически разбросанным офисам одной корпорации, а также партнерам, образующим виртуальное предприятие, безопасно обмениваться данными по Интернету.

Защита информации в персональном компьютере

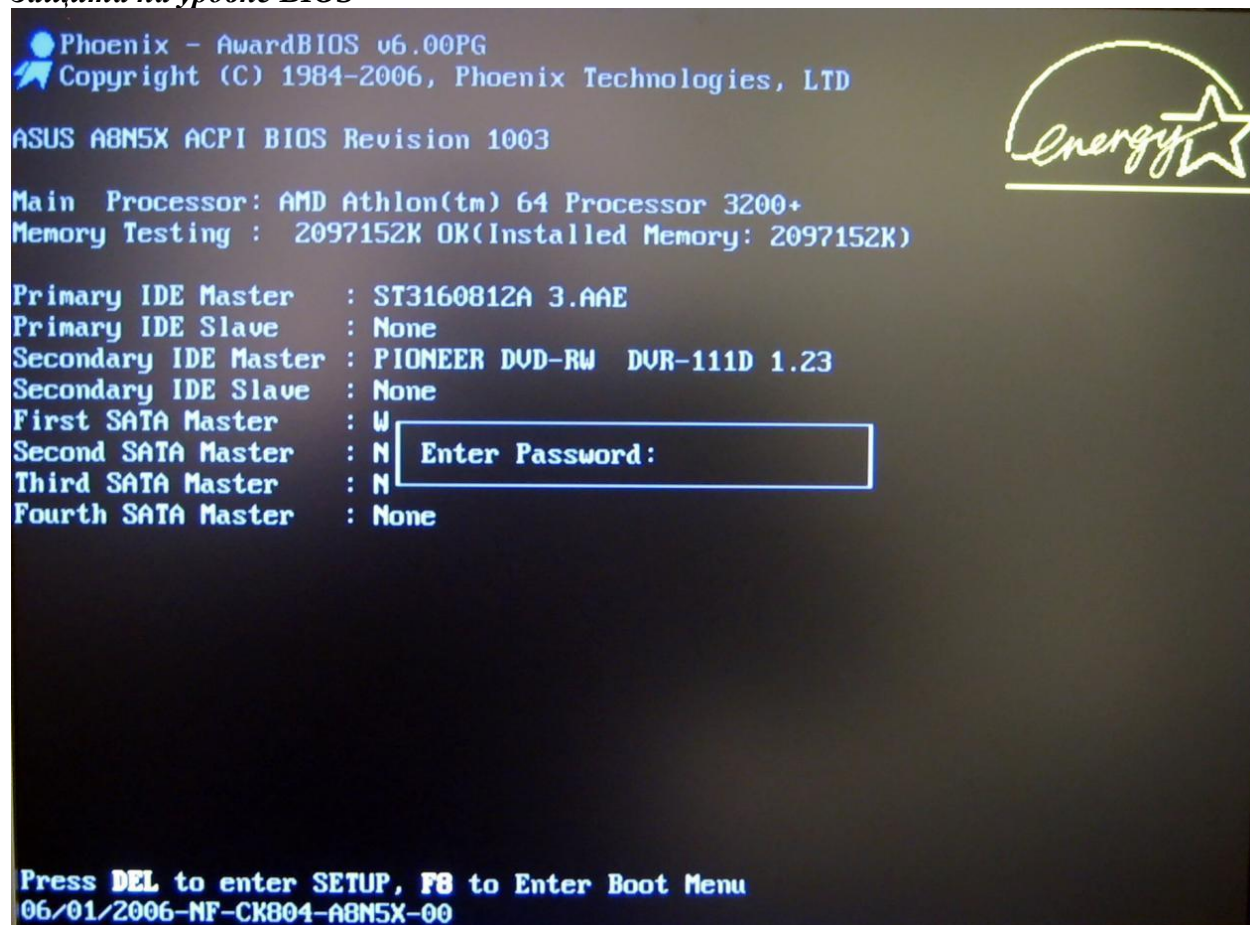
Общие рекомендации по защите

- Избегайте общественного Wi-Fi и компьютеров
- При работе на чужом компьютере не допускайте сохранения своих учетных данных
- Удаляйте временные файлы

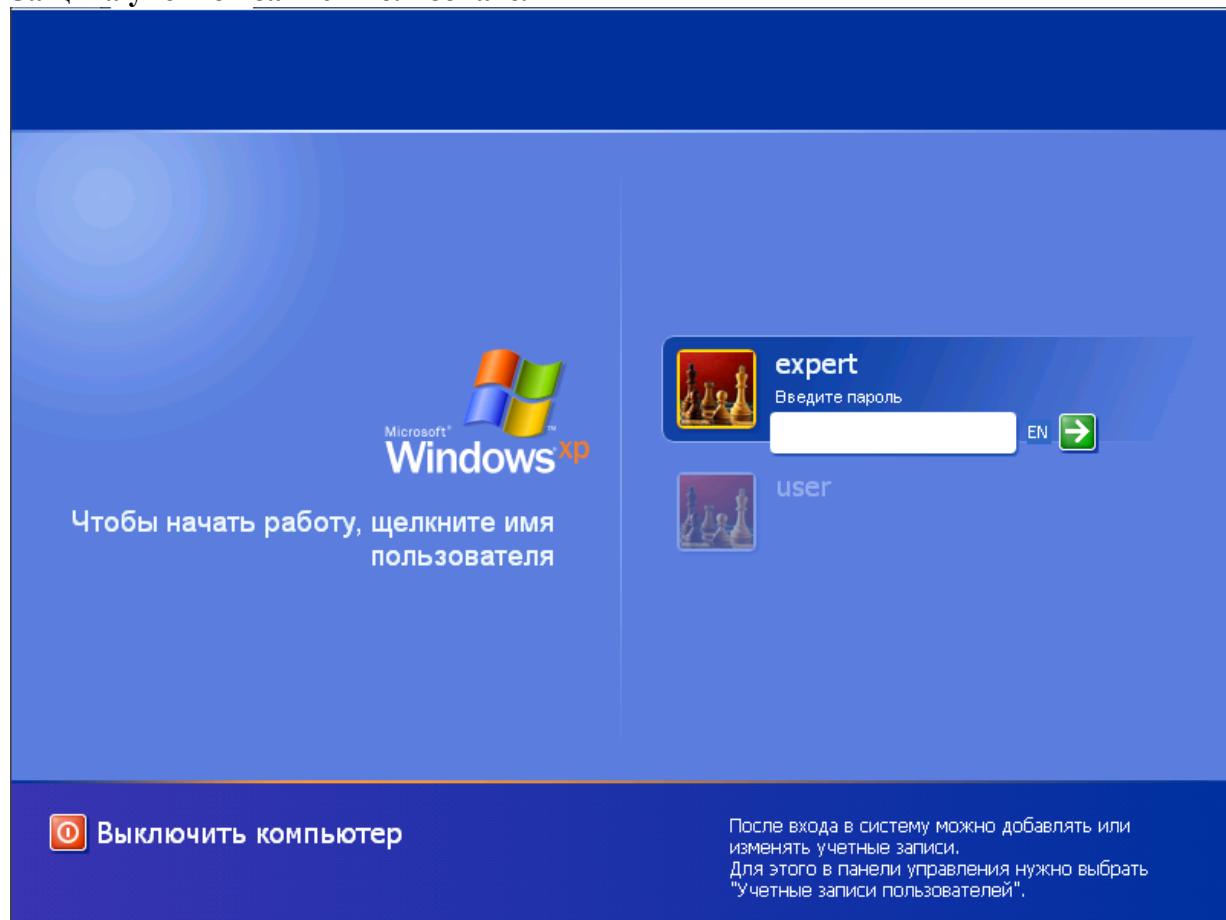
Общие рекомендации по защите

- Ограничение доступа к данным

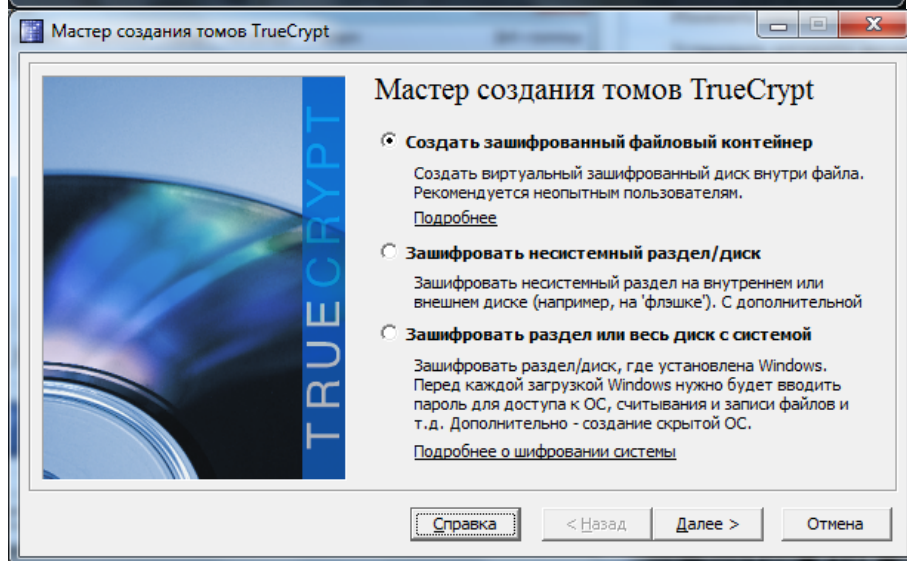
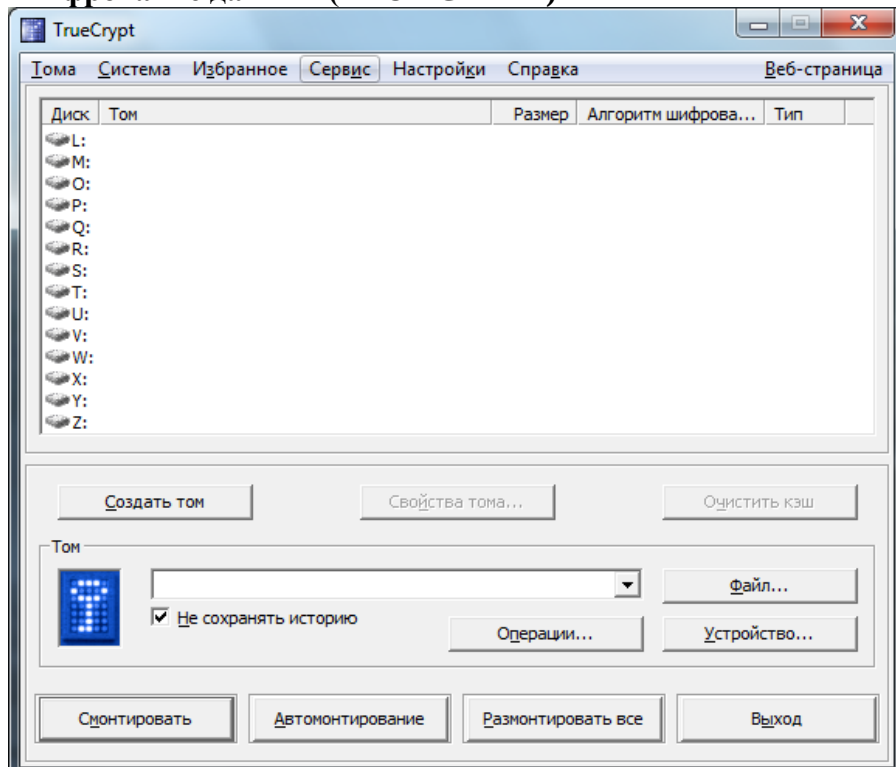
Защита на уровне BIOS



Защита учетной записи пользователя



Шифрование данных (TRUE CRYPT)



Non-System disk or disk error
Replace and strike any key when ready
—

Общие рекомендации по защите

- Регулярное обновление ПО
- Своевременное обновление вирусных баз
- Сканирование съемных носителей
- Периодическая проверка системы
- Использование комплексных систем защиты

Использование комплексных систем защиты

1. Kaspersky	Internet Security 2013
2. BitDefender	Internet Security 2013
3. Norton	Internet Security 2013
4. G-Data	Internet Security 2013
5. AVG	Internet Security 2013
F-SECURE	Internet Security 2013
Trend Micro Titanium	Int. Security 2013
AVAST 7 Free Antivirus	
ESET	SMART SECURITY 6

Общие рекомендации по защите

- Не используйте одинаковый пароль для доступа к разным ресурсам
- Не записывайте пароль в общедоступном месте
- Используйте надежные пароли

Пароли

«неправильные» пароли:

Цифровые (даты, телефоны, номера паспортов)

Слова, имена, клички и т.д.

Малая длина (менее 8 символов)

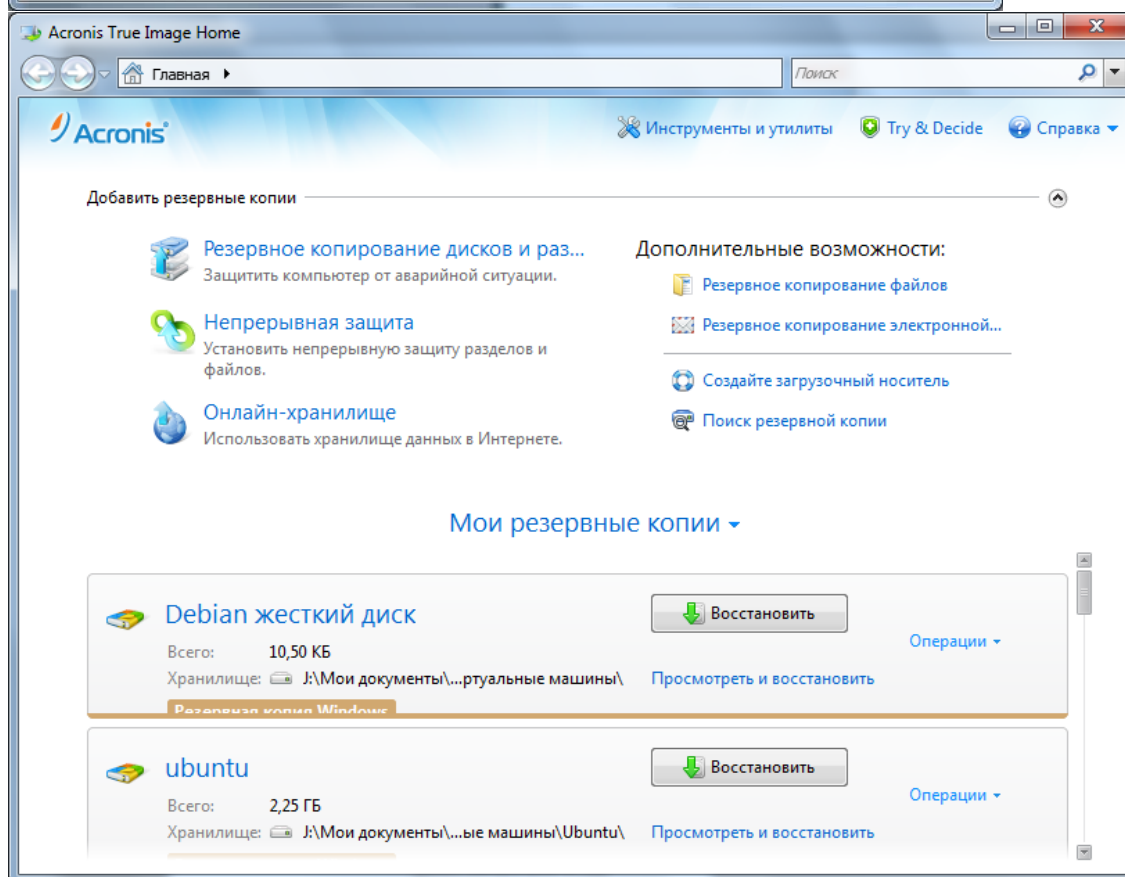
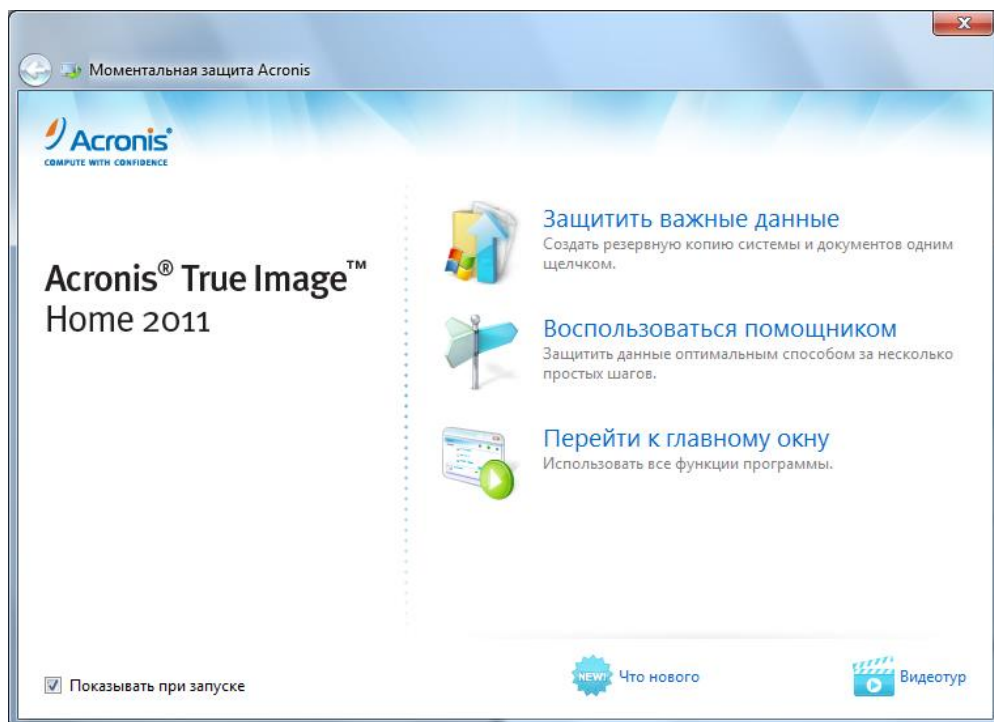
«правильные» пароли:

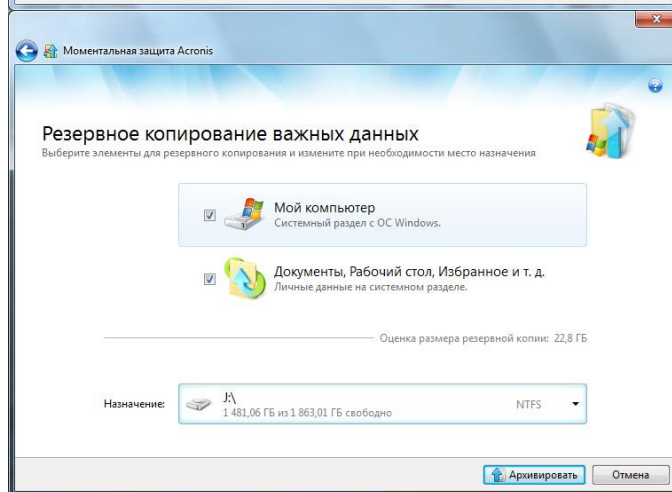
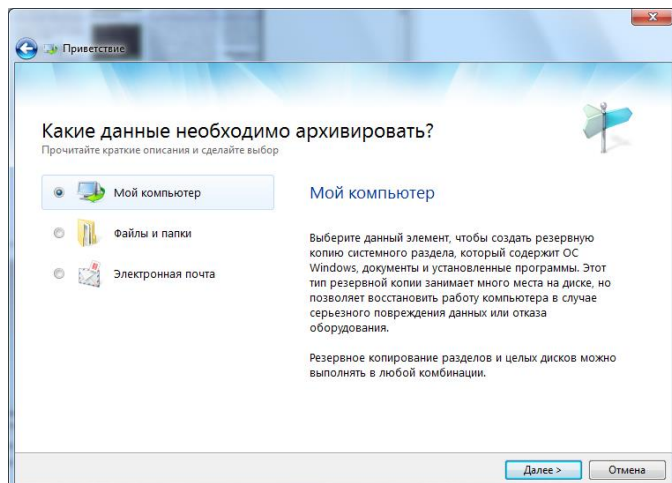
Длина 10 символов и более

Комбинации маленьких и больших букв, специальных символов (точки, кавычки, скобки и др.) и пробела.

Способы защиты

- Резервирование информации
 - Резервирование системного раздела
 - Резервирование пользовательских данных

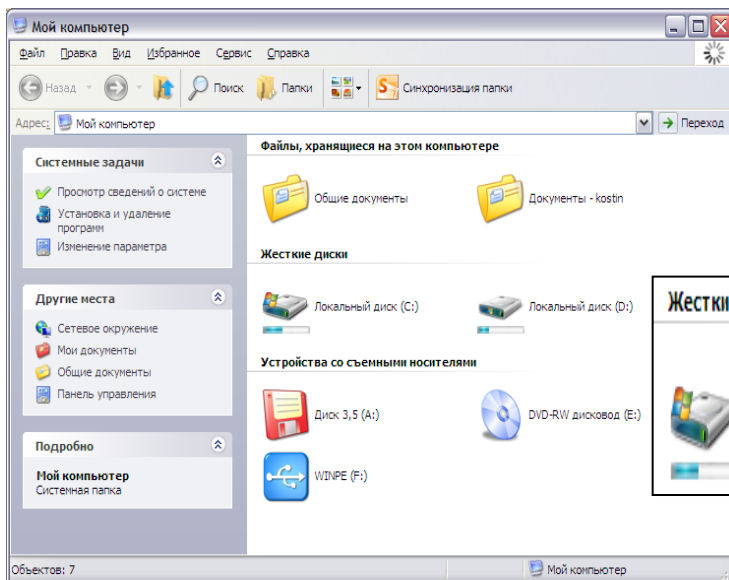




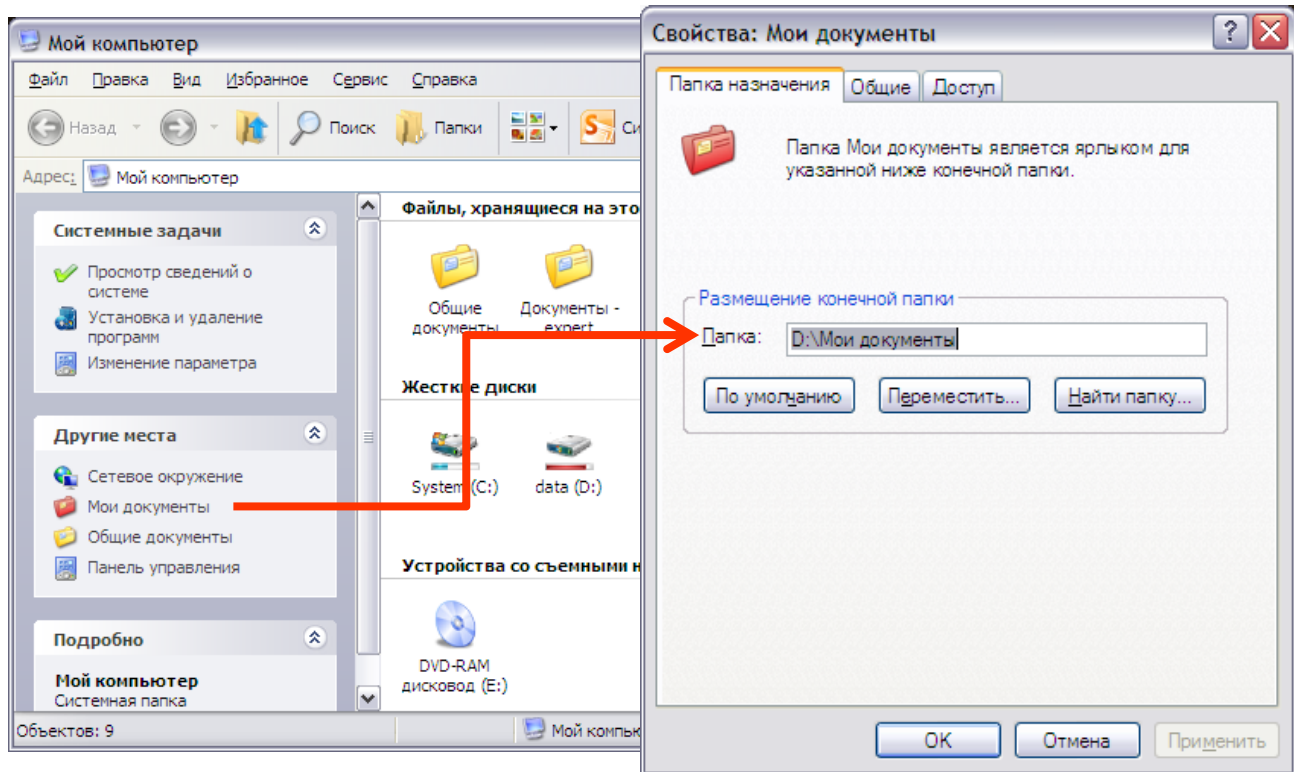
Способы защиты

Организация хранения информации

- Создание отдельных разделов диска для хранения данных



■ Размещение папки «Мои документы» в несистемном разделе диска

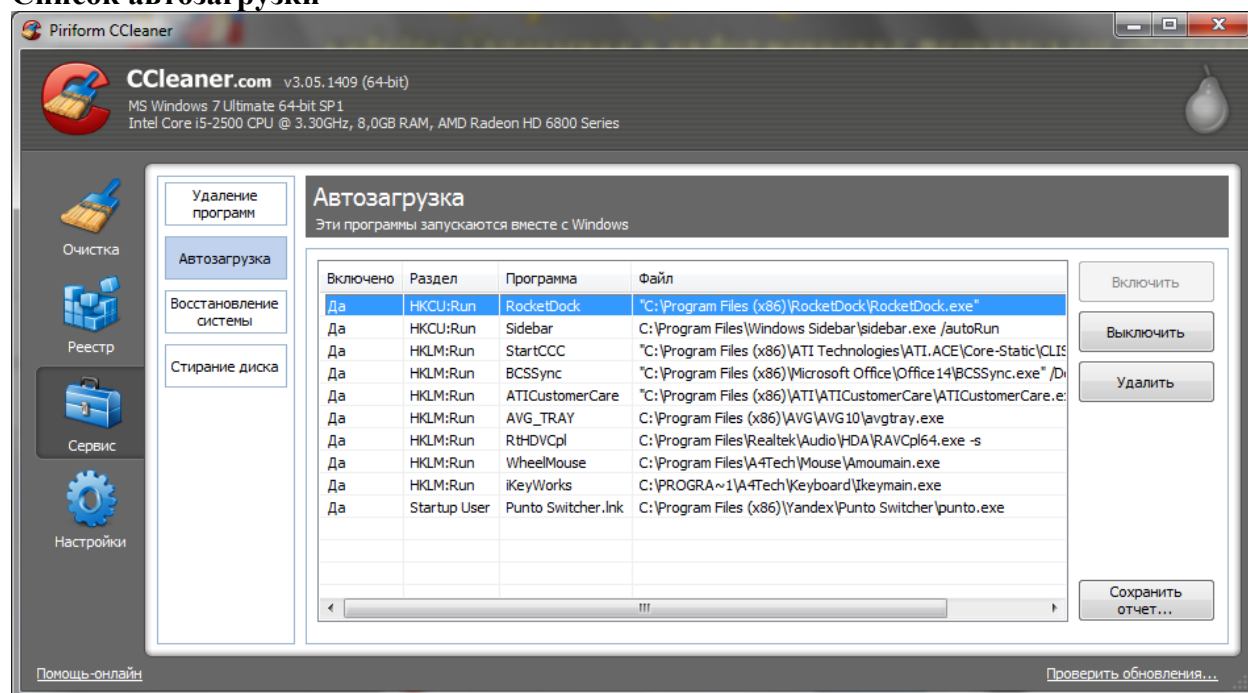


■ Не размещать файлы на «Рабочем столе»

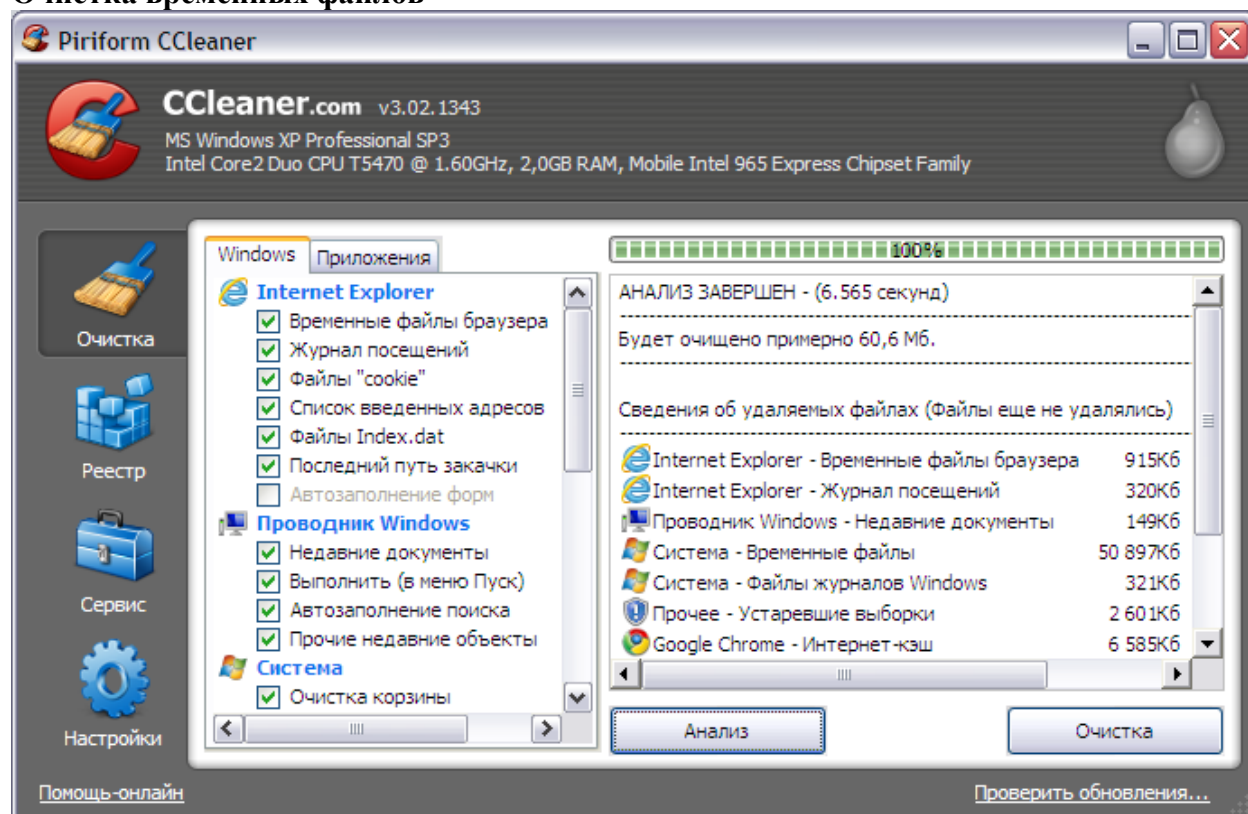


Настройка и обслуживание системы

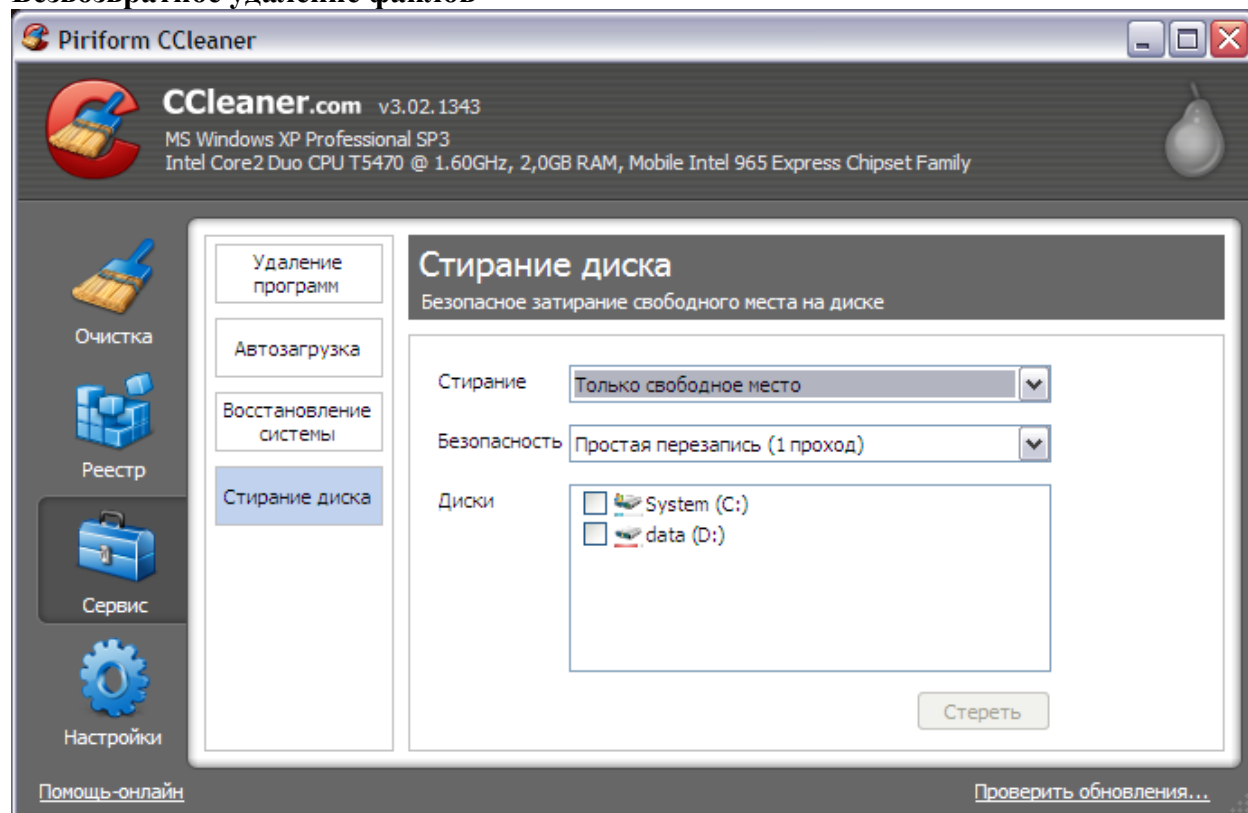
Список автозагрузки



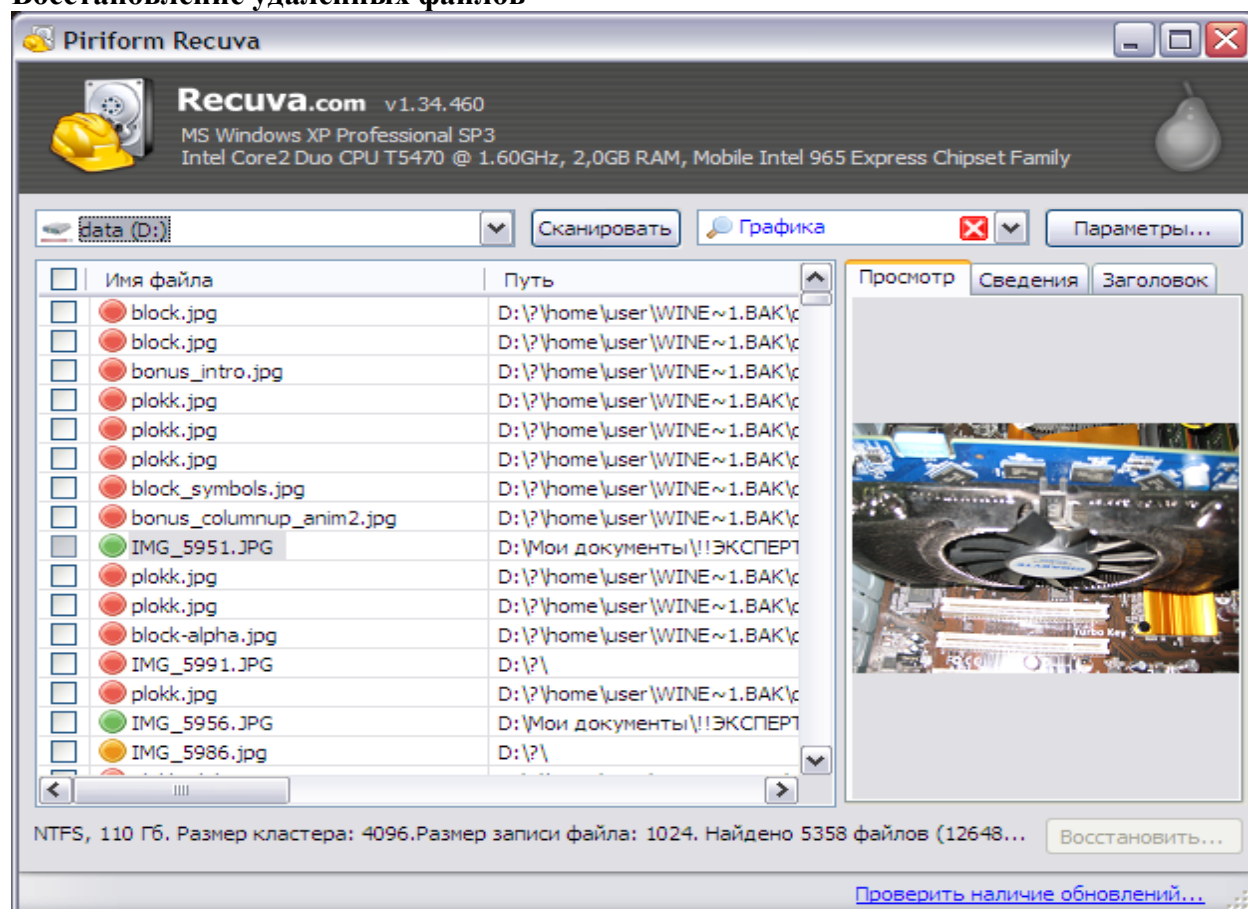
Очистка временных файлов



Безвозвратное удаление файлов



Восстановление удаленных файлов



Основные сервисы системы Интернет

- World Wide Web (WWW) - главный информационный сервис. Гипермедийная информационная система поиска ресурсов Интернет и доступа к ним.
- Программы-браузеры. Информацию, полученную от любого сервера, браузер WWW выводит на экран в стандартной, удобной для восприятия форме.
- Программа удаленного доступа Telnet. Позволяет входить в другую вычислительную систему, работающую в Интернет
- Программа пересылки файлов_Ftp. Перемещает копии файлов с одного узла Интернет на другой.
- Электронная почта (Electronic mail, англ. mail - почта, сокр. E-mail). Служит для передачи текстовых сообщений в пределах Интернет, а также между другими сетями электронной почты.
- Система телеконференций Usenet (от Users Network. Организует коллективные обсуждения по различным направлениям, называемые телеконференциями.
- Системы информационного поиска сети Интернет

Функции электронной почты

- обмен сообщениями между пользователями;
- обмен документами между пользователями;
- обмен данными между приложениями;
- оповещение пользователей о наступлении определенных событий.

Адрес электронной почты имеет вид:

логин@символический адрес сервера.имя зоны

Первая часть почтового адреса — это имя пользователя, вторая часть — доменная. ivanov@unn.ru.

Глава 4 Организация системы защиты информации экономических систем

4.1 Этапы построения системы защиты информации

Каждую систему защиты следует разрабатывать индивидуально, учитывая следующие особенности:

- организационную структуру организации;
- объем и характер информационных потоков (внутри объекта в целом, внутри отделов, между отделами, внешних);
- количество и характер выполняемых операций: аналитических и повседневных;
- количество и функциональные обязанности персонала;
- количество и характер клиентов;
- график суточной нагрузки.

Защита должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. Построение защиты предполагает следующие этапы:

- анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;
- реализация системы защиты на основе результатов анализа риска;
- постоянный контроль за работой системы защиты и АИС в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

На сегодняшний день защита АИС — это самостоятельное направление исследований. Поэтому легче и дешевле использовать для выполнения работ по защите специалистов, чем дважды учить своих людей (сначала их будут учить преподаватели, а потом они будут учиться на своих ошибках).

Главное при защите АИС специалистами (естественно после уверенности в их компетенции в данном вопросе) — наличие здравого смысла у администрации системы. Обычно, профессионалы склонны преувеличивать реальность угроз безопасности АИС и не обращать внимания на такие «несущественные детали» как удобство ее эксплуатации, гибкость управления системой защиты и т.д., без чего применение системы защиты становится трудным делом. Построение системы защиты — это процесс поиска компромисса между уровнем защищенности АИС и сохранением возможности работы в ней. Здравый смысл помогает преодолеть большинство препятствий на этом пути.

Для обеспечения непрерывной защиты информации в АИС целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

Один из самых важных прикладных аспектов теории защиты — защита сети. При этом, с одной стороны, сеть должна восприниматься как единая система и, следовательно, ее защита также должна строиться по единому плану. С другой стороны, каждый узел сети должен быть защищен индивидуально.

Защита конкретной сети должна строиться с учетом конкретных особенностей: назначения, топологии, особенностей конфигурации, потоков информации, количества пользователей, режима работы и т.д.

Кроме того, существуют специфические особенности защиты информации на *ПЭВМ*, в базах данных. Нельзя также упускать из виду такие аспекты, как физическая защита компьютеров, периферийных устройств, дисплейных и машинных залов. Иногда бывает необходим и «экзотический» вид защиты — от электромагнитного излучения или защита каналов связи.

Основные этапы построения системы защиты заключаются в следующем:

Анализ -> Разработка системы защиты (планирование) -> Реализация системы защиты -> Сопровождение системы защиты.

Этап анализа возможных угроз АИС необходим для фиксирования на определенный момент времени состояния АИС (конфигурации аппаратных и программных средств, технологии обработки информации) и определения возможных воздействий на каждый компонент системы. Обеспечить защиту АИС от всех воздействий на нее невозможно, хотя бы потому, что невозможно полностью установить перечень угроз и способов их реализации. Поэтому надо выбрать из всего множества возможных воздействий лишь те, которые могут реально произойти и нанести серьезный ущерб владельцам и пользователям системы.

На этапе планирования формируется система защиты как единая совокупность мер противодействия различной природы.

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: правовые, морально-этические,

административные, физические и технические (аппаратные и программные).

Наилучшие результаты достигаются при системном подходе к вопросам обеспечения безопасности АИС и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Очевидно, что в структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего, надо решить правовые и организационные вопросы.

Результатом этапа планирования является план защиты — документ, содержащий перечень защищаемых компонентов АИС и возможных воздействий на них, цель защиты информации в АИС, правила обработки информации в АИС, обеспечивающие ее защиту от различных воздействий, а также описание разработанной системы защиты информации.

При необходимости, кроме плана защиты на этапе планирования может быть разработан план обеспечения непрерывной работы и восстановления функционирования АИС, предусматривающий деятельность персонала и пользователей системы по восстановлению процесса обработки информации в случае различных стихийных бедствий и других критических ситуаций.

Сущность этапа реализации системы защиты заключается в установке и настройке средств защиты, необходимых для реализации зафиксированных в плане защиты правил обработки информации. Содержание этого этапа зависит от способа реализации механизмов защиты в средствах защиты.

К настоящему времени сформировались два основных способа реализации механизмов защиты.

При первом из них механизмы защиты не реализованы в программном и аппаратном обеспечении АИС; либо реализована только часть их, необходимая для обеспечения работоспособности всей АИС (например, механизмы защиты памяти в мультиспользовательских системах). Защита информации при хранении, обработке или передаче обеспечивается дополнительными программными или аппаратными средствами, не входящими в состав самой АИС. При этом средства защиты поддерживаются внутренними механизмами АИС.

Такой способ получил название «добавленной» (add-on) защиты, поскольку средства защиты являются дополнением к основным программным и аппаратным средствам АИС. Подобного подхода в обеспечении безопасности придерживается, например, фирма IBM, почти все модели ее компьютеров и ОС, от персональных до больших машин, используют добавленную защиту (например, пакет RACF).

Другой способ носит название «встроенной» (built-in) защиты. Он заключается в том, что механизмы защиты являются неотъемлемой частью АИС разработанной и реализованной с учетом определенных требований безопасности. Механизмы защиты могут быть реализованы в виде отдельных компонентов АИС, распределены по другим компонентам системы (то есть в некотором компоненте АИС есть часть, отвечающая за

поддержание его защиты). При этом средства защиты составляют единый механизм, который отвечает за обеспечение безопасности всей АИС.

Оба способа — добавленной и встроенной защиты — имеют свои преимущества и недостатки. Добавленная защита является более гибкой, ее механизмы можно добавлять или удалять по мере необходимости. Это не составит большого труда, так как они все реализованы отдельно от других процедур системы. Однако в этом случае остро встает вопрос поддержки работы этих механизмов встроенными механизмами ОС, в том числе и аппаратными. В том случае, если добавляемые средства защиты не поддерживаются встроенными механизмами АИС, то они не обеспечат необходимого уровня безопасности.

Проблемой может стать сопряжение встроенных механизмов с добавляемыми программными средствами — довольно сложно разработать конфигурацию механизмов защиты, их интерфейс с добавляемыми программными средствами так, чтобы защита охватывала всю систему целиком.

Другой проблемой является оптимальность защиты. При любой проверке прав, назначении полномочий, разрешений доступа и т.д. необходимо вызывать отдельную процедуру. Естественно, это сказывается на производительности системы. Не менее важна и проблема совместимости защиты с имеющимися программными средствами. Как правило, при добавленной защите вносятся некоторые изменения в логику работы системы. Эти изменения могут оказаться неприемлемыми для некоторых прикладных программ. Такова плата за гибкость и облегчение обслуживания средств защиты.

Основное достоинство встроенной защиты — надежность и оптимальность. Это объясняется тем, что средства защиты и механизмы их поддержки разрабатывались и реализовывались одновременно с самой системой обработки информации, поэтому взаимосвязь средств защиты с различными компонентами системы теснее, чем при добавленной защите. Однако встроенная защита обладает жестко фиксированным набором функций, не позволяя расширять или сокращать их. Некоторые функции можно только отключить.

Справедливости ради стоит отметить, что оба вида защиты в чистом виде встречаются редко. Как правило, используются их комбинации, что позволяет объединять достоинства и компенсировать недостатки каждого из них.

Комплексная защита АИС может быть реализована как с помощью добавленной, так и встроенной защиты.

Этап сопровождения заключается в контроле работы системы, регистрации происходящих в ней событий, их анализе с целью обнаружить нарушения безопасности.

В том случае, когда состав системы претерпел существенные изменения (смена вычислительной техники, переезд в другое здание, добавление новых устройств или программных средств), требуется повторение описанной выше последовательности действий.

Стоит отметить тот немаловажный факт, что обеспечение защиты АИС — это итеративный процесс, завершающийся только с завершением жизненного цикла всей системы. На последнем этапе анализа риска производится оценка реальных затрат и выигрыша от применения предполагаемых мер защиты. Величина выигрыша может иметь как положительное, так и отрицательное значение. В первом случае это означает, что использование системы защиты приносит очевидный выигрыш, а во втором — лишь дополнительные расходы на обеспечение собственной безопасности.

Сущность этого этапа заключается в анализе различных вариантов построения системы защиты и выборе оптимального из них по некоторому критерию (обычно по наилучшему соотношению «эффективность/стоимость»).

Приведем пример: необходимо оценить выгоду при защите информации от раскрытия или обработки на основе некорректных данных в течении одного года.

Величину ущерба от реализации этих угроз оценим в \$1.000.000. Предположим, предварительный анализ показал, что в среднем эта ситуация встречается один раз в

десять лет ($P=0.1$).

Тогда стоимость потерь для данной угрозы (CP) составит:

$$CP = C * P = \$1.000.000 * 0.1 = \$100.000$$

Далее зададимся эффективностью методов защиты. Для данного абстрактного случая предположим, что в результате экспертной оценки методов защиты было получено значение 60% (в шести случаях из десяти защита срабатывает), тогда:

$$EM = 60\% * CP = \$60.000$$

Затраты на реализацию этих методов (закупка средств защиты, обучение персонала, изменение технологии обработки информации, зарплата персоналу и т.д.) составили (CM) \$25.000. Тогда величина выгоды равна:

$$PR = EM - CM = \$60.000 - \$25.000 = \$35.000.$$

В рассмотренном случае величина выгоды имеет положительное значение, что говорит о целесообразности применения выбранных методов защиты.

После того, как были определены угрозы безопасности АИС, от которых будет производиться защита и выбраны меры защиты, требуется составить ряд документов, отражающих решение администрации АИС по созданию системы защиты. Это решение конкретизируется в нескольких планах: плане защиты и плане обеспечения непрерывной работы и восстановления функционирования АИС.

План защиты — это документ, определяющий реализацию системы защиты организации и необходимый в повседневной работе. Он необходим:

- Для определения, общих правил обработки информации в АИС, целей построения и функционирования системы защиты и подготовки сотрудников.
- Для фиксирования на некоторый момент времени состава АИС, технологии обработки информации, средств защиты информации.
- Для определения должностных обязанностей сотрудников организации по защите информации и ответственности за их соблюдение.

План представляет собой организационный фундамент, на котором строится все здание системы защиты. Он нуждается в регулярном пересмотре и, если необходимо, изменении.

План защиты обычно содержит следующие группы сведений:

- Политика безопасности.
- Текущее состояние системы.
- Рекомендации по реализации системы защиты.
- Ответственность персонала.
- Порядок ввода в действие средств защиты.
- Порядок пересмотра плана и состава средств защиты.

Рассмотрим подробнее эти группы сведений.

Политика безопасности. В этом разделе должен быть определен набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в АИС. Раздел должен содержать:

- Цели, преследуемые реализацией системы защиты в вычислительной системе (например, защита данных компании от несанкционированного доступа, защита от утери данных и др.).
- Меры ответственности средств защиты и нижний уровень гарантированной защиты (например, в работе небольших групп защищенных компьютеров, в обязанностях каждого из служащих и др.).
- Обязательства и санкции, связанные с защитой (например, штрафы, персональная ответственность и др.).

Рекомендации по реализации системы защиты. Всесторонний анализ риска должен определять размеры наибольших возможных потерь, независимо от вероятности появления соответствующих событий; размеры наибольших ожидаемых потерь; меры, предпринимаемые в случае критических ситуаций, а также стоимость таких мер. Эти результаты используются при определении зон особого контроля и распределении средств для обеспечения защиты. В этом случае план защиты должен

содержать рекомендации, какие средства контроля лучше всего использовать в чрезвычайных ситуациях (то есть имеющие наибольшую эффективность) и какие лучше всего соответствовали бы средствам контроля повседневной работы.

Некоторые ситуации могут приводить к слишком большому ущербу (например, крушение системы), а стоимость средств защиты от них может быть слишком высока или эти средства окажутся неэффективны. В этом случае лучше не учитывать такие ситуации при планировании защиты, хотя их и возникающие при этом возможные последствия следует отразить в плане.

Ответственность персонала. Каждый сотрудник обслуживающего персонала вычислительной системы должен хорошо знать свои обязанности и нести ответственность за свои действия. Ниже приводятся некоторые примеры обязанностей сотрудников и групп сотрудников:

- Пользователь персонального компьютера или терминала несет ответственность за физическую целостность компьютера (терминала) во время сеанса работы с АИС, а также за неразглашение собственного пароля.
- Администратор баз данных несет ответственность за конфиденциальность информации в базах данных, ее логическую непротиворечивость и целостность.
- Сотрудник руководства отвечает за разделение обязанностей служащих в сфере безопасности обработки информации, предупреждение возможных угроз и профилактику средств защиты.

Порядок ввода в действие средств защиты. Ввод в работу крупномасштабных и дорогих средств защиты целесообразно проводить постепенно, давая возможность обслуживающему персоналу и пользователям спокойно ознакомиться со своими новыми обязанностями. Для этого необходимо проводить разного рода тренировки, занятия по разъяснению целей защиты и способов ее реализации.

Этот раздел плана содержит расписание такого рода занятий, а также порядок ввода в действие системы защиты.

Порядок модернизации средств защиты. Важной частью плана защиты является порядок пересмотра состава средств защиты. Состав пользователей, данные, обстановка — все изменяется с течением времени, появляются новые программные и аппаратные средства. Многие средства защиты постепенно теряют свою эффективность и становятся ненужными, или подлежат замене по какой-либо иной причине (например, уменьшается ценность информации, для обработки которой достаточно более простых средств защиты). Поэтому список объектов, содержащих ценную информацию, их содержимое и список пользователей должны периодически просматриваться и изменяться в соответствии с текущей ситуацией. Также

периодически должен проводиться анализ риска, учитывающий изменения обстановки. Последний пункт плана защиты должен устанавливать сроки и условия такого пересмотра, а также условия, при которых может производиться внеочередной пересмотр (например, качественный скачок в разработке методов преодоления защиты, что может нанести серьезный ущерб пользователям и владельцам АИС).

Каким бы всеобъемлющим не был план, все возможные угрозы и защиту от них он предусмотреть не в состоянии. К тому же многие ситуации он должен только описывать — их контроль может оказаться неэффективным (в силу дороговизны средств защиты или малой вероятности появления угроз). В любом случае владельцы и персонал системы должны быть готовы к различным непредвиденным ситуациям.

Для определения действий персонала системы в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АИС необходимо разрабатывать план обеспечения непрерывной работы и восстановления (план ОНРВ). В некоторых случаях план обеспечения непрерывной работы и план восстановления — разные документы. Первый скорее план, позволяющий избежать опасных ситуаций, второй — план реакции на них.

План ОНРВ можно сравнить с планом противопожарной защиты (обеспечение

непрерывной работы) и ликвидации последствий (минимизация ущерба и восстановление функционирования АИС). Про этот план обычно все знают, но никто его не читает, хотя на пепелище об этом обычно сожалеют.

Существует несколько способов смягчения воздействия непредвиденных ситуаций:

- Избегать их. Это наиболее эффективный, но не всегда осуществимый способ. Избегать непредвиденных ситуаций можно с помощью ограничительных мер, предусмотренных планом защиты, а можно и с помощью устранения самой причины потенциального нарушения. Например, с пожаром можно бороться огнетушителем, а можно соблюдением мер противопожарной защиты. С рассерженными пользователями можно бороться административными мерами (разозлив этим их еще больше), а можно и поддержанием здоровой атмосферы в коллективе.

- Если избежать какого-либо нарушения невозможно, необходимо уменьшить вероятность его появления или смягчить последствия от него.

- Если предполагать, что какие-то нарушения все-таки могут произойти, следует предусмотреть меры сохранения контроля над ситуацией. Например, в любой момент может выйти из строя отдельный блок системы — часть компьютера, компьютер целиком, подсеть и т.д., может наступить нарушение энергоснабжения и др. В принципе это может привести к выходу АИС из строя, однако при правильной организации АИС этого можно избежать.

- Если нарушение произошло, необходимо предусмотреть меры по ликвидации последствий и восстановлению информации. Например, в случае сбоя в компьютере — замену сбойного компонента, в случае уничтожения каких-либо данных — восстановление с резервных копий и т.д.

Все приведенные выше четыре способа должны в той или иной мере присутствовать в плане ОНРВ. Для каждой конкретной АИС эти меры следует планировать в процессе анализа риска с учетом особенностей (специфических видов угроз, вероятностей появления, величин ущерба и т.д.) и на основе критерия «эффективность/стоимость». Хороший план ОНРВ должен отвечать следующим требованиям:

* Реальность плана ОНРВ.

План должен оказывать реальную помощь в критических ситуациях, а не оставаться пустой формальностью. Необходимо учитывать психологический момент ситуации, при которой персонал находится в состоянии стресса, поэтому сам план и предлагаемые действия должны быть простыми и ясными. План должен учитывать реальное состояние компонентов системы, способов их взаимодействия и т.д. Повышению действенности плана ОНРВ способствуют тренировки в условиях, приближенных к реальным (естественно без реальных потерь).

* Быстрое восстановление работоспособности системы.

Предлагаемые планом ОНРВ действия должны восстанавливать повседневную деятельность настолько быстро, насколько это возможно. В принципе это главное назначение плана ОНРВ. Расследовать причины и наказать виновных можно потом, главное — продолжить процесс обработки информации.

- Совместимость с повседневной деятельностью.

Предлагаемые планом ОНРВ действия не должны нарушать привычный режим работы. Если его действия противоречат повседневной деятельности (возможно, возобновленной после аварии), то это приведет к еще большим проблемам.

- Практическая проверка.

Все положения плана ОНРВ должны быть тщательно проверены, как теоретически, так и практически. Только в этом случае план ОНРВ будет удовлетворять перечисленным выше требованиям.

- Обеспечение.

Реальная выполнимость плана ОНРВ будет достигнута только в том случае, если предварительно подготовлено, проверено и готово к работе все вспомогательное

обеспечение — резервные копии, рабочие места, источники бесперебойного питания и т.д. Персонал должен совершенно точно знать, как и когда пользоваться этим обеспечением.

Наличие любого плана ОНРВ — полного или краткого, но главное — реального, благотворно влияет на моральную обстановку в коллективе. Пользователи должны быть уверены в том, что даже в самых неблагоприятных условиях какая-то часть их труда будет сохранена; руководство должно быть уверено, что не придется начинать все с начала.

План ОНРВ лучше всего строить как описание опасных ситуаций и способов реакции на них в следующем порядке:

- описание нарушения;
- немедленная реакция на нарушение - действия пользователей и администрации в момент обнаружения нарушения (сведение ущерба до минимума, уведомление руководства, остановка работы, восстановительные процедуры и т.д.);
- оценка ущерба от нарушения — в чем заключаются потери и какова их стоимость (включая восстановление);
- возобновление обработки информации. После устранения нарушения и первичного восстановления необходимо как можно быстрее возобновить работу, так как машинное время — это деньги;
- полное восстановление функционирования системы - удаление и замена поврежденных компонентов системы, возобновление обработки информации в полном объеме.

В части, посвященной реакции на нарушения, план ОНРВ должен содержать перечень действий, которые выполняются персоналом при наступлении различных ситуаций. Причем действия должны быть реальными, иначе в них нет никакого смысла.

Эта часть плана должна определять:

- что должно быть сделано;
- когда это должно быть сделано;
- кем и как это должно быть сделано;
- что необходимо для того, чтобы это было сделано.

При планировании подобных действий необходимо помнить об их экономической эффективности. Например, всю информацию системы в резервных копиях держать в принципе невозможно — ее слишком много и она слишком часто обновляется. В копиях должна содержаться только самая ценная информация, значимость которой уменьшается не слишком быстро. Вообще определение степени дублирования ресурсов (критичной нагрузки; critical workload) — самостоятельная и достаточно сложная задача. Она должна решаться индивидуально для конкретных условий с учетом стоимости дублирования и загрузки системы, размеров возможного ущерба, имеющихся ресурсов и других факторов.

Для определения конкретных действий по восстановлению и возобновлению процесса обработки, включаемых в план ОНРВ, может быть полезен приводимый ниже список способов организации восстановления программ и данных, а также процесса обработки информации (первый способ для восстановления программ и данных, остальные — для возобновления самого процесса обработки информации).

Способы организации восстановления работы:

Резервное копирование и внешнее хранение программ и данных. Это основной и наиболее действенный способ сохранения программного обеспечения и данных. Резервные копии делаются с наборов данных, потеря или модификация которых могут нанести значительный ущерб. Обычно в таких копиях хранятся системное программное обеспечение и наборы данных, наиболее важное прикладное программное обеспечение, а также наборы данных, являющиеся основными в данной системе (например, база данных счетов в банке).

Резервное копирование может быть полным (копии делаются со всех наборов данных), возобновляемым (копии некоторых наборов данных периодически

обновляются) и выборочным (копии делаются только с некоторых наборов данных, но потом не обновляются). Способы резервного копирования определяются для каждой конкретной АИС индивидуально с точки зрения критерия экономической эффективности.

Резервное копирование не имеет никакого, смысла, если копии могут быть уничтожены вместе с оригиналами. Поэтому копии должны храниться в надежном месте, исключающем возможность уничтожения. В тоже время, должны существовать возможность их оперативного использования. Иногда хранят две и более копий каждого набора данных. Например, одна копия может храниться в сейфе, находящемся в границах доступа персонала системы, а другая — в другом здании. В случае сбоя оборудования в системе используется первая копия (оперативно!), а в случае ее уничтожения (например, при пожаре) — вторая.

Взаимодействие служб. Услуги по возобновлению процесса обработки предоставляются по взаимной договоренности другими службами или организациями, обычно безвозмездно. Взаимопомощь бывает двух видов:

- Внешняя — другая организация предоставляет свою АИС, возможно программное обеспечение для временной обработки информации пострадавшей стороной. Такой способ возобновления процесса обработки информации может использоваться для обработки небольших объемов некритичной информации. При этом желательно, чтобы две организации были примерно одного типа и работали в одной области.

- Внутренняя — возможность обработки информации предоставляется другими подразделениями одной и той же организации (департаментами, отделами, группами).

Такой способ обычно не требует больших затрат и легко доступен, если дублирующая АИС позволяет проводить такого рода обработку.

Любой план хорош в том случае, если он выполним. Для обеспечения выполнимости планов необходимо чтобы работу по их составлению выполняла группа квалифицированных специалистов, размеры которой зависят от характера организации и масштабов предполагаемых мер защиты. Оптимальная численность группы 5-7 человек. Можно привлечь дополнительных сотрудников для обработки и анализа выводов и рекомендаций основной группы, или, в случае больших объемов работы, каждая группа должна составлять один план или один из пунктов плана.

Специализация сотрудников, входящих в группу разработки планов, зависит от конкретных условий. Использование защищенных протоколов, механизмов защиты операционных систем и сетей требует привлечения системных программистов. Применение средств защиты, встраиваемых в прикладное программное обеспечение делает необходимым участие в группе проблемных программистов. Необходимость организации защиты физических устройств, организации резервных рабочих мест также требует присутствия в рабочей группе соответствующих специалистов. И, наконец, поскольку система функционирует для пользователя, то целесообразно присутствие пользователей различных категорий - для учета взгляда со стороны на удобство и эффективность предлагаемых методов и средств защиты. В большинстве случаев целесообразно, чтобы в эту группу входили следующие специалисты, каждый из которых должен отвечать за свой участок работы:

- специалисты по техническим средствам;
- системные программисты;
- проблемные программисты;
- сотрудники, отвечающие за подготовку, ввод и обработку данных;
- специалисты по защите физических устройств;
- представители пользователей.

После подготовки плана необходимо его принять и реализовать, что напрямую зависит от его четкости, корректности и ясности для сотрудников организации.

Понимание необходимости мер защиты и контроля - неременное условие

нормальной работы. Известен случай о том, как пользователь менял каждый раз 24 пароля и возвращался к первоначальному, так как система была защищена от повторного использования предыдущих 23 паролей. Если сотрудники не понимают или не согласны с предлагаемыми мерами, то они будут стараться обойти их, так как любые меры контроля предполагают увеличение сложности работы.

Другой ключевой момент — управление средствами защиты и восстановления. Надежное управление осуществимо лишь в случае понимания обслуживающим персоналом размеров возможных убытков, ясного изложения планов и выполнения персоналом своих обязанностей. Многие сотрудники, обслуживающие системы, не всегда осознают риск, связанный с обработкой информации. Только специальная предварительная подготовка персонала способствует правильной и эффективной работе средств защиты.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов.

Разработка политики и программы безопасности начинается с анализа рисков, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными угрозами.

Главные угрозы - внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе нарушений растет доля внешних атак, но основной ущерб по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить базовый уровень безопасности при минимальных интеллектуальных и разумных материальных затратах.

Существенную помощь в разработке политики безопасности может оказать британский стандарт BS 7799:1995, предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия уровня детализации. Они должны подразделяться на несколько уровней, трактующих вопросы разной степени специфичности. Важным элементом программы является разработка и поддержание в актуальном состоянии карты ИС.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение жизненного цикла ИС и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Меры процедурного уровня ориентированы на людей (а не на технические средства) и подразделяются на следующие виды; управление персоналом;

- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

Здесь также применимы объектный подход и понятие жизненного цикла. Первый позволяет разделить контролируемые сущности (территорию, аппаратуру и т.д.) на относительно независимые подобъекты, рассматривая их с разной степенью детализации и контролируя связи между ними.

Понятие жизненного цикла полезно применять не только к информационным системам, но и к сотрудникам. На этапе инициации должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности; на этапе выведения из эксплуатации следует действовать аккуратно, не допуская нанесения ущерба обиженными сотрудниками.

Информационная безопасность во многом зависит от аккуратного ведения

текущей работы, которая включает:

- поддержку пользователей; поддержку программного обеспечения; конфигурационное управление;
- резервное копирование; управление носителями;
- документирование;
- регламентные работы.

Элементом повседневной деятельности является отслеживание информации в области ИБ; как минимум, администратор безопасности должен подписаться на список рассылки по новым пробелам в защите (и своевременно знакомиться с поступающими сообщениями).

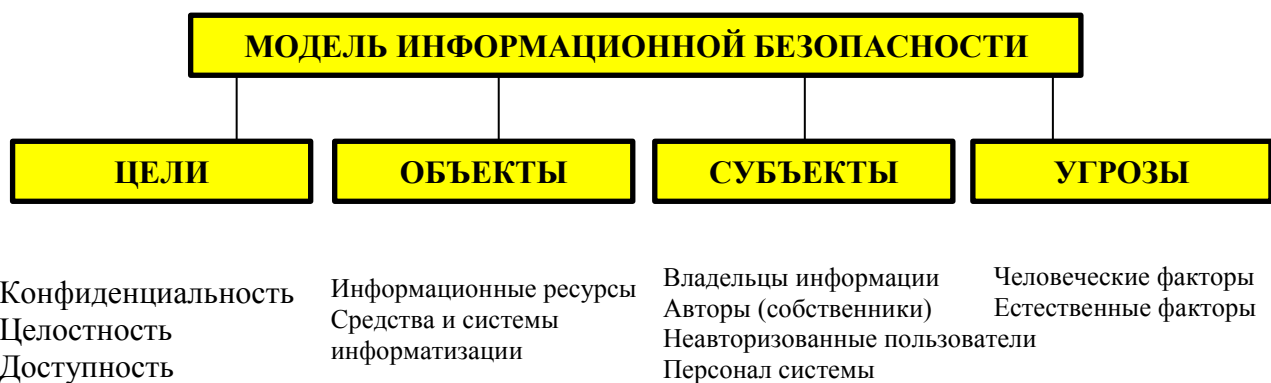
Нужно, однако, заранее готовиться к событиям неординарным, то есть к нарушениям ИБ. Заранее продуманная реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

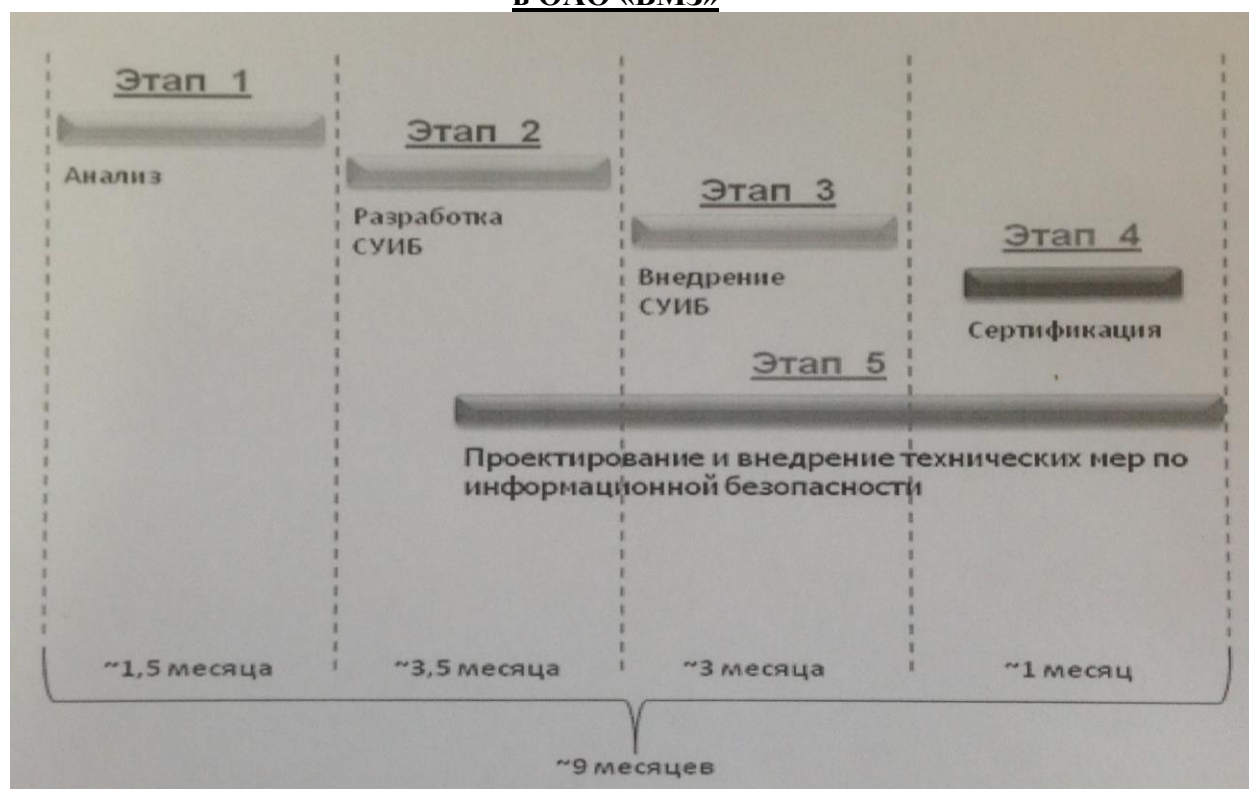
Выявление нарушителя - процесс сложный, но первый и третий пункты можно и нужно тщательно продумать и отработать.

В случае серьезных аварий необходимо проведение восстановительных работ. Процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ; подготовка к реализации выбранной стратегии;
- проверка стратегии.



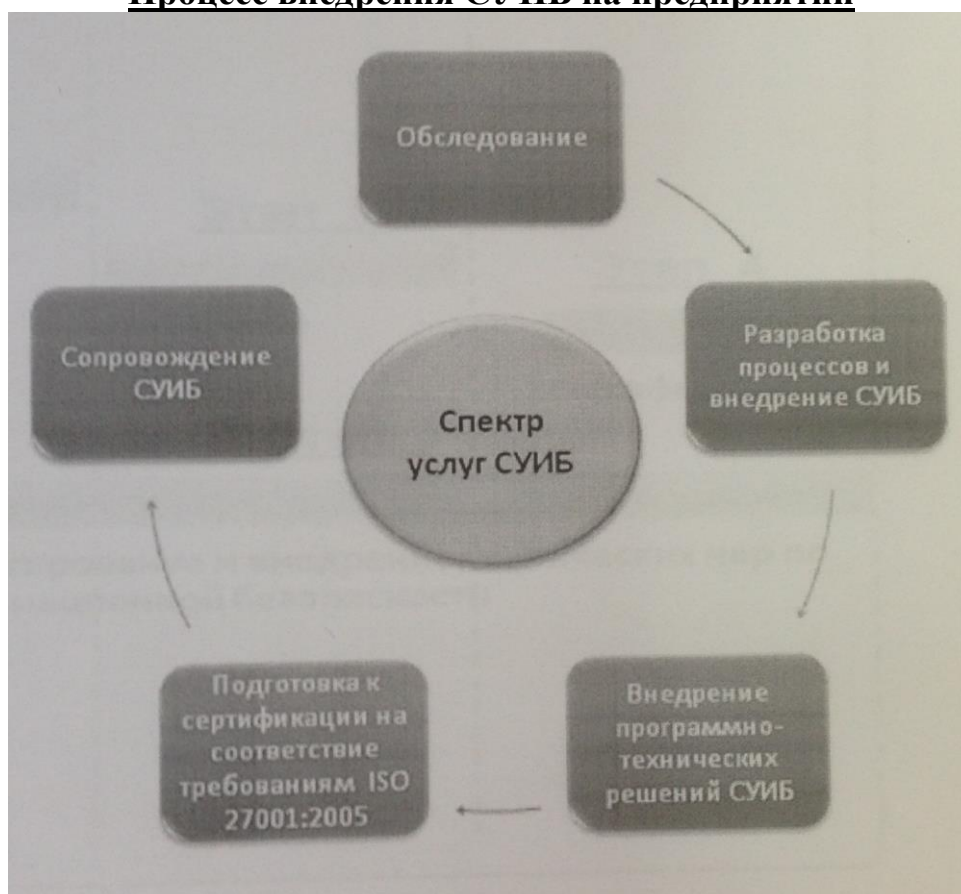
**Этапы построения системы управления информационной безопасностью
в ОАО «ВМЗ»**



Место СУИБ в организации



Процесс внедрения СУИБ на предприятии



4.3 Оценка эффективности инвестиций в информационную безопасность

Реалии современного бизнеса таковы. Что в условиях рынка практически любая компания сосредоточена на поддержании своей конкурентоспособности – не только продуктов и услуг, но и конкурентоспособности компании в целом.

В этих условиях качество и эффективность информационной системы влияют на конечные финансовые показатели опосредованно, через качество бизнес-процессов. Проигрывают те компании, где финансирование защиты информации ведется по остаточному принципу.

При этом важно ответить на вопрос: как относиться к вложениям в информационную безопасность – как к затратам или как к инвестициям? Если относиться к вложениям в ИБ как к затратам, то сокращение этих затрат является важной для компании проблемой. Однако это заметно отдалит компанию от решения стратегической задачи, связанной с повышением ее адаптивности к рынку, где безопасность в целом и ИБ в частности играет далеко не последнюю роль. Поэтому, если у компании есть долгосрочная стратегия развития, она, как правило, рассматривает вложения в ИБ как инвестиции. Разница в том, что затраты – это, в первую очередь, «осознанная необходимость», инвестиции – это перспектива окупаемости. И в этом случае требуется тщательная оценка эффективности таких инвестиций и экономическое обоснование планируемых затрат.

Основным экономическим эффектом, к которому стремится компания, создавая систему защиты информации (СЗИ), является существенное уменьшение материального ущерба вследствие реализации существующих угроз информационной безопасности.

Отдача от таких инвестиций в развитие компании должна быть вполне прогнозируемой.

В основе большинства методов оценки эффективности вложений в информационную безопасность лежит сопоставление затрат, требуемых на создание СЗИ, и ущерба, который может быть причинен компании из-за отсутствия этой системы.

ROI – это процентное отношение прибыли (или экономического эффекта) от проекта к инвестициям, необходимым для реализации этого проекта. При принятии решения об инвестициях полученное значение сравнивают со средним в отрасли либо выбирают проект с лучшим значением ROI из имеющихся вариантов. Несмотря на длительный опыт применения этого показателя в ИТ, на сегодняшний день достоверных методов расчета ROI не появилось, а попытки определить его путем анализа показателей деятельности компаний, внедривших у себя те или иные информационные технологии, привели к появлению показателя TCO, предложенного компанией Gartner Group в конце 80-х годов.

В основу общей модели расчета **TCO** положено разделение всех затрат на две категории: прямые и косвенные. Под косвенными затратами, как правило, понимаются скрытые расходы, которые возникают в процессе эксплуатации СЗИ. Эти незапланированные расходы могут существенно превысить стоимость самой системы защиты. По данным той же Gartner Group, прямые затраты составляют 15-21 % от общей суммы затрат на использование ИТ.

Одним из ключевых преимуществ показателя TCO является то, что он позволяет сделать выводы о целесообразности реализации проекта в области ИБ на основании оценки одних лишь только затрат. Тем более, что в случае с защитой информации нередко возникает ситуация, когда экономический эффект от внедрения СЗИ оценить нельзя, но объективная необходимость в ее создании существует.

Другим преимуществом этого показателя является то, что модель расчета TCO предполагает оценку не только первоначальных затрат на создание СЗИ, но и затрат, которые могут иметь место на различных этапах всего жизненного цикла системы. Но,

несмотря на это, показатель ТСО, впрочем, как и ROI, является статичным, отражающим некий временной срез – «фотографический снимок», не учитывая изменения ситуации во времени. Ведь информационные системы с течением времени подвергаются постоянным изменениям, появляются новые угрозы и уязвимости. Таким образом, обеспечение ИБ – это процесс, который необходимо рассматривать именно во времени. Поэтому для анализа эффективности инвестиций в ИБ предлагается рассмотреть возможность применения системы динамических показателей, основанных на методе дисконтированных потоков денежных средств (**Discounted Cash Flows – DCF**).

Целью любых инвестиций является увеличение притока денежных средств (в данном случае – уменьшение размера ущерба в результате реализации угроз ИБ) по сравнению с существующим. При оценке инвестиционного проекта необходимо рассмотреть все потоки денежных средств, связанные с реализацией данного проекта. При этом необходимо учитывать зависимость потока денежных средств от времени. Ведь очевидно, что за получение через год экономического эффекта, например, в размере 50 тыс. рублей сегодня инвесторы будут готовы заплатить существенно меньшую сумму, а никак не эти же 50 тыс. рублей.

Поэтому будущие поступления денежных средств (снижение ущерба) должны быть дисконтированы, то есть приведены к текущей стоимости. Для этого применяют ставку дисконтирования, величина которой отражает риски, связанные с обесцениванием денег из-за инфляции и с возможностью неудачи инвестиционного проекта, который может не принести ожидаемого эффекта. Другими словами, чем выше риски, связанные с проектом, тем больше значение ставки дисконтирования. Эта ставка также отражает общий уровень стоимости кредита для инвестиций.

Нередко ставка дисконтирования определяется показателем средневзвешенной стоимости капитала (**Weighted Average Cost of Capital – WACC**). Это средняя норма дохода на вложенный капитал, которую приходится выплачивать за его использование. Обычно WACC рассматривается как минимальная норма отдачи, которая должна быть обеспечена инвестиционным проектом.

Непосредственно для оценки эффективности инвестиций используют показатель чистой текущей стоимости (**Net Present Value – NPV**). По сути, это текущая стоимость будущих денежных потоков инвестиционного проекта с учетом дисконтирования и за вычетом инвестиций. Этот показатель рассчитывается по следующей формуле:

$$NP = \frac{CF_i}{(1+r)^n} - CF_0 \quad (1)$$

где CF_i – чистый денежный поток для i -го периода\$

CF_0 – начальные инвестиции\$

n – ставка дисконтирования (стоимость капитала, привлеченного для инвестиционного проекта).

При значении NPV большем или равном нулю, считается, что вложение капитала эффективно. При сравнении нескольких проектов принимается тот из них, который имеет большее значение NPV, если только оно положительное.

Предположим, некой компании требуется оценить проект по защите одного из сегментов сети своей информационной системы при помощи системы обнаружения вторжений (IDS). Допустим, известна величина риска, исчисляемая в денежном выражении (20000 долл. за год), которая учитывает потери от реализации тех или иных атак и вероятности их осуществления. Также известно, что величина риска после внедрения IDS сократится на 70%. Стоимость IDS составляет 15000 долл. Ставку дисконтирования возьмем среднюю для ИТ рынка – 30 %. Подробнее потоки денежных средств по данному проекту представлены в таблице 6.

Таблица 6

Периоды	Первонач. инвестиции	Выгоды (размер риска)	Размер остаточного риска	Стоимость годовой поддержки	Затраты на администрирование и инфраструктуру	Итог
0	-15000,0					-15000,0
1		20000,0	-6000,0	-2000,0	-5400,0	6600,0
2		20000,0	-6000,0	-2000,0	-5400,0	6600,0
3		20000,0	-6000,0	-2000,0	-5400,0	6600,0

Если на основе данных, представленных в таблице 6, рассчитать показатель ROI, то получится, что внедрение IDS в данном случае даст экономический эффект, на 39% превышающий вложения. При анализе этого проекта с учетом стоимости капитала мы имеем следующий результат, инвестирование в этот проект не будет эффективным, так как значение NPV будет отрицательным (3014).

Кроме того, можно рассчитать внутренний коэффициент отдачи (**Internal Rate of Return – IRR**). Для этого необходимо найти такую ставку дисконтирования, при которой значение NPV будет равно нулю. В данном случае получим значение IRR равное 15%. Это значение имеет конкретный экономический смысл дисконтированной точки безубыточности. В этой точке дисконтированный поток затрат равен дисконтированному потоку доходов. Данный показатель также позволяет определить целесообразность вложения средств.

В рассматриваемом примере инвестиции в проект нецелесообразны, так как мы получили значение IRR меньше заданной ставки дисконтирования (30%).

Очевидно, что для оценки эффективности инвестиций в создание СЗИ недостаточно лишь определения показателей. Необходимо еще учесть риски, связанные с реализацией того или иного проекта. Это могут быть риски, связанные с конкретными поставщиками средств защиты информации, или риски, связанные с компетентностью и опытом команды внедрения.

Кроме того, полезно проводить анализ чувствительности полученных показателей. Например, в рассмотренном примере увеличение исходного значения риска всего на 12% приведет к получению положительного значения NPV и увеличению ROI на 8%. А если учесть, что риск – это вероятностная величина, то погрешность в 12% вполне допустима. Так же можно проанализировать чувствительность полученных результатов и к другим исходным данным, например к затратам на администрирование.

Не следует забывать и о том, что далеко не весь ущерб от реализации угроз ИБ можно однозначно выразить в денежном исчислении. Например, причинение урона интеллектуальной собственности компании может привести к таким последствиям, как потеря позиций на рынке, потеря постоянных и временных конкурентных преимуществ или снижение стоимости торговой марки. Поэтому нередко даже при наличии рассчитанных показателей ROI и ТСО решение о создании СЗИ принимается на основе качественной оценки возможных эффектов.

Любой метод оценки эффективности инвестиций в ИБ является всего лишь набором математических формул и логических выкладок, корректность применения которых – только вопрос обоснования. Поэтому качество информации, необходимой для принятия решения о целесообразности инвестиций, в первую очередь, будет зависеть от исходных данных, на основе которых производились вычисления. Уязвимым местом в любой методике расчета является именно сбор и обработка первичных данных, их качество и достоверность.

Кроме того, четкое понимание целей, ради которых создается СЗИ, и непосредственное участие постановщика этих целей в процессе принятия решений также является залогом высокого качества и точности оценки эффективности инвестиций в ИБ. Такой подход гарантирует, что система защиты информации не будет являться

искусственным дополнением к уже внедренной системе управления, а будет изначально спроектирована как важнейший элемент, поддерживающий основные бизнес-процессы компании.

Обеспечение безопасности должностных лиц и представителей деловых кругов⁹

Некоторые общие меры предосторожности:

1. Будьте бдительны.
2. Наблюдайте за празднующими, торговцами и хулиганами.
3. Не носите дорогих украшений.
4. Определяйте воров-карманников.
5. Не стойте в хвосте автобуса.
6. Будьте внимательны в метро.
7. Избегайте такси.
8. Толпа всегда опасна.
9. Не рекламируйте свою национальность.
10. Избегайте скопления туристов.
11. Пользуйтесь многолюдными улицами
12. Гуляйте в парке.
13. Всегда имейте при себе медицинскую карту.

Определение наличия наблюдения:

1. Определение «хвоста».
2. «Хвосты» работают посменно.
3. Постоянные атрибуты и приметы.

Контрмеры

1. Сначала увеличьте скорость, затем сбавьте.
2. Отойдите в сторону и осмотритесь.
3. Останавливайтесь у витрин магазинов.
4. Войдите в здание и резко остановитесь.

Уклонение от преследования

1. Если вы женщина, подойдете и укажете на человека, которого вы подозреваете.
2. Если вы женщина, а ваш «хвост» - мужчина, постарайтесь, чтобы он потерял вас в магазине для женщин или в туалете.
3. Измените свою внешность.

Самозащита без оружия

⁹ Методика информационной безопасности. – М.: Издательство «Экзамен», 2004. Авторы: Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А., Жогла Н.Л., Зайцев О.А., Курбатов Г.Л., Петренко А.И., Федотов Н.В.

Использование импровизированного оружия

Поездка за границу

1. Никогда не теряйте ваш паспорт из виду

Путешествие самолетом

1. Летайте экономическим классом.
2. Не одевайтесь слишком вычурно.
3. Избегайте страны, где террористы пользуются режимом наибольшего благоприятствования.
4. Храните в секрете цель вашей поездки.
5. Имейте в своей ручной клади необходимые медикаменты.
6. Не злоупотребляйте алкогольными напитками.

Проживание в гостиницах

Другие советы

1. Знайте культуру и обычаи страны пребывания.
2. Знайте, как, когда и с кем шутить.
3. Не будьте склочными и задиристыми.

Обеспечение безопасности во время поездок на автомобиле

Меры по обеспечению безопасности бизнеса

Получение корпоративной информации

1. Контрразведывательные операции.
2. Оценка риска пребывания и деятельности компании в конкретной стране.

Уязвимые места

1. Обман и угрозы.
2. Саботаж и диверсии
3. Промышленный шпионаж
4. Нападение на сотрудников компании.
5. Порча изделий и продукции может иметь самые серьёзные негативные последствия для компании.

Служба безопасности

1. Нанимайте на работу людей, серьезно относящихся к делу.
2. Требуйте, чтобы сотрудники службы безопасности были тактичны и вежливы.

3. Проинформируйте сотрудников, с какой целью предпринимаются те или иные меры предосторожности.
4. Проследуйте за тем, что все сотрудники службы безопасности имели хорошую профессиональную подготовку.
5. Рутинная и скучная – враги хорошей службы безопасности.
6. Дайте почувствовать сотрудникам службы безопасности, что их работа важна.
7. Регулярно интересуйтесь мнением сотрудников службы безопасности.

Охрана территории

Освещение

Системы сигнализации и замки

Сотрудники

1. Проверяйте всех сотрудников, включая руководство компании.
2. Использование детектора лжи.
3. Обучайте сотрудников своей компании элементам безопасности.
4. Увольняйте сотрудников, которые нарушают правила безопасности.

Обеспечение внутренней безопасности

1. Защищенные файлы.
2. Проводите политику «чистых столов».
3. Компьютеры

Выбор телохранителей

1. Больше не всегда означает лучше.
2. Опыт
3. Инициативные и думающие телохранители
4. Контактность, предусмотрительность, ответственность и благоразумие.
5. Физическое состояние
6. Круглосуточное обеспечение безопасности
7. Медицинская подготовка
8. Школы обучения мерам по обеспечению безопасности.

Глава 5 Информационная безопасность отдельных экономических систем

5.1 Обеспечение информационной безопасности автоматизированных банковских систем (АБС)

Банки играют огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Благодаря своей специфической роли, со времени своего появления они всегда притягивали преступников. К 90-м годам XX века банки перешли к компьютерной обработке информации, что значительно повысило производительность труда, ускорило расчеты и привело к появлению новых услуг. Однако компьютерные системы, без которых в настоящее время не может обойтись ни один банк, являются также источником совершенно новых угроз, неизвестных ранее. Большинство из них обусловлены новыми информационными технологиями и не являются специфическими исключительно для банков.

В условиях финансовых кризисов первоочередное внимание в работе банков уделяется вопросам, влияющим на повышение их конкурентоспособности, одним из важнейших аспектов этой проблемы является повышение уровня безопасности операций, выполняемых банком. При современных технологиях автоматизации увеличивается объем информации, обрабатываемой в электронном виде, что ведет к снижению общего уровня безопасности в работе банка. Решение этой проблемы во многом зависит от технологий, используемых конкретным банком, иными словами – от автоматизированной банковской системы.

Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений шел не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связано с использованием автоматизированных систем обработки информации банка. Следовательно, при создании и модернизации АБС необходимо уделять пристальное внимание обеспечению ее безопасности.

Именно эта проблема является сейчас наиболее актуальной и наименее исследованной. Если в обеспечении физической и классической информационной безопасности давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то в связи с частыми радикальными изменениями в компьютерных технологиях методы безопасности АБС требуют постоянного обновления. Как показывает практика, не существует сложных компьютерных систем, не содержащих ошибок. А поскольку идеология построения крупных АБС регулярно меняется, то исправления найденных ошибок и «дыр» в системах безопасности хватает ненадолго, так как новая компьютерная система приносит новые проблемы и новые ошибки, заставляет по-новому перестраивать систему безопасности.

Во многие банковские системы заложена идеология и схема бизнес-процессов многофилиального банка, имеющего, в том числе, структурные подразделения в различных регионах. Возможность работы в режиме удаленного доступа предъявляет дополнительные требования к защитным механизмам. А высокая степень интегрированности информации в комбинации с уникальными возможностями адаптации системы к самым разным сетевым операционным системам делает проблему информационной безопасности банка чрезвычайно актуальной.

Безопасность информации напрямую влияет на уровень рентабельности, ибо потери, связанные с ее нарушением, могут свести на нет все достижения эффективного управления. При этом, как правило, чем более совершенна система управления банком, тем опаснее утечки информации.

Современные АБС – это сложные, структурированные, территориально распределенные сети. Как правило, они строятся на основе передовых технологий и программных средств, которые в силу своей универсальности не обладают достаточной защищенностью.

Особенно актуальна данная проблема в России. В западных банках программное обеспечение (ПО) разрабатывается конкретно под каждый банк, и устройство АБС во многом является коммерческой тайной. В России получили распространение «стандартные» банковские пакеты, информация о которых широко известна, что облегчает несанкционированный доступ в банковские компьютерные системы. Причем, во-первых, надежность «стандартного» ПО ниже из-за того, что разработчик не всегда хорошо представляет конкретные условия, в которых этому ПО придется работать, а, во-вторых, некоторые российские банковские пакеты не удовлетворяли условиям безопасности. Например, ранние версии самого популярного российского банковского пакета требовали наличия дисководов у персонального компьютера и использовали ключевую дискету как инструмент обеспечения безопасности. Такое решение. Во-первых, технически ненадежно, а, во-вторых, одно из требований безопасности АБС – закрытие дисководов и портов ввода-вывода в компьютерах сотрудников, не работающих с внешними данными.

Доступность средств вычислительной техники привела к распространению компьютерной грамотности в широких слоях населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих, в частности банковских, систем, как со злым умыслом, так и из чисто «спортивного интереса». Многие из этих попыток имели успех и нанесли значительный урон владельцам информации и вычислительных систем.

Современный банк трудно представить себе без автоматизированной информационной системы. Компьютер на столе банковского служащего давно превратился в привычный и необходимый инструмент. Связь компьютеров между собой и более мощными компьютерами, а также с ЭВМ других банков – также необходимое условия успешной деятельности банка – слишком велико количество операций, которые необходимо выполнять в течение короткого периода времени.

Уровень оснащенности средствами автоматизации играет немаловажную роль в деятельности банка и, следовательно, напрямую отражается на его положении и доходах. Усиление конкуренции между банками приводит к необходимости сокращения времени на производство расчетов, увеличения номенклатуры и повышения качества предоставляемых услуг.

Чем меньше времени будут занимать расчеты между банком и клиентом. Тем выше станет оборот банка и, следовательно, прибыль. Кроме того. Банк более оперативно сможет реагировать на изменение финансовой ситуации. Разнообразие услуг банка (в первую очередь это относится к возможности безналичных расчетов между банком и его клиентами с использованием пластиковых карт) может существенно увеличить число его клиентов и, как следствие, повысит прибыль.

В то же время АБС становится одним из наиболее уязвимых мест во всей организации, притягивающим злоумышленников как извне, так и из числа сотрудников самого банка. Для подтверждения этого тезиса можно привести несколько фактов:

Потери банков и других финансовых организаций от воздействия на их системы обработки информации составляют около \$ 3 млрд. в год.

Объем потерь, связанных с использованием пластиковых карточек, оценивается в \$ 2 млрд. в год, что составляет 0,03-2% от общего объема платежей в зависимости от используемой системы.

Средняя величина ущерба от банковской кражи с применением электронных средств составляет около \$ 9000.

Один из самых громких скандалов связан с попыткой семерых человек украсть \$ 700 млн. в первом национальном банке, Чикаго. Она была предотвращена ФБР.

27 млн. фунтов стерлингов были украдены из Лондонского отделения Union Bank of Switzerland.

DM 5 млн. украдены из Chase Bank (Франкфурт). Служащий перевел деньги в банк Гонконга – они были взяты с большого количества счетов (атака «салями»). Кража оказалась успешной.

\$ 3 млн. – банк Стокгольма. Кража была совершена с использованием привилегированного положения нескольких служащих в информационной системе банка и также оказалась успешной.

Чтобы обезопасить себя и своих клиентов, большинство банков предпринимают необходимые меры защиты, в числе которых защита АБС занимает не последнее место. При этом необходимо учитывать, что защита АБС – дорогостоящее и сложное мероприятие. Так, например, Barclays Bank тратит на защиту своей автоматизированной системы около \$ 20 млн. ежегодно.

Datapro Information Services Group провела почтовый опрос среди случайно выбранных менеджеров информационных систем. Целью опроса явилось выяснение состояния дел в области защиты. Было получено 1153 анкеты, на основе которых получены приводимые ниже результаты:

- около 25% всех нарушений составляют стихийные бедствия; около половины систем испытывали внезапные перерывы электропитания или связи, причины которых носили искусственный характер;

- около 3% систем испытывали внешние нарушения (проникновение в систему организации);

- 70-75% – внутренние нарушения, из них:

 - 10% совершены обиженными и недовольными служащими-пользователями АБС банка;

 - 10% – совершены из корыстных побуждений персоналом системы;

 - 50-55% – результат неумышленных ошибок персонала и/или пользователей системы в результате небрежности, халатности или некомпетентности.

Эти данные свидетельствуют о том, что чаще всего происходят не такие нарушения, как нападения хакеров или кража компьютеров с ценной информацией, а самые обыкновенные, проистекающие из повседневной деятельности. В то же время именно умышленные атаки на компьютерные системы приносят наибольший единовременный ущерб, а меры защиты о них наиболее сложны и дорогостоящи. В этой связи проблема оптимизации защиты АБС является наиболее актуальной в сфере информационной безопасности банков.

Встроенные механизмы разграничения доступа в сетевых ОС при систематическом администрировании и строгом разграничении доступа к информационным ресурсам (что бывает далеко не всегда) позволяют достаточно надежно защитить данные, хранимые на серверах. Практически все операционные системы содержат минимальный набор защитных механизмов и для локальных рабочих мест.

Классические угрозы безопасности информации в АБС – это вывод системы из строя, отказ в обслуживании и компрометация или подмена данных. И эти угрозы слишком реальны.

По сведениям Национального центра данных о преступности, связанной с

ЭВМ (Лос-Анджелес, США), компьютерные правонарушения наиболее часто совершаются программистами, студентами и операторами ввода исходных данных. В табл.7 указаны основные типы и субъекты угроз для компьютерных систем.

Таблица 7

Типы и субъекты угроз

Тип угрозы	Оператор	Руководитель	Программист	Инженер (техник)	Пользователь	Конкурент
Изменение кодов	+		+			
Копирование файлов	+		+			
Уничтожение файлов	+	+	+		+	+
Присвоение программ			+	+		+
Шпионаж	+	+	+			+
Установка подслушивания			+	+		+
Саботаж	+		+	+		+
Продажа данных	+	+	+		+	
Воровство		+	+		+	+

Субъектов компьютерных преступлений с точки зрения профессиональной подготовленности принято подразделять на лиц, совершающих преступления:

- а) «нетехнические»; б) «технические», требующие минимума специальных знаний;
- в) «высокотехнические», возможные при условии основательного владения вычислительной техникой.

Практика показывает, что большинство преступлений категории «а» совершают малознакомые с вычислительной техникой служащие со средним образованием. Однако этих людей отличают два качества: они имеют доступ к компьютеру и знают, какие функции выполняет он в их организации. «Нетехнические» преступления совершаются главным образом путем кражи пароля доступа к файлам информации, хранящейся в машинной памяти. Владея паролем и определенными навыками, можно войти в засекреченные файлы, изменить их содержание и т.п. Эти преступления довольно просты для расследования, и, усилив защиту системы, их легко предупредить.

«Технические» преступления связаны с манипуляциями программами, которые составлены специалистами. Изменить их могут лишь лица, имеющие соответствующую квалификацию. Наибольшую трудность для правоохранительных органов представляют «высокотехнические» преступления.

Субъекты, совершившие несанкционированный доступ к информации, называются нарушителями. С точки зрения защиты информации несанкционированный доступ может иметь следующие последствия: утечка обрабатываемой конфиденциальной информации, а также ее искажение или разрушение в результате умышленного нарушения работоспособности АБС.

Нарушителем может быть любой человек из следующих категорий сотрудников:

штатные пользователи АБС; сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение системы; обслуживающий персонал (инженеры);

другие сотрудники, имеющие санкционированный доступ к АИТ (в том числе подсобные рабочие, уборщицы и т.д.).

Доступ к АБС других лиц (посторонних, не принадлежащих к указанным категориям) исключается организационно-режимными мерами.

Под каналом несанкционированного доступа к информации понимается последовательность действий лиц и выполняемых ими технологических процедур, которые либо выполняются несанкционированно, либо обрабатываются неправильно в результате ошибок персонала или сбоя оборудования, что приводит в конечном итоге к факту несанкционированного доступа.

Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким с целью удобства для клиентов.

Обычная компания строит свою информационную безопасность, исходя лишь из узкого круга потенциальных угроз – главным образом защита информации от конкурентов (в российских реалиях основной задачей является защита информации от налоговых органов и преступного сообщества с целью уменьшения вероятности неконтролируемого выплат налоговых выплат и рэкета). Такая информация интересна лишь узкому кругу заинтересованных лиц и организаций и редко бывает ликвидна, т.е. обращается в денежную форму.

Информационная безопасность банка должна учитывать следующие специфические факторы:

Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д. Вполне понятно, что незаконное манипулирование с такой информацией может привести к серьезным убыткам. Эта особенность резко расширяет круг преступников, покушающихся именно на банки (в отличие от, например, промышленных компаний, внутренняя информация которых мало кому интересна).

Информация в банковских системах затрагивает интересы большого количества физических и юридических лиц – клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом. Поэтому клиент должен иметь возможность быстро и без томительных процедур распоряжаться своими деньгами. Но такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов.

Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

- силу этих обстоятельств к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации.

- США, странах Западной Европы и многих других, столкнувшихся с этой проблемой довольно давно, в настоящее время создана целая индустрия защиты экономической информации, включающая разработку и производство безопасного аппаратного и программного обеспечения, периферийных устройств, научные изыскания и др.

Сфера информационной безопасности – наиболее динамичная область развития индустрии безопасности в целом. Если обеспечение физической безопасности имеет давнюю традицию и устоявшиеся подходы, то информационная безопасность постоянно требует новых решений, т.к. компьютерные и телекоммуникационные технологии постоянно обновляются, на компьютерные системы возлагается все большая ответственность.

Под безопасностью АБС будем понимать ее свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Иными словами под безопасностью системы понимается защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Следует отметить, что природа воздействия может быть самой различной. Это и попытки проникновения злоумышленника, и ошибки персонала, и стихийные бедствия (ураган, пожар), и выход из строя составных частей АБС.

Безопасность АБС достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

Конфиденциальность информации – это свойство информации быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы. (пользователям, программам, процессам и т.д.). Для остальных субъектов системы эта информация как бы не существует.

Целостность компонента (ресурса) системы – свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.

Доступность компонента (ресурса) системы – свойство компонента (ресурса) быть доступным для использования авторизованными субъектами системы в любое время.

Обеспечение безопасности АБС требует применения различных мер защитного характера. Обычно вопрос о необходимости защиты компьютерной системы не вызывает сомнений. Наиболее трудными бывают ответы на вопросы:

- От чего надо защищать систему?
- Что надо защищать в самой системе?
- Как надо защищать систему (при помощи каких методов и средств)?
- При выработке подходов к решению проблемы безопасности следует всегда исходить из того, что конечной целью применения любых мер противодействия угрозам является защиты владельца и законных пользователей АБС от нанесения им материального или морального ущерба в результате случайных ил преднамеренных воздействий на нее.

Помимо обеспечения безопасности работы с персональными компьютерами, необходимо разработать более широкую, комплексную программу компьютерной безопасности, которая должна обеспечить сохранность электронных данных во всех файлах банка. Она может включать следующие основные этапы реализации:

защита информации от несанкционированного доступа;

защита информации в системах связи; защита юридической значимости электронных документов;
защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
защита от несанкционированного копирования и распространения программ
• ценной компьютерной информации. Для каждого направления определяются основные цели и задачи.

Под несанкционированным доступом понимается нарушение установленных правил разграничения доступа, последовавшее в результате случайных или преднамеренных действий пользователей или других субъектов системы разграничения, являющейся составной частью системы защиты информации.

Обеспечение безопасности АБС в целом предполагает создание препятствия для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов. То есть защиту всех компонентов системы: оборудования, программного обеспечения, данных и персонала. В этом смысле защита информации от несанкционированного доступа является только частью общей проблемы обеспечения безопасности АБС, а борьбу следует вести не только с «несанкционированным доступом» (к информации), а шире – с «несанкционированными действиями».

Выявление всего множества каналов несанкционированного доступа проводится в ходе проектирования путем анализа технологии хранения, передачи и обработки информации, определенного порядка проведения работ, разработанной системы защиты информации и выбранной модели нарушителя.

Защита конфиденциальной и ценной информации от несанкционированного доступа и модификации призвана обеспечить решение одной из наиболее важных задач: защиту имущественных прав владельцев и пользователей компьютеров, защиту собственности, воплощенную в обрабатываемой информации, от всевозможных вторжений и хищений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб.

Центральной в проблеме защиты информации от несанкционированного доступа является задача разграничения функциональных полномочий и доступа к информации, направленная на предотвращение не только возможности потенциального нарушителя «читать» хранящуюся в ПЭВМ информацию, но и возможности нарушителя модифицировать ее штатными и нештатными средствами.

Требования по защите информации от несанкционированного доступа направлены на достижение (в определенном сочетании) трех основных свойств защищаемой информации:

конфиденциальность (засекреченная информация должна быть доступна только тому, кому она предназначена);

целостность (информация, на основе которой принимаются важные решения, должна быть достоверной и точной и должна быть защищена от возможных непреднамеренных и злоумышленных искажений);

готовность (информация и соответствующие информационные службы должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость).

В основе контроля доступа к данным лежит система разграничения доступа между пользователями АБС и информацией, обрабатываемой системой. Для успешного функционирования любой системы разграничения доступа необходимо решение двух задач.

1. Сделать невозможным обход системы разграничения доступа действиями,

находящимися в рамках выбранной модели:

2. Гарантировать идентификацию пользователя, осуществляющего доступ к данным (аутентификация пользователя).

Одним из эффективных методов увеличения безопасности АБС является регистрация. Система регистрации и учета, ответственная за ведение регистрационного журнала, позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В регистрационном журнале фиксируются все осуществленные или неосуществленные попытки доступа к данным или программам. Содержание регистрационного журнала может анализироваться как периодически, так

- непрерывно.

- регистрационном журнале ведется список всех контролируемых запросов, осуществляемых пользователями системы.

Система регистрации и учета осуществляет:

регистрацию входа (выхода) субъектов доступа в систему (из системы) либо регистрацию загрузки и инициализации операционной системы и ее программного останова (регистрация выхода из системы или останова не проводится в моменты аппаратного отключения АИТ), причем в параметрах регистрации указываются: время

- дата входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы; результат попытки входа – успешный или неуспешный (при попытке несанкционированного доступа), идентификатор (код или фамилия) субъекта, предъявляемый при попытке доступа;

регистрацию и учет выдачи печатных (графических) документов на твердую копию;

регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

учет всех защищаемых носителей информации с помощью их любой маркировки (учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи / приема, должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации).

Защита информации в системах связи направлена на предотвращение возможности несанкционированного доступа к конфиденциальной и ценной информации, циркулирующей по каналам связи различных видов. В своей основе данный вид защиты преследует достижение тех же целей: обеспечение конфиденциальности и целостности информации. Наиболее эффективным средством защиты информации в неконтролируемых каналах связи является применение криптографии и специальных связных протоколов.

Защита юридической значимости электронных документов оказывается необходимой при использовании систем и сетей для обработки, хранения и передачи информационных объектов, содержащих в себе приказы, платежные поручения, контракты и другие распорядительные, договорные, финансовые документы. Их общая особенность заключается в том, что в случае возникновения споров (в том числе и судебных) должна быть обеспечена возможность доказательства истинности факта того, что автор действительно фиксировал акт своего волеизъявления в отчуждаемом электронном документе. Для решения данной проблемы используются современные криптографические методы проверки подлинности информационных объектов, связанные с применением так называемых «цифровых подписей». На практике вопросы защиты значимости электронных документов решаются совместно с вопросами защиты компьютерных информационных систем.

Защита информации от утечки по каналам побочных электромагнитных излучений и наводок является важным аспектом защиты конфиденциальной и

секретной информации в ПЭВМ от несанкционированного доступа со стороны посторонних лиц. Данный вид защиты направлен на предотвращение возможности утечки информативных электромагнитных сигналов за пределы охраняемой территории. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры перехвата, регистрации и отображения электромагнитных сигналов. Для защиты от побочных электромагнитных излучений и наводок широко применяется экранирование помещений, предназначенных для размещения средств вычислительной техники, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования (ПЭВМ и средств связи).

В некоторых ответственных случаях может быть необходима дополнительная проверка вычислительного оборудования на предмет возможного выявления специальных закладных устройств финансового шпионажа, которые могут быть внедрены с целью регистрации или записи информативных излучений компьютера, а также речевых и других, несущих уязвимую информацию сигналов.

Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ приобрела за последнее время особую актуальность. Масштабы реальных проявлений вирусных эпидемий оцениваются сотнями тысяч случаев заражения персональных компьютеров. Хотя некоторые из вирусных программ оказываются вполне безвредными, многие из них имеют разрушительный характер. Особенно опасны вирусы для компьютеров, входящих в состав однородных локальных вычислительных сетей. Некоторые особенности современных компьютерных информационных систем создают благоприятные условия для распространения вирусов. К ним, в частности, относятся:

необходимость совместного использования программного обеспечения многими пользователями;

трудность ограничения в использовании программ;

ненадежность существующих механизмов защиты;

разграничения доступа к информации в отношении противодействия вирусу

• т.д.

В методах защиты от вирусов существуют два направления:

Применение «иммуностойких» программных средств, защищенных от возможности несанкционированной модификации (разграничение доступа, методы самоконтроля и самовосстановления).

- Применение специальных программ-анализаторов, осуществляющих постоянный контроль возникновения отклонений в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (например, обнаружение нарушений целостности программного обеспечения), а также входной контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований).

- Защита от несанкционированного копирования и распространения программ

- ценной компьютерной информации является самостоятельным видом защиты имущественных прав, ориентированных на проблему охраны интеллектуальной собственности, воплощенной в виде программ ПЭВМ и ценных баз данных. Данная защита обычно осуществляется с помощью специальных программных средств, подвергающих защищаемые программы и базы данных предварительной обработке (вставка парольной защиты, проверок по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочей ПЭВМ по ее уникальным характеристикам и т.д.), которая приводит исполняемый код защищаемой программы и базы данных в состояние, препятствующее его выполнению на «чужих» машинах. Для повышения защищенности применяются дополнительные

аппаратные блоки (ключи), подключаемые к разъему принтера или к системной шине ПЭВМ, а также шифрование файлов, содержащих исполняемый код программы. Общим свойством средств защиты программ от несанкционированного копирования является ограниченная стойкость такой защиты, так как в конечном случае исполняемый код программы поступает на выполнение в центральный процессор в открытом виде и может быть прослежен с помощью аппаратных отладчиков. Однако это обстоятельство не снимает потребительские свойства средств защиты до нуля, так как основной целью их применения является в максимальной степени затруднить, хотя бы временно, возможность несанкционированного копирования ценной информации.

Контроль целостности программного обеспечения проводится с помощью:

- внешних средств (программ контроля целостности);
- внутренних средств (встроенных в саму программу).

Контроль целостности программ внешними средствами выполняется при старте системы и состоит в сравнении контрольных сумм отдельных блоков программ с их эталонными суммами. Контроль можно производить также при каждом запуске программы на выполнение.

Контроль целостности программ внутренними средствами выполняется при каждом запуске программы на выполнение и состоит в сравнении контрольных сумм отдельных блоков программ с их эталонными суммами. Такой контроль используется в программах для внутреннего пользования.

Одним из потенциальных каналов несанкционированного доступа к информации является несанкционированное изменение прикладных и специальных программ нарушителем с целью получения конфиденциальной информации. Эти изменения могут преследовать цель изменения правил разграничения доступа или обхода их (при внедрении в прикладные программы системы защиты) либо организацию незаметного канала получения конфиденциальной информации непосредственно из прикладных программ (при внедрении в прикладные программы). Одним из методов противодействия этому является метод контроля целостности базового программного обеспечения специальными программами. Однако этот метод недостаточен, поскольку предполагает, что программы контроля целостности не могут быть подвергнуты модификации нарушителем.

При защите коммерческой информации, как правило, используются любые существующие средства и системы защиты данных от несанкционированного доступа, однако в каждом случае следует реально оценивать важность защищаемой информации и ущерб, который может нанести ее утрата.

Чем выше уровень защиты, тем она дороже. Сокращение затрат идет в направлении стандартизации технических средств. В ряде случаев, исходя из конкретных целей и условий, рекомендуется применять типовые средства, прошедшие аттестацию, даже если они уступают по некоторым параметрам.

Защита информации может обеспечиваться разными методами, но наибольшей надежностью и эффективностью обладают (а для каналов связи являются единственно целесообразными) системы и средства, построенные на базе криптографических методов. В случае использования некриптографических методов большую сложность составляет доказательство достаточности реализованных мер и обоснование надежности системы защиты от несанкционированного доступа.

Необходимо иметь в виду, что подлежащие защите сведения могут быть получены «противником» не только за счет осуществления «проникновения» к ЭВМ, которые с достаточной степенью надежности могут быть предотвращены (например, все данные хранятся только в зашифрованном виде), но и за счет побочных электромагнитных излучений и наводок на цепи питания и заземления ЭВМ, а также каналы связи. Все без исключения электронные устройства, блоки и узлы ЭВМ излучают подобные сигналы, которые могут быть достаточно мощными и могут

распространяться на расстояния от нескольких метров до нескольких километров. При этом наибольшую опасность представляет собой получение «противником» информации о ключах. Восстановив ключ, можно предпринять ряд успешных действий по завладению зашифрованными данными, которые, как правило, охраняются менее тщательно, чем соответствующая открытая информация. С этой точки зрения выгодно отличаются именно аппаратные и программно-аппаратные средства защиты от несанкционированного доступа, для которых побочные сигналы о ключевой информации существенно ниже, чем для чисто программных реализаций.

Основной вывод, который можно сделать из анализа развития банковской отрасли, заключается в том, что компьютеризация банковской деятельности продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный уход на безналичные расчеты с использованием пластиковых карт, сети Internet и удаленных терминалов управления счетом юридических лиц.

В связи с этим следует ожидать дальнейшее динамичное развитие средств информационной безопасности банков, поскольку их значение постоянно возрастает.

5.2 Информационная безопасность электронной коммерции (ЭК)

Количество пользователей Интернета достигло несколько сот миллионов и появилось новое качество в виде «виртуальной экономики». В ней покупки совершаются через торговые сайты, с использованием новых моделей ведения бизнеса, своей стратегией маркетинга и пр.

Электронная коммерция (ЭК) – это предпринимательская деятельность по продаже товаров через Интернет. Как правило выделяются две формы ЭК:

- торговля между предприятиями (business to business, B2B);
- торговля между предприятиями и физическими лицами, т.е. потребителями (business to consumer, B2C).

ЭК породила такие новые понятия как:

- Электронный магазин – витрина и торговые системы, которые используются производителями или дилерами при наличии спроса на товары.
- Электронный каталог – с большим ассортиментом товаров от различных производителей.
- Электронный аукцион – аналог классического аукциона с использованием Интернет-технологий, с характерной привязкой к мультимедийному интерфейсу, каналу доступа в Интернет и показом особенностей товара.
- Электронный универмаг – аналог обычного универмага, где обычные фирмы выставляют свой товар, с эффективным товарным брендом (Гостиный двор, ГУМ и т.д.).
- Виртуальные комьюнити (сообщества), в которых покупатели организуются по группам интересов (клубы болельщиков, ассоциации и т.д.).

Интернет в области ЭК приносит существенные выгоды:

- экономия крупных частных компаний от перевода закупок сырья и комплектующих на Интернет-биржи достигает 25 - 30%;
- участие в аукционе конкурирующих поставщиков со всего мира в реальном масштабе времени приводит к снижению запрограммированных ими за поставку товаров или услуг цен;
- повышение цен за товары или услуги в результате конкуренции покупателей со всего мира;
- экономия за счет сокращения числа необходимых сотрудников и объема бумажного делопроизводства.

Доминирующее положение в ЭК в западных странах стал сектор B2B, который

- 2007 году по разным оценкам достигнет от 3 до 6 трлн. долларов.

Первыми получили преимущества от перевода своего бизнеса в Интернет компании, продающие аппаратно-программные средства и представляющие компьютерные и телекоммуникационные услуги.

Каждый интернет-магазин включает две основных составляющих: электронную витрину и торговую систему.

Электронная витрина содержит на Web-сайте информацию о продаваемых товарах, обеспечивает доступ к базе данных магазина, регистрирует покупателей, работает с электронной «корзиной» покупателя, оформляет заказы, собирает маркетинговую информацию, передает сведения в торговую систему.

Торговая система доставляет товар и оформляет платеж за него. Торговая система - это совокупность магазинов, владельцами которых являются разные фирмы, берущие в аренду место на Web-сервере, который принадлежит отдельной компании.

Технология функционирования интернет-магазина выглядит следующим образом:

Покупатель на электронной витрине с каталогом товаров и цен (Web-сайт) выбирает нужный товар и заполняет форму с личными данными (ФИО, почтовый и электронный адреса, предпочитаемый способ доставки и оплаты). Если происходит оплата через Интернет, то особое внимание уделяется информационной безопасности.

Передача оформленного товара в торговую систему интернет-магазина, где происходит комплектация заказа. Торговая система функционирует ручным или автоматизированным способом. Ручная система функционирует по принципу Посылторга, при невозможности приобретения и наладки автоматизированной системы, как правило, при незначительном объеме товаров.

Доставка и оплата товара. Доставка товара покупателю осуществляется одним из возможных способов:

- курьером магазина в пределах города и окрестностей;
- специализированной курьерской службой (в том числе из-за границы);
- почтой;
- самовывозом;
- по телекоммуникационным сетям доставляется такой специфический товар как информация.

Оплата товара может осуществляться следующими способами:

- предварительной или в момент получения товара;
- наличными курьеру или при визите в реальный магазин;
- почтовым переводом;
- банковским переводом;
- наложенным платежом;
- при помощи кредитных карт (VISA, MASTER CARD и др);

посредством электронных платежных систем через отдельные коммерческие банки (ТЕЛЕБАНК, ASSIST и др.).

В последнее время электронная коммерция или торговля посредством сети Интернет в мире развивается достаточно бурно. Естественно, что этот процесс осуществляется при непосредственном участии кредитно-финансовых организаций. И этот способ торговли становится все более популярным, по крайней мере, там, где новым электронным рынком можно воспользоваться значительной части предприятий и населения.

Коммерческая деятельность в электронных сетях снимает некоторые физические ограничения. Компании, подключая свои компьютерные системы к Интернет, способны предоставить клиентам поддержку 24 часа в сутки без праздников и выходных. Заказы на продукцию могут приниматься в любое время из любого места.

Однако у этой «медали» есть своя обратная сторона. За рубежом, где наиболее широко развивается электронная коммерция, сделки или стоимость товаров часто ограничиваются величиной 300-400 долларов. Это объясняется недостаточным решением проблем информационной безопасности в сетях ЭВМ. По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. В США этот вид преступной деятельности по доходности занимает третье место после торговли оружием и наркотиками.

Объем мирового оборота электронной коммерции через Интернет в 2006 году, по прогнозам компании Forrester Tech., может составить от 1,8 до ,2 трлн. долл. Столь широкий диапазон прогноза определяется проблемой обеспечения экономической безопасности электронной коммерции. Если уровень безопасности сохранится на сегодняшнем уровне, то мировой оборот электронной коммерции может оказаться еще меньшим. Отсюда следует, что именно низкая защищенность системы электронной коммерции является сдерживающим фактором развития электронного бизнеса.

Решение проблемы обеспечения экономической безопасности электронной

коммерции в первую очередь связано с решением вопросов защиты информационных технологий, применяемых в ней, то есть с обеспечением информационной безопасности.

Интеграция бизнес-процессов в среду Интернет приводит к кардинальному изменению положения с обеспечением безопасности. Порождение прав и ответственности на основании электронного документа требует всесторонней защиты от всей совокупности угроз, как отправителя документа, так и его получателя.

К сожалению, руководители предприятий электронной коммерции в должной степени осознают серьезность информационных угроз и важность организации защиты своих ресурсов только после того, как последние подвергнутся информационным атакам. Как видно, все перечисленные препятствия относятся к сфере информационной безопасности.

Среди основных требований к проведению коммерческих операций – конфиденциальность, целостность, аутентификация, авторизация, гарантии и сохранение тайны.

При достижении безопасности информации обеспечение ее доступности, конфиденциальности, целостности и юридической значимости являются **базовыми задачами**. Каждая угроза должна рассматриваться с точки зрения того, как она может затронуть эти четыре свойства или качества безопасной информации. *Конфиденциальность* означает, что информация ограниченного доступа должна быть доступна только тому, кому она предназначена. Под *целостностью* информации понимается ее свойство существования в неискаженном виде. *Доступность* информации определяется способностью системы обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия. *Юридическая значимость* информации приобретает важность в последнее время, вместе с созданием нормативно-правовой базы безопасности информации в нашей стране.

Если первые четыре требования можно обеспечить техническими средствами, то выполнение двух последних зависит и от технических средств, и от ответственности отдельных лиц и организаций, а также от соблюдения законов, защищающих потребителя от возможного мошенничества продавцов.

В рамках обеспечения комплексной информационной безопасности, прежде всего, следует выделить ключевые **проблемы в области безопасности электронного бизнеса**, которые включают: защиту информации при ее передаче по каналам связи; защиту компьютерных систем, баз данных и электронного документооборота; обеспечение долгосрочного хранения информации в электронном виде; обеспечение безопасности транзакций, секретность коммерческой информации, аутентификацию, защиту интеллектуальной собственности и др.

Существует несколько видов угроз электронной коммерции:

Проникновение в систему извне.

Несанкционированный доступ внутри компании.

Преднамеренный перехват и чтение информации.

Преднамеренное нарушение данных или сетей.

Неправильная (с мошенническими целями) идентификация пользователя.

Взлом программно-аппаратной защиты.

Несанкционированный доступ пользователя из одной сети в другую.

Вирусные атаки.

Отказ в обслуживании.

Финансовое мошенничество.

Для противодействия этим угрозам используется целый ряд методов, основанных на различных технологиях, а именно: шифрование – кодирование данных,

препятствующее их прочтению или искажению; цифровые подписи, проверяющие подлинность личности отправителя и получателя; stealth-технологии с использованием электронных ключей; брандмауэры; виртуальные и частные сети.

Ни один из методов защиты не является универсальным, например, брандмауэры не осуществляют проверку на наличие вирусов и не способны обеспечить целостность данных. Не существует абсолютно надежного способа противодействия взлому автоматической защиты, и ее взлом – это лишь вопрос времени. Но время взлома такой защиты, в свою очередь, зависит от ее качества. Надо сказать, что программное и аппаратное обеспечение для защиты соединений и приложений в Интернет разрабатывается уже давно, хотя внедряются новые технологии несколько неравномерно.

Какие **угрозы** подстерегают компанию, ведущую электронную коммерцию **на каждом этапе**:

подмена web-страницы сервера электронного магазина (переадресация запросов на другой сервер), делающая доступными сведения о клиенте, особенно о его кредитных картах, сторонним лицам;

создание ложных заказов и разнообразные формы мошенничества со стороны сотрудников электронного магазина, например, манипуляции с базами данных (статистика свидетельствует о том, что больше половины компьютерных инцидентов связано с деятельностью собственных сотрудников);

перехват данных, передаваемых по сетям электронной коммерции; проникновение

злоумышленников во внутреннюю сеть компании и

компрометация компонентов электронного магазина; реализация атак типа «отказ в обслуживании» и нарушение

функционирования или вывода из строя узла электронной коммерции.

- результате реализации таких угроз компания теряет доверие клиентов, теряет деньги от потенциальных и/или несовершенных сделок, нарушается деятельность электронного магазина, затрачивает время, деньги и человеческие ресурсы на восстановление функционирования.

Конечно, угрозы, связанные с перехватом передаваемой через Интернет информации, присущи не только сфере электронной коммерции. Особое значение применительно к последней представляет то, что в ее системах обращаются сведения, имеющие важное экономическое значение: номера кредитных карт, номера счетов, содержание договоров и т. п.

На первый взгляд, может показаться, что каждый подобный инцидент – не более чем внутреннее дело конкретного субъекта электронного бизнеса. Однако вспомним 2000-й год, который был ознаменован случаями массового выхода из строя ведущих серверов электронного бизнеса, деятельность которых носит поистине общенациональный характер: Yahoo!, eBay, Amazon, Buy, CNN, ZDNet, Datek и E*Trade. Расследование, проведенное ФБР, показало, что указанные серверы вышли из строя из-за многократно возросшего числа направленных в их адрес запросов на обслуживание в результате реализованных DoS-атак. Например, потоки запросов на сервер Buy превысили средние показатели в 24 раза, а предельные – в 8 раз. По разным оценкам, экономический ущерб, понесенный американской экономикой от этих акций, колеблется вокруг полуторамилиардной отметки.

Обеспечение безопасности является не только необходимым условием успешного ведения электронного бизнеса, но и фундаментом для доверительных отношений между контрагентами. Сама суть электронного бизнеса предполагает активный информационный обмен, проведение транзакций через незащищенную сеть общего доступа, которые попросту невозможны без доверительных отношений между субъектами бизнеса. Поэтому обеспечение безопасности имеет комплексный характер,

включая такие задачи, как доступ к Web-серверам и Web-приложениям, аутентификация и авторизация пользователей, обеспечение целостности и конфиденциальности данных, реализация электронной цифровой подписи и проч.

С ростом коммерциализации Интернет вопросам защиты передаваемой по сети информации уделяется все больше внимания. Специализированные протоколы, предназначенные для организации защищенного взаимодействия через Интернет (например, SET, SOCKS5, SSL, SHTTP и др.), получили широкое признание во всем мире и успешно используются зарубежными разработчиками для создания банковских и торговых электронных систем на базе Интернет.

За рубежом решением проблемы информационной безопасности электронного бизнеса занимается независимый консорциум – Internet Security Task Force (ISTF) – общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронного бизнеса и провайдеров Интернет - услуг.

Консорциум ISTF выделяет *двенадцать областей информационной безопасности*, на которых в первую очередь должно быть сосредоточено внимание организаторов электронного бизнеса:

механизм объективного подтверждения идентифицирующей информации;
право на персональную, частную информацию; определение событий безопасности;
защита корпоративного периметра; определение атак;
контроль потенциально опасного содержимого; контроль доступа; администрирование;
реакция на события.

Известно, что надежно защититься от многих угроз позволяет применение алгоритмов электронной цифровой подписи (ЭЦП), однако это справедливо только в том случае, если эти алгоритмы вплетены в обоснованные протоколы взаимодействия, юридически верную конструкцию отношений и логически замкнутую систему доверия.

В основе защиты информации лежит простая логика процессов вычисления цифровой подписи и ее проверки парой соответствующих ключей, впрочем, логика, базирующаяся на фундаментальных математических исследованиях. Вычислить цифровую подпись может только владелец закрытого ключа, а проверить – каждый, у кого имеется открытый ключ, соответствующий закрытому ключу.

Безусловно, обеспечением информационной безопасности должны заниматься специалисты в данной области, но руководители органов государственной власти, предприятий и учреждений независимо от форм собственности, отвечающие за экономическую безопасность тех или иных хозяйственных субъектов, должны постоянно держать данные вопросы в поле своего зрения. Для них ниже приведены *основные функциональные компоненты организации комплексной системы информационной безопасности*:

коммуникационные протоколы; средства криптографии;

механизмы авторизации и аутентификации; средства контроля доступа к рабочим местам из сетей общего

пользования; антивирусные комплексы;

программы обнаружения атак и аудита;

средства централизованного управления контролем доступа

пользователей, а также безопасного обмена пакетами данных и сообщений любых приложений по открытым сетям.

- Интернет уже давно существует целый ряд комитетов, в основном, из организаций - добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета (Internet Engineering Task Force, IETF) провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернете. Такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а так же SNMP (Simple Network Management Protocol) для управления сетью – непосредственные результаты усилий IETF. Тип применяемого продукта защиты зависит от нужд компании.

- Интернет популярны протоколы безопасной передачи данных, а именно SSL, SET, IP v.6. Перечисленные протоколы появились в Интернет сравнительно недавно, как необходимость защиты ценной информации, и сразу стали стандартами де-факто. Напомним, что Интернет создавалась несколько десятилетий назад для научного обмена информацией не имеющей большой стоимости.

К сожалению, в России пока еще с большой осторожностью относятся к возможности внедрения Интернет в те сферы деятельности, которые связаны с передачей, обработкой и хранением конфиденциальной информации. Подобная осторожность объясняется не только консервативностью отечественных финансовых структур, опасаящихся открытости и доступности Интернет, но, отчасти, и тем, что большинство программных средств защиты информации западных фирм-производителей поступают на наш рынок с экспортными ограничениями, касающимися реализованных в них криптографических алгоритмов. Например, в экспортных вариантах программного обеспечения WWW-серверов и браузеров таких производителей, как Microsoft и Netscape Communications, имеются ограничения на длину ключа для одноключевых и двухключевых алгоритмов шифрования, используемых протоколом SSL, что не обеспечивает полноценной защиты при работе в Интернет.

Однако приложения электронной коммерции, кроме внутренних угроз, подвержены также и внешней опасности, исходящей от Интернет. И поскольку нерационально присваивать каждому анонимному посетителю отдельный идентификатор входа (так как приложение при этом не увеличивается), компаниям необходимо использовать другой вид аутентификации. Кроме того, необходимо подготовить сервера к отражению атак. И, наконец, следует соблюдать исключительную осторожность по отношению к критическим данным – например, таким, как номера кредитных карт.

Шифрование данных

На бизнес-сайте обрабатывается чувствительная информация (например, номера кредитных карточек потребителей). Передача такой информации по Интернет без какой-либо защиты может привести к непоправимым последствиям. Любой может подслушать передачу и получить таким образом доступ к конфиденциальной информации. Поэтому данные необходимо шифровать и передавать по защищенному каналу. Для реализации защищенной передачи данных используют протокол Secure Sockets Layer (SSL).

Для реализации этой функциональности необходимо приобрести цифровой сертификат и установить его на ваш(и) сервер(а). За цифровым сертификатом можно обратиться в один из органов сертификации. К общеизвестным коммерческим сертификационным организациям относятся: VerySign, CyberTrust, GTE.

SSL представляет собой схему для таких протоколов, как HTTP (называемого HTTPS в случае его защищенности), FTP и NNTP. При использовании SSL для

передачи данных:

- данные зашифрованы; между сервером-источником и сервером назначения установлено
- защищенное соединение;
- активирована аутентификация сервера.

Когда пользователь отправляет номер кредитной карточки с применением протокола SSL, данные немедленно шифруются, так что хакер не может видеть их содержание. SSL не зависит от сетевого протокола.

Программное обеспечение сервера Netscape обеспечивает также аутентификацию – сертификаты и цифровую подпись, удостоверяя личность пользователя и целостность сообщений и гарантируя, что сообщение не меняло своего маршрута.

Аутентификация подразумевает подтверждение личности пользователя и цифровой подписи для проверки подлинности документов, участвующих в обмене информацией и финансовых операциях. Цифровая подпись представляет собой данные, которые могут быть приложены к документу во избежание подлога.

Выявление вторжений

Системы выявления вторжений (Intrusion Detection Systems, IDS) могут идентифицировать схемы или следы атак, генерировать аварийные сигналы для предупреждения операторов и побуждать маршрутизаторы прерывать соединение с источниками незаконного вторжения. Эти системы могут также предотвращать попытки вызвать отказ от обслуживания.

Защита данных сайта

Для защиты данных сайта необходимо проанализировать данные, используемые сайтом, и определить политику безопасности. Эти данные могут представлять собой HTML-код, подробности о клиентах и продуктах, хранящиеся в базе данных, каталоги, пароли и другую аутентификационную информацию. Вот несколько основных принципов, которые можно использовать при определении политики безопасности данных:

Необходимо держать чувствительные данные за внутренним брандмауэром, в защищенной внутренней сети. К чувствительным данным должно быть обеспечено минимальное число точек доступа. При этом необходимо помнить, что добавление уровней безопасности и усложнение доступа в систему влияет на работу системы в целом.

Базы данных, хранящие низко чувствительные данные, могут располагаться на серверах DMZ.

Пароли могут храниться после преобразования с помощью односторонних алгоритмов. Однако это делает невозможным реализацию общепринятой (и популярной) возможности обрабатывать сообщения типа "Я забыл мой пароль, пожалуйста, вышлите мне его по электронной почте", хотя при этом можно создать новый пароль и высылать его в качестве альтернативы.

Чувствительная информация – такая, как номера кредитных карт – может храниться в базах данных и после шифрования. Расшифровывать ее каждый раз при возникновении такой необходимости могут только

авторизованные пользователи и приложения. Однако это также влияет на скорость работы системы в целом.

Можно защитить данные сайта и с помощью компонент среднего яруса. Эти компоненты могут быть запрограммированы для аутентификации пользователей, разрешая доступ к базе данных и ее компонентам только авторизованным пользователям и защищая их от внешних угроз.

Можно реализовать дополнительные функции безопасности серверной части

системы. Например, для предотвращения несанкционированного внутреннего доступа к базе данных можно использовать пользовательские функции безопасности SQL Server.

Заметьте, что не менее важно защищать и резервные копии, содержащие информацию о потребителях.

Ситуация усугубляется еще и тем, что каждую неделю обнаруживаются все новые и новые способы проникновения или повреждения данных, следить за появлением которых в состоянии только профессиональные организации, специализирующиеся на информационной безопасности.

Интеграция коммерции в Интернет сулит кардинальное изменение положения с обеспечением безопасности. С ростом коммерциализации Интернет вопросам защиты передаваемой по сети информации уделяется все больше внимания. Поэтому прогресс в области безопасности информации во многом определяет развитие процесса электронной коммерции.

- России развитие электронной коммерции сдерживается:

Отсутствием или слабым развитием инфраструктуры ЭК, в частности, надежной и повсеместной инфраструктуры доставки товара покупателю (курьерские службы и т.п.), особенно через «электронный магазин», находящийся в другом городе.

Отставанием государственной правоприменительной практики и, как следствие, отсутствие или слабые гарантии исполнения сделок, заключенных в электронной форме.

Наличием объективных и субъективных предпосылок для развития мошенничества, связанных с использованием Интернета для коммерции.

Слабой маркетинговой проработкой проектов ЭК.

Трудностями в оплате товаров, в частности, отсутствие доверия населения к коммерческим банкам.

Низкий уровень доходов большинства населения России делает деньги более весомым богатством, чем время, поэтому многие Россияне не согласны оплачивать наряду со стоимостью товара расходы на его доставку, и предпочитают делать покупки в обычных магазинах. Поэтому ЭК может широко распространиться в России только после существенного улучшения экономической обстановки в стране.

5.3 Обеспечение компьютерной безопасности учетной информации

Переход России к рыночным отношениям выдвигает на первый план проблемы коренной перестройки учета. Если раньше учетная функция управления сводилась к прямому счетоводству и составлению отчетности, то в новых условиях бухгалтер – это центральная фигура управленческого персонала, он главный консультант директора фирмы, аналитик, финансист. Для выполнения новых функций и, прежде всего, создания учета как средства управления и регулирования использование компьютера, а также современных средств связи и коммуникаций жизненно необходимо.

Бухгалтер должен принимать непосредственное участие в создании компьютерной информационной системы бухгалтерского учета, ставить задачи и контролировать достоверность данных, их соответствие реальным хозяйственным операциям, анализировать бухгалтерскую информацию и исправлять неблагоприятные ситуации.

Новые информационные технологии в бухгалтерском учете на базе современных ПЭВМ, с одной стороны, обеспечивают высокое качество выполняемых работ, а с другой, - создают множество угроз, приводящих к непредсказуемым и даже катастрофическим последствиям. К числу *таких угроз* относятся следующие: проникновение посторонних лиц в базы учетных данных, повсеместное распространение компьютерных вирусов, ошибочный ввод учетных данных, ошибки в процессе проектирования и внедрения учетных систем и др. Противостоять возможной реализации угроз можно только приняв адекватные меры, которые способствуют обеспечению безопасности учетной информации. В этой связи каждый бухгалтер, использующий в своей работе компьютеры и средства связи, должен знать, от чего защищать информацию и как это делать.

*Под защитой учетной информации понимается состояние защищенности информации и поддерживающей ее инфраструктуры (компьютеров, линий связи, систем электропитания и т.п.) от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям этой информации.**

Понятие информационной безопасности учетных данных в узком смысле этого слова подразумевает:

- надежность работы компьютера;
 - сохранность ценных учетных данных;
 - защиту учетной информации от внесения в нее изменений неуполномоченными лицами;
 - сохранение документированных учетных сведений в электронной связи.
- К объектам информационной безопасности в учете относятся:
- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде баз учетных данных **;
 - средства и системы информатизации – технические средства, используемые в

* Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

** Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

информационных процессах (средства вычислительной и организационной техники, информативные и физические поля компьютеров, общесистемное и прикладное программное обеспечение, в целом автоматизированные системы учетных данных предприятий).^{*}

Угроза информационной безопасности бухгалтерского учета заключается в потенциально возможном действии, которое посредством воздействия на компоненты учетной системы может привести к нанесению ущерба владельцам информационных ресурсов или пользователям системы.

Правовой режим информационных ресурсов определяется нормами, устанавливающими:

порядок документирования информации; право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных

системах^{**}; категорию информации по уровню доступа к ней; порядок правовой защиты информации.

Основной принцип, нарушаемый при реализации информационной угрозы в бухгалтерском учете, - это принцип документирования информации^{***}. Учетный документ, полученный из автоматизированной информационной системы учета, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

Все множество потенциальных угроз в учете по природе их возникновения можно разделить на два класса: *естественные (объективные)* и *искусственные*.

Естественные угрозы вызываются объективными причинами, как правило, не зависящими от бухгалтера, ведущими к полному или частичному уничтожению бухгалтерии вместе с ее компонентами. К таким стихийным явлениям относятся: землетрясения, удары молнией, пожары и т.п.

Искусственные угрозы связаны с деятельностью людей. Их можно разделить на непреднамеренные (неумышленные), вызванные способностью сотрудников делать какие-либо ошибки в силу невнимательности, либо усталости, болезненного состояния и т.п. Например, бухгалтер при вводе сведений в компьютер может нажать не ту клавишу, сделать неумышленные ошибки в программе, занести вирус, случайно разгласить пароли.

Преднамеренные (умышленные) угрозы связаны с корыстными устремлениями людей – злоумышленников, намеренно создающих недостоверные документы.

Угрозы безопасности с точки зрения их направленности можно подразделить на следующие группы:

угрозы проникновения и считывания данных из баз учетных данных и компьютерных программ их обработки;

угрозы сохранности учетных данных, приводящие либо к их уничтожению, либо к изменению, в том числе фальсификация платежных документов (платежных требований, поручений и т.п.);

угрозы доступности данных, возникающие, когда пользователь не может получить доступа к учетным данным;

угроза отказа от выполнения операций, когда один пользователь передает сообщение другому, а затем не подтверждает переданные данные.

* Информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационная система – организационно-упорядоченная совокупность документов (массивов документов и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы).

Документирование информации осуществляется в порядке, установленном органами государственной власти, ответственными за организацию делопроизводства стандартизацию документов и их массивов, безопасность Российской Федерации.

В зависимости от источника угроз их можно подразделить на **внутренние и внешние**.

Источником *внутренних угроз* является деятельность персонала организации. **Внешние угрозы** приходят извне от сотрудников других организаций, от хакеров и прочих лиц.

Внешние угрозы можно подразделить на:

локальные, которые предполагают проникновение нарушителя на территорию организации и получение им доступа к отдельному компьютеру или локальной сети;
удаленные угрозы характерны для систем, подключенных к глобальным сетям (Internet, система международных банковских расчетов SWIFT и др.).

Такие опасности возникают чаще всего в **системе электронных платежей** при расчетах поставщиков с покупателями, использовании в расчетах сетей Internet. Источники таких информационных атак могут находиться за тысячи километров. Причем воздействию подвергаются не только ЭВМ, но и бухгалтерская информация.

Умышленными и неумышленными ошибками в учете, приводящими к увеличению учетного риска, являются следующие:

ошибки в записи учетных данных;
неверные коды; несанкционированные
учетные операции; нарушение
контрольных лимитов; пропущенные
учетные записи;
ошибки при обработке или выводе данных; ошибки при
формировании или корректировке справочников; неполные
учетные записи; неверное отнесение записей по периодам;
фальсификация данных;

нарушение требований нормативных актов;
нарушение принципов учетной политики;
несоответствие качества услуг потребностям пользователей.

Процедуры, в которых обычно возникают ошибки и их типы, представлены в таблице 8 (172).

Таблица 8

Места возникновения бухгалтерских ошибок

Виды ошибок	Сферы преобразования учетных данных		
	Первичный учет (сбор и регистрация)	Систематизация и обобщение	Вывод
Ошибки в записи учетных данных	+	-	-
Неверные коды	+	+	-
Несанкционированные учетные операции	+	+	-
Нарушение контрольных лимитов;	+	+	-
Пропущенные учетные записи;	+	+	+
Ошибки при обработке или выводе данных;	-	+	+
Ошибки при формировании или корректировке справочников;	+	+	-
Неполные учетные записи;	+	+	+
Неверное отнесение записей по периодам;	+	+	+
Фальсификация данных;	+	+	+
Нарушение требований нормативных актов;	+	+	+
Нарушение принципов	+	+	+

учетной политики;			
Несоответствие качества услуг потребностям пользователей	+	+	+

Незащищенные учетные данные приводят к серьезным недостаткам в системе управления предприятием:

множеству недокументированных эпизодов управления; отсутствию у руководства целостной картины происходящего на предприятии в отдельных структурных подразделениях; задержки в получении актуальной на момент принятия решения информации;

разногласиям между структурными подразделениями и отдельными исполнителями, совместно выполняющими работу, проистекающими из-за плохой взаимной информированности о состоянии деловых процессов;

жалобам сотрудников всех уровней на информационные перегрузки;

неприемлемым срокам разработки и рассылки деловых документов;

длительным срокам получения ретроспективной информации, накопленной на предприятии; сложностям получения информации о текущем состоянии документа или делового процесса; нежелательной утечке информации, происходящей вследствие

неупорядоченного хранения больших объемов документов.

Особую опасность представляют сведения, *составляющие коммерческую тайну* и относящиеся к учетной и отчетной информации (данные о партнерах, клиентах, банках, аналитическая информация о деятельности на рынке).^{*} Чтобы эта и аналогичная информация была защищена, необходимо оформить договора с сотрудниками бухгалтерии, финансовых служб и других экономических подразделений с указанием перечня сведений, не подлежащих огласке.

Защита информации в автоматизированных учетных системах строится исходя из следующих основных принципов:

обеспечение физического разделения областей, предназначенных для обработки секретной и несекретной информации.

Обеспечение криптографической защиты информации.

Обеспечение аутентификации абонентов и абонентских установок.

Обеспечение разграничения доступа субъектов и их процессов к информации.

Обеспечение установления подлинности и целостности документальных сообщений при их передаче по каналам связи.

Обеспечение защиты от отказов от авторства и содержания электронных документов.

Обеспечение защиты оборудования и технических средств системы, помещений, где они размещаются, от утечки конфиденциальной информации по техническим каналам.

Обеспечение защиты шифротехники, оборудования, технических и программных средств от утечки информации за счет аппаратных и программных закладок.

Обеспечение контроля целостности программной и информационной части автоматизированной системы.

Использование в качестве механизмов защиты только отечественных

^{*} Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне и конфиденциальную. Перечень сведений конфиденциального характера, в частности сведений, связанных с коммерческой деятельностью, установлен Указом президента Российской Федерации от 6 марта 1997 г. № 188 (приложение №)

разработок.

Обеспечение организационно-режимных мер защиты. Целесообразно использование и дополнительных мер по обеспечению безопасности связи в системе.

Организация защиты сведений об интенсивности, продолжительности и трафиках обмена информации.

Использование для передачи и обработки информации каналов и способов, затрудняющих перехват.

Защита информации от несанкционированного доступа направлена на формирование у защищаемой информации трех основных свойств:

конфиденциальность (засекреченная информация должна быть доступна только тому, кому она предназначена);

целостность (информация, на основе которой принимаются важные решения, должна быть достоверной, точной и полностью защищенной от возможных непреднамеренных и злоумышленных искажений);

готовность (информация и соответствующие информационные службы должны быть доступны, готовы к обслуживанию заинтересованных лиц всегда, когда в них возникает необходимость).

Методами обеспечения защиты учетной информации являются: препятствия; управление доступом, маскировка, регламентация, принуждение, побуждение.

Препятствием нужно считать метод физического преграждения пути злоумышленника к защищаемой учетной информации. Этот метод реализуется пропускной системой предприятия, включая наличие охраны на входе в него, преграждение пути посторонних лиц в бухгалтерию, кассу и пр.

Управлением доступом является метод защиты учетной и отчетной информации, реализуемой за счет:

идентификации пользователей информационной системы. (Каждый пользователь получает собственный персональный идентификатор);

аутентификации – установления подлинности объекта или субъекта по предъявленному им идентификатору (осуществляется путем сопоставления введенного идентификатора с хранящимся в памяти компьютера);

проверки полномочий – проверки соответствия запрашиваемых ресурсов и выполняемых операций по выделенным ресурсам и разрешенным процедурам;

регистрации обращений к защищаемым ресурсам; информирования и реагирования при попытках несанкционированных действий. (Криптография – способ защиты с помощью преобразования информации (шифрования)).

Пример 1.

В комплексе БЭСТ-4 разграничение доступа к информации производится на уровне отдельных подсистем и обеспечивается путем задания раздельных паролей доступа. При начальной настройке или в любой момент работы с программой администратор системы может задать или сменить один или несколько паролей. Пароль запрашивается при каждом входе в подсистему.

Помимо этого в некоторых модулях предусмотрена своя система разграничения доступа к информации. Она обеспечивает возможность защиты специальными паролями каждого пункта меню. Паролями можно также защитить доступ к отдельным подмножествам первичных документов: так, в АРМ «Учет запасов на складе» и «Учет товаров и продукции» присутствует возможность задавать пароли доступа к каждому складу в отдельности, в АРМ «Учет кассовых операций» – пароли доступа к каждой кассе, в АРМ «Учет расчетов с банком» – пароли доступа к каждому банковскому счету.

Особо следует отметить то обстоятельство, что для эффективного

разграничения доступа к информации необходимо в первую очередь защитить паролями сами режимы определения паролей по доступу к тем или иным блокам.

Пример 2.

В 1С:Предприятие, версия 7.7 существует своя защита информации – **права доступа**. С целью интеграции и разделения доступа пользователей к информации при работе с системой 1С:Предприятие в сети персональных компьютеров, конфигуратор системы позволяет установить для каждого пользователя права на работу с информацией, обрабатываемой системой. Права могут быть заданы в достаточно широких пределах – от возможности только просмотра некоторых видов документов до полного набора прав по вводу, просмотру, корректировке и удалению любых видов данных.

Назначение пользователю прав доступа производится в 2 этапа. На первом этапе создаются типовые наборы прав по работе с информацией, отличающиеся, как правило, широтой предоставляемых возможностей доступа. На втором этапе пользователю ставится в соответствие один из таких типовых наборов прав.

Вся работа по созданию типовых наборов прав производится на закладке «Права» окна «Конфигурация». Это окно вызывается на экран выбором пункта «открыть конфигурацию» из меню «Конфигурация» главного меню программы.

Окно «Права» содержит список типовых наборов прав.

Находясь в окне «Наборы прав», можно:

- создать новый набор прав; создать новый набор прав по образцу существующего;
- отредактировать свойства набора прав; удалить набор прав из списка;
- упорядочить список набора прав и пр.

Конфигуратор системы 1С:Предприятие содержит средства администрирования, предназначенные для решения задач интеграции и разделения доступа при работе в сети персональных компьютеров.

Существует возможность создания списка пользователей, которым разрешена работа с системой 1С:Предприятие. Для работы с системой пользователь должен указать имя из этого списка.

Для эффективной работы каждому пользователю может быть задан индивидуальный пользовательский интерфейс. Такой интерфейс включает расширенное системное меню и панели инструментов, настроенные на работу пользователя с той информацией, доступ к которой разрешен его набором прав.

Вся работа по созданию списка пользователей, присвоению паролей, закреплению за пользователями прав и интерфейса ведутся в окне «Пользователи». Это окно вызывается на экран выбором функции «Пользователи» из меню «Администрирование» главного меню программы.

Чтобы назначить пользователю пароль:

Выберите в списке имя пользователя, которому необходимо присвоить пароль.

Выберите пункт «изменить пароль» в меню «Действия» главного меню Конфигуратора. В запросе «Смена пароля» введите пароль пользователя.

Пароль представляет собой символьную строку длиной не более 10 символов и не должен включать пробелы и специальные символы. Вводимый пароль на экране не показывается, вместо него выводятся символы «*».

Нажмите кнопку ОК.

Запрос «Смена пароля» будет выдан на экран еще раз. Необходимо повторить ввод пароля.

Нажмите кнопку ОК.

Пароль будет присвоен пользователю.

Маскировка – метода криптографической защиты информации в автоматизированной информационной системе предприятия;

Принуждение – метод защиты учетной информации ввиду угрозы материальной, административной или уголовной ответственности. Последнее реализуется тремя статьями Уголовного кодекса:

«Неправомерный доступ к компьютерной информации» (ст. 272); «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273);

Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сетей. (ст. 274).

Побуждение – метод защиты информации путем соблюдения пользователями сложившихся морально-этических норм в коллективе предприятия. К морально-этическим средствам относятся, в частности, Кодекс профессионального поведения членов ассоциации пользователей ЭВМ в США.

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

При передаче документов (платежных поручений, контрактов, распоряжений) по компьютерным сетям необходимо доказательство истинности того, что документ был действительно создан и отправлен автором, а не фальсифицирован или модифицирован получателем или каким-либо третьим лицом. Кроме того, существует угроза отрицания авторства отправителем с целью снятия с себя ответственности за передачу документа. Для защиты от таких угроз в практике обмена финансовыми документами используются методы аутентификации сообщений при отсутствии у сторон доверия друг к другу. Документ (сообщение) дополняется цифровой подписью и секретным криптографическим ключом. Подделка подписей без знания ключа посторонними лицами исключается и неопровержимо свидетельствует об авторстве.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования. Бухгалтер (пользователь) подписывает электронной цифровой подписью с использованием личного ключа, известного только ему, документы, передает их в соответствии со схемой документооборота, а аппаратно-программная система производит проверку подписи. Конфиденциальные документы могут шифроваться на индивидуальных ключах и недоступны для злоумышленников. Система основывается на отечественных стандартах и нормах делопроизводства, практике организации учета документов и контроля действий исполнителей в структурах любой формы собственности (государственной и негосударственной).

Защищенность учетных данных дает возможность:

обеспечить идентификацию/аутентификацию пользователя;

определить для каждого пользователя функциональные права – права на выполнение тех или иных функций системы (в частности, на доступ к тем или иным журналам регистрации документов);

определить для каждого документа уровень конфиденциальности, а для каждого пользователя – права доступа к документам различного уровня конфиденциальности;

подтвердить авторство пользователя с помощью механизма электронной подписи;;

обеспечить конфиденциальность документов путем их шифрования, а также шифрования всей информации, передающейся по открытым каналам связи (например, по электронной почте); шифрование производится с использованием

сертифицированных криптографических средств; протоколировать все действия пользователей в журналах аудита (в журнале аудита входа и выхода из системы, журнале совершенных операций).

Подделка подписи без знания ключа злоумышленниками исключается. При защите учетной информации нужно соблюдать следующий принцип: если вы оцениваете информацию в 100000 рублей, то тратить 150000 рублей на ее защиту не стоит.

Средства контроля в автоматизированных учетных системах размещаются в тех точках, где возможный риск способен обернуться убытками.

Такие точки называются «точками риска», или «контрольными точками». Это те точки, где контроль будет наиболее эффективным и вместе с тем наиболее экономичным. Но как бы ни были эффективны средства контроля, они не могут обеспечить стопроцентную гарантию, в частности, в силу неумышленных ошибок, когда человек вместо цифры 3 набирает цифру 9 или наоборот.

5.4. Информационная безопасность предпринимательской деятельности

Дополнение к учебному пособию "Информационная безопасность экономических систем" Желев В. Н. :
1 Информационная безопасность предпринимательской деятельности.

Мировой опыт убедительно свидетельствует, что экономика не может успешно функционировать без информационно-аналитического обеспечения. Эта объективная необходимость приобретает особое значение для развития российской экономики в современных условиях. С одной стороны, это вызывается настоятельной необходимостью утвердить в сфере российского бизнеса цивилизованные отношения. С другой стороны — необходимостью защитить российский бизнес от существующих угроз. Как свидетельствует практика, эти угрозы становятся все более многочисленными и разнообразными. Сегодня, когда идет активный процесс развития информационно-аналитического обеспечения бизнеса, его безопасности, складывания его рынка, важное значение приобретает анализ места и роли информационно-аналитического обеспечения бизнеса.

Новый рабочий класс — информационщики, применяющий гибкие технологии, способствует замене грубых силовых методов воздействия на производство, распределение, обмен и потребление не только продуктов потребительской корзины, но и самой информации на контрольно-координационные. Мировое сообщество и его региональные альянсы начали испытывать информационное оружие в целях более точного воздействия на человека, вплоть до блокирования его энергетики. На этом фоне различные структуры управления бизнесом не успевают приспособиться к системе помех, диверсий с помощью ЭВМ и в равной степени зависят от узловых воздействий информационного оружия.

Предприниматели-россияне на сегодня не способны оценить и принять решения федеральных и местных структур административного управления в части тарифов, налогов и отчетности. Та же хроническая усталость информационных и карательных систем просматривается в налоговых институтах, банках, образовательных учреждениях, судах.

Многие предприниматели уже испытали на себе многократные покушения на эксклюзивные информационные системы связи (сегодняшняя техника позволяет сотни раз в сутки взламывать защиту компьютеров). Контрмеры не дают более 5–7% эффекта в поимке хакеров. При этом унификации ЭВМ — врожденный порок Интернета; «допускает» к секретам до 90% желающих ими завладеть. И

Информационная безопасность

... Закономерно, что экономическая информация, за которой пять-шесть лет назад предпочитали охотиться конкуренты, уступила свои позиции социальной и правовой информации. Для территорий и предприятий в момент, когда исторически сложившиеся связи между ними разрушились в угоду «рынка», стала актуальной проблема информационной безопасности всех трех указанных сфер. Комплектация этих сфер зарубежными технологиями и аппаратурой неизбежно приводит к «палке о двух концах». Экспорт «чипов» сопряжен с риском бумеранга, который может быть запущен, сбит, возвращается неизвестно откуда и неизвестно чьей рукой. Естественно, когда прибористика не в состоянии что-то делать с требуемой точностью и надежностью, нужны новые технологии. Биоэнергoinформационные ресурсы (маги, экстрасенсы, биоэнергетики, психотерапевты) сегодня уже не являются одиночными факторами, сопровождающимися нанотехнологией. Ряд стран использует их как «биологические системы передачи информации». Существуют целые школы экспертов-биоэнергетиков, специали-

сты которых приглашаются бизнесменами для ведения переговоров, слежения за партнером, предсказания возможных результатов той или иной совместной деятельности, сделки. Обслуживающий вас персонал легко считывает с затылка намерения, настроения и даже незначительные пожелания. ~~Экстрасенсорная перцепция~~ Считывание свойств объекта: звуков, мыслей бесконтактным способом — один из атрибутов современных информационных технологий. Ст

Влияние биоэнергoпроцессов на аппаратуру, электронные узлы управления и контрольно-измерительные приборы базируется на доктрине «бесшумных» информационных войн в регионах нефтедобычи, особенно локализованной, например, морской, рыболовстве, космических исследо-

ваниях и производстве новых материалов в космосе. Также главные цели — изменение поведенческой линии соперника или партнера. Китайские, индийские и филиппинские компьютерные центры в США используют эти технологии весьма успешно на Ближнем Востоке.

Поиски мифических «шпионов» в биржевой, налоговой, таможенной деятельности есть не что иное, как спекуляция деградантов от управления, которые неспособны на то, чтобы государственную, свою безопасность обеспечить. В этой связи хочется отметить, что собственная безопасность начинается с упорядочения биоэнергетических центров самого лица, принимающего решение, отладки межличностных управленческих отношений, организации обязательного исполнения экономического порядка. То, что называется многими конфиденциальной экономической информацией, чаще представляет угрозу для нас самих, так как не спецслужбы иностранных государств, а «двойные» бухгалтерии и канцелярии аппаратов управления отечественной экономикой лишили лидеров политики нормативов экономической и правовой баз. Поэтому, только кадрово-восстановительная работа в узловых сферах информатики, экономики, политики способна сдвинуть с места «завязшие» в болоте инфопатологии функции управления.

**Факторы, влияющие на безопасность
предпринимательской деятельности в России,
и состояние ее защиты**

Социально-экономические преобразования, происходящие в России, как и всякие общественные явления, имеют сложную и во многом противоречивую природу. Если попытаться кратко сформулировать основные факторы, влияющие на безопасность деятельности российских предпринимателей, положительные и отрицательные последствия их воздействия на указанную деятельность, то они заключаются в следующем.

Экономический фактор. В условиях несовершенства российского законодательства, регулирующего предпринимательскую деятельность, мощного и все более усиливающегося прессинга на среду частного бизнеса со стороны преступных группировок, предпринимателям приходится осуществлять свою деятельность на фоне:

- общей нестабильности экономики страны;
- часто меняющегося политического руководства страны;
- зависимости от курсового соотношения рубль — доллар;
- зависимости от импортных поставок;
- ограниченной деловой практики на внешних рынках;
- организационной слабости механизмов согласования интересов государства и предпринимателей;
- несовершенства и противоречивости предпринимательского права;
- низкой эффективности института страхования предпринимательских рисков;
- противоправных посягательств со стороны недобросовестных конкурентов и несостоятельных партнеров;
- посягательств на коммерческую тайну и интеллектуальную собственность;
- низкого профессионализма, недобросовестности, а в ряде случаев и продажности собственного персонала;

Фактор организационно-правового обеспечения безопасности предпринимательской деятельности. В различных сегментах рынка (в наибольшей степени это касается банковской сферы, рынка ценных бумаг, приватизации собственности и др.) сложился своеобразный правовой вакуум. Отсутствие продуманной долгосрочной стратегии и тактики проведения экономических реформ, ведомственная раздробленность и разобщенность государственного регулирования финансового и фондового рынка

способствуют формированию атмосферы непредсказуемости, неуверенности предпринимателей в завтрашнем дне. Со стороны многих субъектов рынка систематически не выполняются требования действующего законодательства. Недостаточно эффективны, а порой и просто бездействуют государственные органы, тогда как обстановка требует конкретных санкций за нарушение законов, противоправные и преступные действия.

Это, в свою очередь, порождает у части предпринимателей и населения правовой нигилизм и уверенность в безнаказанности противоправной, авантюрной и мошеннической деятельности. Это своеобразная питательная среда для криминального бизнеса.

Криминальный фактор. На нем хотелось бы остановиться подробнее. Уже для всех стало ясно, что проблема преступности переходит в устойчивый недуг, проникающий во все поры общества, парализующий его жизнедеятельность. Едва ли не обыденным явлением стали покушения на убийство, смерть банкиров, предпринимателей и их охранников от рук наемных убийц.

В сложившихся условиях правовые отношения, регулирующие деятельность частных охранных структур, также переживают острый кризис. Наиболее остро это относится к основополагающим законам о частной детективно-охранной деятельности и об оружии. Принятие этих законов преследовало цель создания системы обеспечения безопасности предпринимательской деятельности. Но жизнь не стоит на месте, и уже сегодня стало совершенно очевидным, что законодательная база частной детективной и охранной деятельности и подготовки кадров в РФ остается несовершенна.

Криминальные структуры на законном основании имеют оружие, надежные средства защиты, современную спецтехнику слухового и визуального наблюдения. По данным МВД России, в каждом из крупных преступных сообществ имеются хорошо организованные «боевые формирования», в которых десятки человек на официальном основании вооружены, имеют средства связи, защиты, спецтехнику. Между группировками идет ожесточенная борьба за сферы влияния и передел собственности. Высокий процент экономических преступлений, коррумпированность властных и деловых структур показывает, что преступные посягательства стали изощреннее, с трудом раскрываются и не имеют тенденции к сокращению. В последнее время преступный мир острее своих атак обратил в направлении средних и крупных промышленных предприятий, банков, коммерческих структур. Центр их тяжести смещается в сторону «интеллектуальных» преступлений, не всегда даже поддающихся учету.

Таким образом, ситуация в сфере обеспечения безопасности бизнеса, реакция общественности на убийства известных предпринимателей свидетельствуют о том, что одной из главных причин низкой эффективности системы обеспечения безопасности бизнеса является недостаточное взаимодействие, во-первых, в самой предпринимательской среде, во-вторых, с государственными правоохранительными и специальными органами и, в-третьих, отсутствие достаточной государственной поддержки.

Главными источниками угроз безопасности для предпринимательства являются:

- рэкет со стороны частных лиц;
- реальная возможность физического насилия над сотрудниками фирм и членами их семей;

Сотрудники, работающие в отделах бухгалтерии, закупок, продаж, маркетинга, часто имеют прямой доступ к деньгам и / или товарам и поэтому являются первичным источником риска, но это не исключает, что другие работники, у которых имеются гораздо меньшие возможности для незаконных действий, не занимаются мошенничеством или кражами.

Заказчики и поставщики. Представители этих групп также иногда могут войти в сговор с вашими постоянными сотрудниками и совместно спланировать операцию против вас. Обычно здесь прибегают к таким приемам, как подкуп сотрудника, ведущего учет продаж, чтобы тот списал задолженность компании-партнера, за что тот получит свои «законные» комиссионные, или, если говорить о приобретениях, дача взятки сотруднику, производящему закупки для фирмы, чтобы тот купил товары у конкретной фирмы.

Журналисты-репортеры. Эти люди могут стать очень серьезной угрозой, особенно когда они «работают» над репортажем. Они могут распространить слухи о готовящемся большом заказе, что может оказаться нежелательным, так как предполагаемая сделка может быть со страной, которая, по мнению общественности, может считаться «плохой», с которой «порядочным людям» не стоит иметь никаких отношений. Другие проблемы, за которыми охотятся журналисты и которые компании не любят выпускать из своих стен, — экологические загрязнения, серьезные аварии на производстве, финансовые затруднения, заработки и вознаграждения директората, возможные слияния с другими структурами, предстоящее сокращение персонала, судебные предписания и разногласия среди членов руководства компании. Ясно, что подобная информация, если она подана не в благоприятном для компании свете, может существенно негативно сказаться на ее бизнесе.

Следует быть настороже и при общении с **торговыми и техническими представителями**, которые любят вести посторонние разговоры и задавать вопросы, не имеющие отношения к направлению их деятельности. Увлечшись подобной болтовней, можно легко выдать конфиденциальную информацию, что может пойти во вред компании. Такие люди обычно любят похвастаться своей осведомленностью и понесут ваши сведения дальше как эстафетную палочку, делясь ими в своих дальнейших разговорах, и дело может закончиться тем, что ваши секретные сведения станут секретом Полишинеля. Особенно «приятно», когда такой представитель сразу же после вас отправляется к вашему конкуренту. Похожую угрозу

Описанные выше угрозы и опасности исходят от людей, но, к сожалению, возможные несчастья грозят и с другой стороны: аварии и природные катаклизмы несут свои опасности делу. Из последних особенно выделим пожары и наводнения. Вы, конечно, знаете о тех многочисленных пожарах, которые постоянно случаются и парализуют на очень долго жизнь предприятий, в считанные часы переводя их из процветающих в умирающие. Это масштабные события, но есть и более мелкие, возможно, менее заметные, но происходящие в офисах компаний гораздо чаще — это **травмы, ошибочные решения, упущения в работе** и т.п. — все это в совокупности ведет к большим убыткам и обуславливает введение соответствующей организации работы и системы контроля за ней.

В целом кратко рассмотрен весь спектр возможных угроз, связанных с деятельностью офиса. Теперь необходимо исследовать отдельные опасности более детально, так как только хорошо разбираясь в их сущности, можно подготовить соответствующие меры по эффективному противо-