ФЕДЕРАЛЬНОЕ АГЕНСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Нижегородский государственный университет им. Н.И. Лобачевского»

В.Н. Ясенев

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Учебно-методическое пособие

Рекомендовано методической комиссией финансового факультета для студентов высших учебных заведений, обучающихся по направлению подготовки 080105 «Финансы и кредит», 080109 «Бухгалтерский учет, анализ и аудит», 080107 «Налоги и налогообложение», 080301 «Коммерция (торговое дело)», 080503 «Антикризисное управление» и 080115 «Таможенное дело».

Нижний Новгород
2006

ББК 66.01
К 86

Рецензент:

Доцент Ротков В.Ю., проректор по информационной безопасности ННГУ им. Н.И. Лобачевского, руководитель центра "Безопасности информационных систем и средств коммуникации" радиофизического факультета ННГУ;

Ясенев В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ: Учебное пособие – Н. Новгород: Изд-во ННГУ, 2006

Учебное пособие «Информационная безопасность в экономических системах» предназначено для студентов экономических специальностей высших учебных заведений.

Рассматриваются основные понятия информационной безопасности, классификация информационных угроз и характеристика их последствий, построение системы защиты информации, особенности организации информационной безопасности в отдельных экономических системах.

Для студентов, обучающихся по спец. «Финансы и кредит», «Бухгалтерский учет, анализ и аудит», «Налоги и налогообложение», «Антикризисное управление», «Таможенное дело», «Коммерция (торговое дело)».

ISBN 5-85746-736-6

Оглавление

Безопасность есть предотвращение зла
Платон

Введение

В современном мире информация становится стратегическим ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость экономики от информационных воздействий.

Распространение компьютерных систем, объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Проблема компьютерной преступности во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил общественности для организации борьбы с данным видом преступлений. Особенно широкий размах получили преступления в автоматизированных банковских системах и в электронной коммерции. По зарубежным данным, потери в банках в результате компьютерных преступлений ежегодно составляют многие миллиарды долларов. Хотя уровень внедрения новейших информационных технологий в практику в России не столь значителен, компьютерные преступления с каждым днем дают о себе знать все более и более, а защита государства и общества от них превратилась в суперзадачу для компетентных органов.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

Одной из основных причин, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого.

В связи с этим, основной задачей преподавания дисциплины "Информационная безопасность экономических систем" является подготовка экономистов, обладающих знаниями, навыками, умениями, в сфере обеспечения информационной безопасности организаций различных форм собственности.

Несмотря на большое количество публикаций по рассматриваемой проблеме, до настоящего времени отсутствует комплексная проработка трех взаимосвязанных задач. Во-первых, анализ потенциальных угроз в автоматизированных информационных системах при реализации программных злоупотреблений, во-вторых, методология построения системы информационной безопасности, и, в-третьих, особенности защиты информации в отдельных

экономических системах. В качестве отправной точки для исследования выделенных задач могут использоваться работы: Галатенко В.А.(35), Иванов А.З.(74), Гринберга А.С.(41), Горбатова В.С.(43), Столингса В.(199), Уфимцева Ю.С.(210), Мельникова В.В.(137), Конеева И.(111), Батурин Ю.М.(15), Козлова В.Е.(101), Крысина А.(117), Карпычева В.Ю.(106).

Несмотря на обширный список специальной литературы, ощущается недостаток учебно-методической литературы, предназначенной именно для студентов экономических специальностей вузов. Этот пробел призвано восполнить в какой-то степени настоящее пособие.

Учебная дисциплина "Информационная безопасность экономических систем" состоит из трех разделов. Материалы первого раздела знакомят обучаемого с основными понятиями информационной безопасности, информационными угрозами, их классификацией и возможными последствиями для организаций различных форм собственности.

Второй раздел посвящен вопросам обеспечения информационной безопасности организации и проблемам создания (концептуального проектирования) систем информационной безопасности.

В третьем разделе рассматриваются особенности создания информационной безопасности автоматизированных банковских систем (АБС), защиты учетной информации организации и пр.

Содержательные аспекты дисциплины "Информационная безопасность" логически связаны с такими учебными дисциплинами как: "Информатика", "Информационные системы в экономике", "Менеджмент", "Маркетинг", "Финансы", "Денежное обращение и кредит", "Электронные платежи", "Бухгалтерский учет, анализ и аудит" и др.

Тематическим планом преподавания дисциплины предусматриваются следующие виды занятий: лекции, практические занятия, самостоятельная работа. Контроль знаний обучаемых осуществляется в ходе тестирования и сдачи зачета.

Преподавание дисциплины "Информационная безопасность экономических систем" имеет целью:

- дать студентам знания по теоретическим основам обеспечения информационной безопасности организаций различных форм собственности;
- сформировать у обучаемых умения и практические навыки применения методов и средств защиты информации.

Глава 1 Теоретические аспекты информационной безопасности экономических систем

1.1 Основные понятия

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 информационные 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. 1Структура 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 разглашении.

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 целей 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 РФот 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. Тайца 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.

Глава 2 Понятие информационных угроз и их виды

2.1 Информационные угрозы

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.

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 блокировать 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.

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.

Возможен ***бесконтрольный уход конфиденциальной информации*** по визуально-оптическим, акустическим, электромагнитным и другим каналам.

По физической природе возможны следующие средства переноса информации:

1. Световые лучи.
2. Звуковые волны.
3. Электромагнитные волны.
4. 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;
- выпытывание;
- 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

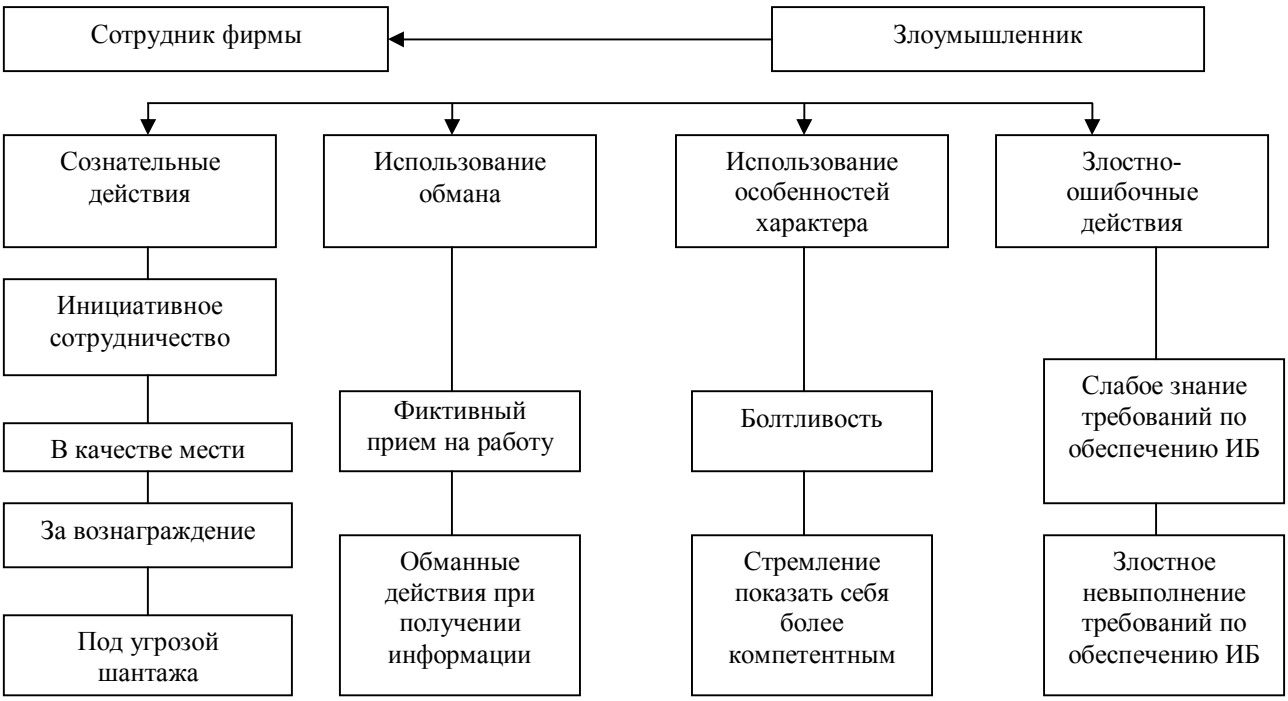

Рис. 3 Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности

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.

На втором месте по размерам ущерба стоят кражи и подлоги. Весьма опасны так называемые обиженные сотрудники - нынешние и бывшие. Как правило, их действиями руководит желание нанести вред организации-обидчику. С этой целью они могут:

- повредить оборудование;
- "встроить" логическую бомбу;
- ввести данные или изменить их;

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно.

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 программно-аппаратных 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 нарушение 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 действи;

– 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.

2.2 Вредоносные программы

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 помешает 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);
- наличию в большинстве случаев определенного инкубационного периода;
- способности «заражать» еще незараженные системы;
- трудности борьбы с вирусами и т.д.

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 Microsoft Word. 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.

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 («троянских 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 «троянские» 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 прочитать 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

Рис. 4 Основные классы вирусов

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

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 WordBasik, 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 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 программу 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 антивиирусов 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 7-й конференции по безопасности информации.

В 1989 г. американский студент сумел создать вирус, который вывел из строя около 6000 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 "троянские 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.

2.3 Компьютерные преступления и наказания

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.

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.

Пример (128)

В Минске имел место случай, когда некто Ч., используя портативный персональный компьютер с модемом, из специально предоставленной ему сообщниками квартиры подключился к электронным почтовым ящикам государственного предприятия "Белорусский межбанковский расчетный центр" во время сеанса связи и передачи плановых платежей. Он внес изменения в номер и код счета. Переданная ложная информация была обработана в централизованном порядке.

В специальной научной литературе описан случай сговора программиста с преступной группой, в результате чего программист, работающий над банковским программным обеспечением, умышленно ввел подпрограмму (программное закладное средство), которая после установки на компьютерную систему обеспечила преступникам несанкционированный доступ с целью извлечения денежных средств.

Бесконтактное подключение к передающим линиям может быть реализовано при помощи различных технических средств (см. разд. 1). На данный момент разработаны устройства подключения к волоконно-оптическим линиям связи.

В специальной литературе описаны также и некоторые иные разновидности несанкционированных подключений (101):

- считывание данных в массивах других пользователей;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы в форме несанкционированного подключения с воздействием на парольно-ключевые системы средств электронной защиты;
- иные.

Под копированием информации (рис. 5) понимается воспроизведение точного или относительно точного ее оригинала.

Рис. 5

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, обусловливающих 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).

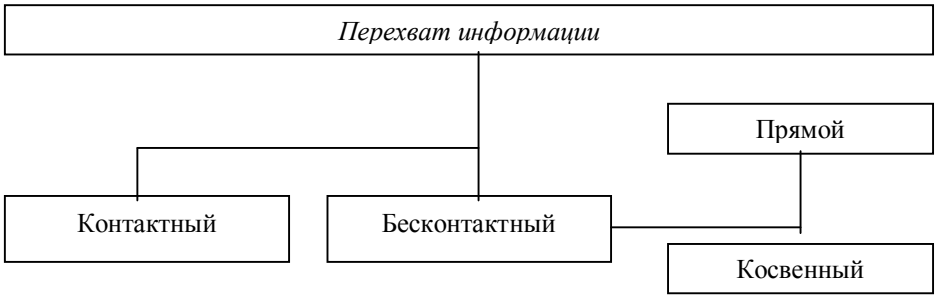

Рис. 6

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 PTT ().

Для анализа собранной информации в стационарных условиях возможно использование преступниками видеомагнитофонов. 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.

Пример 2

В ноябре 1999 года в г. Липецке (Российская Федерация) была произведена злонамеренная вирусная модификация сервера FidoNet. Данное деяние совершено двумя школьниками Н. и Ш., проживающими в указанном городе. Сам вирус был написан Н., который являлся гордостью школы № 69, отличаясь способностями в математике и информатике, Ш. осуществил внедрение вируса в сеть, подсмотрев чужой пароль для входа в нее.

От имени владельца пароля было выставлено электронное объявление "Внимание! Разработан новый архиватор! Попробуйте все!" Расчет был сделан на любопытство пользователей сети. Код вируса содержался в файле kos.exe, замаскированном под новый архиватор.

Попав в компьютер, программа действительно выполняла функции архиватора, однако при перезагрузке вся информация с жесткого диска уничтожалась. Вирус был обнаружен и обезврежен специалистами Липецкэлектросвязи менее чем за сутки. По иронии судьбы единственный пострадавший компьютер принадлежал сотруднику следственного управления УВД Липецкой области ().

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 табуляграммы 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 нападениям 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.

Вместе с тем из-за высокой латентности этого вида преступлений, отсутствия статистических отчетов, очень сложно определить истинные масштабы этого явления.

22 марта 1995 года неустановленный преступник, узнав пароль и используя программное обеспечение компьютера Пинского филиала БелАКБ "Магнатбанк", внедрился в компьютерную сеть ЗАО "Белорусский межбанковский расчетный центр" и перевел денежные средства с корреспондентского счета банка в размере 1 млрд. 700млн. рублей на расчетный счет ООО "Арэса ЛТД" в Советское отделение БелАКБ "Промстройбанк". На следующий день коммерческий директор ООО "Арэса ЛТД" получил выписку с указанием счета о поступлении денег с тем, чтобы перевести их на другие фирмы и обналичить, однако довести до конца свой замысел не сумел, так как был задержан работниками службы безопасности банка.

Правоохранительными органами Минска было предъявлено обвинение 22-летнему Евгению Холину в том, что он, работая старшим специалистом отдела операций с безналичной валютой Главного управления валютных операций АКБ "Приорбанк", использовал свое служебное положение для совершения преступления.

По предварительному сговору с другими лицами Холин в период с ноября 1993 г. по май 1994 г. систематически совершал хищения валютных средств из АКБ "Приорбанк", применяя компьютер на своем рабочем месте. В результате Холин перечислил за границу около 190 тыс. долларов. А всего с сообщниками с использованием поддельных платежных документов им было похищено со счетов "Приорбанка" около 230 тыс. долл.

Совершались указанные преступления в "Приорбанке" весьма просто. Используя свое служебное положение, Холин находил клиентов, имевших в банке счет, но не имевших в карточке образцов печати. С помощью сообщников он подделывал подписи клиентов, сам же подтверждал их достоверность и под паролями коллег внедрялся в компьютерную сеть "Приорбанка" с фиктивной "платежкой".

С целью сокрытия следов преступления Холин трижды уничтожал базу данных АКБ "Приорбанк". Для этих целей он купил себе компьютер и специально разработал программу для уничтожения базы данных. Прототип этой программы (программу "Киллер") он приобрел на "черном" рынке в Москве и специально адаптировал ее к базе данных "операционный день банка". В результате Холин практически уничтожил базу данных банка, но преступнику не повезло - в банке сохранились копии. После инцидента с базой данных компетентные органы и вышли на личность Е.Холина.

Изучение материалов дела Е.Холина показывает, что в АКБ "Приорбанк" сложились благоприятные условия для зондирования компьютерной системы банка, чем и воспользовался злоумышленник. Холину был разрешен доступ к сети банка по выходным дням. Ему давались ключи от комнаты с серверами, и он самостоятельно включал сервер сети и работал. Более того, Холин имел доступ к делам по открытию счетов клиентов в банке. В отделе, где работал Холин, была картотека банковских счетов и их владельцев, а также за неимением дополнительного помещения, хранились дела с заявлениями клиентов банка на открытие счетов с образцами подписей и печатей. Рядом трудились доверчивые коллеги, которые и не думали скрывать от Холина личные пароли-доступы в компьютерную сеть банка.

По приговору суда Центрального района г. Минска Е.Холин осужден к 10 годам лишения свободы.

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 тоже;
- 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:

1. *Физические злоупотребления,* которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
2. *Операционные злоупотребления,* представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.
3. *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; "троянский конь" - включение в обычную программу своего задания).
4. *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.

1. *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.

2. 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.

"*За дураком*". Этот способ часто используется преступниками для проникновения в запретные зоны - электронные системы. Преступник (из числа внутренних пользователей) путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру (обычно используются так называемые "шнурки" - шлейф, изготовленные кустарным способом, либо внутренняя электронная проводка) в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал или персональный компьютер в активном режиме, производит неправомерный доступ к компьютерной информации.

"За хвост". Этот способ съема компьютерной информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его "на себя", а потом законный пользователь заканчивает активный режим, осуществляет доступ к системе. Этот способ технологически можно сравнить с работой двух и более неблокированных телефонных аппаратов, соединенных параллельно и работающих на одном абонентском номере: когда телефон "А" находится в активном режиме, на другом телефоне "Б" поднимается трубка, когда разговор по телефону "А" закончен и трубка положена - продолжается разговор с телефона "Б".

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

"Брешь". 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.

"Мистификация". Иногда по аналогии с ошибочными телефонными звонками, случается так, что пользователь с терминала или персонального компьютера подключается к чьей-либо системе, будучи абсолютно уверенным в том, что он работает с нужным ему абонентом. Этим фактом и пользуется преступник, формируя правдоподобные ответы на запросы владельца информационной системы, к которой произошло фактическое подключение, и поддерживая это заблуждение в течении некоторого периода времени, получая при этом требуемую информацию, например коды доступа или отклик на пароль.

"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.

"Склад без стен". Несанкционированный доступ к компьютерной информации в этом случае осуществляется преступником путем использования системной поломки, в результате которой возникает частичное или полное нарушение нормального режима функционирования систем защиты данных. Например, если нарушается система иерархичного либо категорийного доступа к информации, у преступника появляется возможность получить доступ к той категории информации, в получении которой ему ранее было отказано.

"Подмена данных". Наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, которое осуществляется, как правило, при вводе/выводе информации. В частности, данный способ совершения преступления применяется для приписывания счета "чужой" истории, т.е. модификации данных в автоматизированной системе банковских операций, приводящей к появлению в системе сумм, которые реально на данный счет не зачислялись. Например, по данным зарубежной печати, одно туристическое агентство в Великобритании было разорено конкурентами. Преступники, использовав несанкционированный доступ в автоматизированную компьютерную систему продажи авиабилетов, совершили финансовую сделку - путем подмены данных они произвели закупку билетов на

самолеты на всю сумму денежных средств, находящихся на счетах туристического агентства.

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.

В данной категории преступлений выделяют также:

а) преступления, совершаемые в отношении компьютерной информации, находящейся в компьютерных сетях, в том числе сети Интернет;

б) преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.).

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:

1. персональные данные;
2. корпоративная информация, составляющая коммерческую тайну;
3. объекты интеллектуальной собственности и материалы, защищенные авторским правом;
4. 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.

Хищение услуг. К данной группе правонарушений относится получение несанкционированного доступа к какой-то системе, чтобы бесплатно воспользоваться предоставляемыми ею услугами.

Примером преступления данной категории является фоун-фрейкинг - использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи.

Сюда же можно отнести использование ресурсов систем - объектов

несанкционированного доступа для решения задач, требующих сложных расчетов, например, для определения закодированных паролей, которые они похищают с других узлов.

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.

Объектом подобных атак могут стать компьютеры, соединенные с Интернетом. Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

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.

Методы манипуляции.

Сущность методов манипуляции состоит в подмене данных, которая осуществляется, как правило, при вводе/выводе данных. Это простейший и поэтому очень часто применяемый способ.

Вариантом подмены данных является *подмена кода.*

Рассмотрим некоторые конкретные методы:

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

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.

Реверсивная модель. Существо метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели "вперед-назад" может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

"Воздушный змей". В простейшем случае требуется открыть в двух банках по небольшому счету. Далее, деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в тот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически, она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, и владелец счетов скрывается. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике, в такую игру включают большое число банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Манипулирование данными осуществляется также и самими руководителями коммерческих структур с целью нанесения ущерба государству.

Как правило, компьютерные преступления совершаются с помощью различных комбинаций вышеописанных способов.

Таблица, составленная по результатам опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.

Таблица 2

Вирус	83%
Злоупотребление сотрудниками компании доступом к Internet	69%
Кража мобильных компьютеров	58%
Неавторизованный доступ со стороны сотрудников компании	40%
Мошенничество при передаче средствами телекоммуникаций	27%
Кража внутренней информации	21%
Проникновение в систему	20%

Допускалось несколько вариантов ответов.
Источник: Computer Security Institute.

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	Руков о-дитель	Прог-раммист	Инженер (техник)	Польз о-ватель	Конку -рент
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.

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 отличии 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.

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).

В соответствии со ст. 272 УК РФ преступлением является неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Ст. 272 УК РФ - "неправомерный доступ к компьютерной информации"

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети,-

наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети,-

наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Тот факт, что ст. "Неправомерный доступ к компьютерной информации" (ст.272 УК РФ) находится на первом месте в главе не случаен. Это обусловлено актуальностью проблемы, связанной со сложившимся катастрофическим положением на отечественном рынке компьютерной информации, а также свободным доступом пользователей ПК к информационным ресурсам и бесконтрольным копированием последних. Особый размах получило так называемое "компьютерное пиратство". Масштабы этого явления в России достаточно большие.

Предметом посягательства является охраняемая законом компьютерная информация на машинном носителе, в ЭВМ, компьютере, системе ЭВМ или их сети.

Объективная сторона преступления по ст. 272 включает совокупность

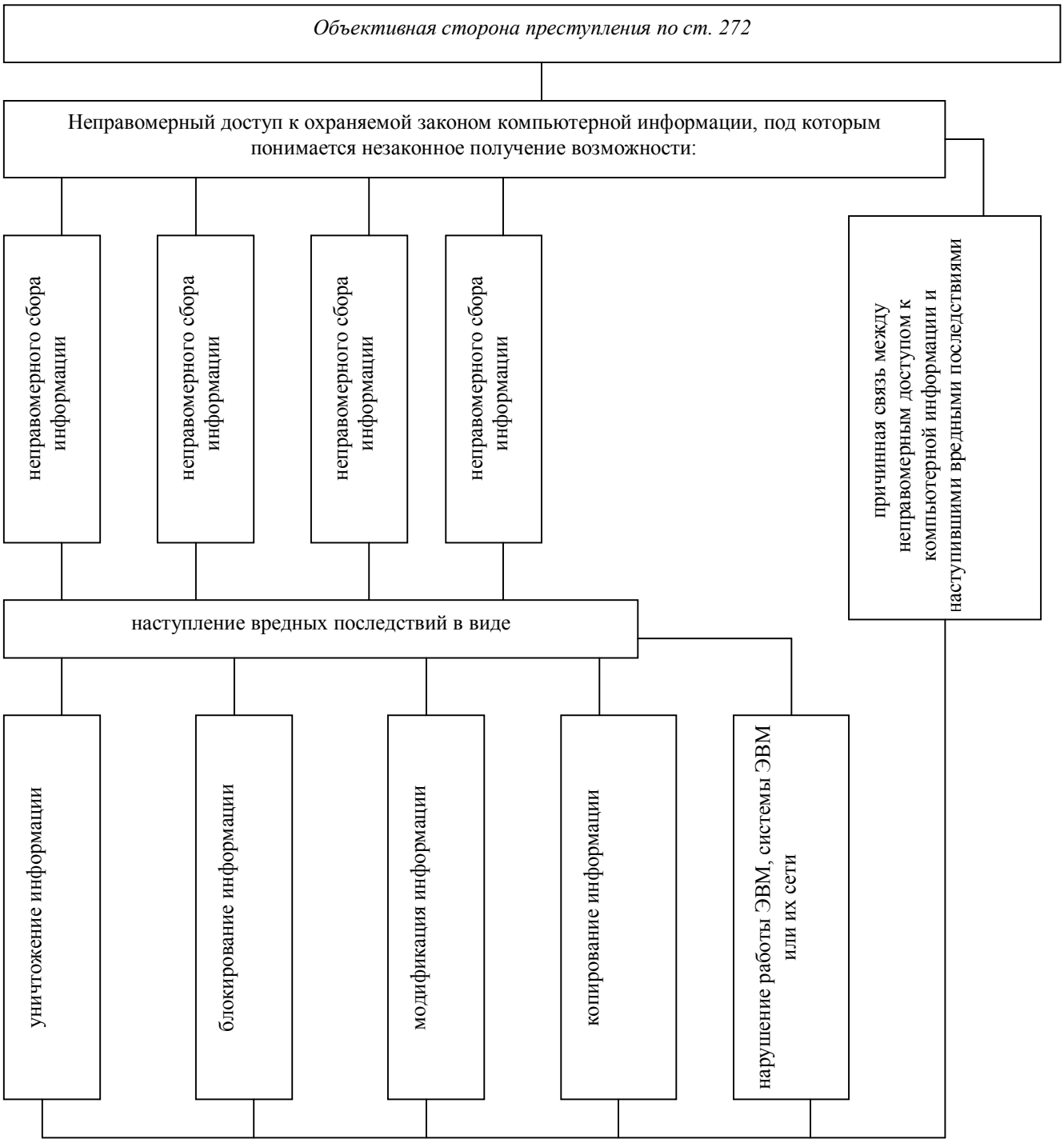

Рис. 7

Отягчающие обстоятельства, предусматриваемые ч.2 ст. 272 представлены на рис. 8

Отягчающие обстоятельства, предусмотренные ч.2 ст.272

Совершение прес тупления группой лиц по предвари-тельному сговору т.е. с участием лиц, заранее дого ворившихся о сов местном соверше нии преступления	Совершение преступле-ния организованной группой лиц, т.е. устой-чивой группой лиц, заранее объединившихся для совершения одного или нескольких преступ-лений (ч.3 ст.35 УК РФ)	Совершение преступления лицом с использованием своего служеб-ного положения либо лицом, име ющим доступ к ЭВМ, системе ЭВМ или их сети, т.е. виновный получает доступ к компьютерной информации, незаконно использ-зуя права, предоставл ему в силу выполн. им служеб. деятельности

Рис. 8

Ст. 273 УК РФ - "Создание, использование и распространение вредоносных программ для ЭВМ"

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ, а равно использование либо распространение таких программ или машинных носителей с такими программами,-

наказывается лишением свободы на срок до трех лет, со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия,- наказываются лишением свободы на срок от трех до семи лет.

Статья 273 УК предусматривает ответственность за создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушение работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Опасность распространения вредоносных программ для ЭВМ заключается в причинении вреда интересам владельца информации, нарушении авторских прав и иных законных интересов - как граждан, так и организаций, общества или государства, а также к угрозе причинения вреда.

Непосредственным объектом этого преступления является право владельца компьютерной системы на неприкосновенность информации (программного обеспечения).

Помимо компьютерных вирусов существует большое количество программ, которые также способны наносить большие ущербы. К этим программам можно отнести также хорошо известные специалистам продукты программирования как "троянские кони", "троянские матрешки", "салями", "логическая бомба", временная бомба, загруженные "атлеты", которые могут использоваться как в положительных целях, так и в преступных и иные программы, которые можно отнести к вредоносным. В большинстве случаев эти программы используются для хищения денег со счетов, шпионажа (коммерческого или промышленного), в хулиганских целях, из мести, озорства и т.д.

Объективную сторону преступлений по ст. 273 УК образуют несколько самостоятельных действий:

1) создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушении работы ЭВМ, системы ЭВМ либо их сети;

2) использование таких программ;

3) распространение таких программ или машинных носителей с такими программами.

Для наступления уголовной ответственности по ч.1 ст.273 необходимо, чтобы вредоносная программа *создавала опасность* наступления следующих негативных последствий:

- уничтожение компьютерной информации;
- блокирования компьютерной информации;
- модификации компьютерной информации;
- копирования компьютерной информации;
- нарушения работы ЭВМ, системы ЭВМ или их сети.

Статья 274 УК предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Ст. 274 УК РФ - "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети"

1.Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред,-

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

3. То же деяние, повлекшее по неосторожности тяжкие последствия,- наказываются лишением свободы на срок до четырех лет.

Объективная сторона данного преступления включает совокупность элементов, схематично представленных на рис. 9

Рис. 9

Под нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети подразумевается нарушение установленных собственником, владельцем, законом либо иным нормативным актом инструкций или правил обращения с аппаратным обеспечением ЭВМ, системой ЭВМ, их сетями либо программного обеспечения, предназначенного для функционирования этих компьютерных устройств.

Вредные последствия могут наступить в виде:

- уничтожения;
- блокирования;
- модификации охраняемой законом компьютерной информации.

Нарушения правил эксплуатации ЭВМ могут быть подразделены на:

1. физические (неправильная установка приборов, нарушение температурного режима в помещении, неправильное подключение ЭВМ к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных приборов и узлов);
2. интеллектуальные (неверное ведение диалога с компьютерной программой, ввод данных, обработка которых непосильна данным средствам вычислительной техники).

а) безвозвратная утрата особо ценной информации;

б) выход из строя важных технических средств (например, систем оборонного назначения), повлекший несчастные случаи с людьми, аварии, катастрофы;

в) причинение крупного имущественного ущерба, т.е. ущерба, превышающего 500 минимальных размеров оплаты труда на момент совершения преступления.

К иным тяжким последствиям могут быть отнесены, например, дезорганизация технологического процесса на производстве, крупная авария и т.п.

Субъект компьютерного преступления общий - лицо, достигшее 16 лет. В ст.274 и ст. 272 УК формулируются признаки специального субъекта: лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Объект компьютерных преступлений достаточно сложен. В обществе существуют определенные ценностные отношения по поводу использования автоматизированных систем обработки данных. Содержанием этих отношений являются права и интересы лиц, общества и государства относительно компьютерных систем, которые понимаются в качестве подлежащего правовой охране блага. Компьютерные преступления посягают на эти права и интересы, которые и являются видовым (групповым) объектом преступлений в сфере компьютерной информации. Таким образом, видовым (групповым) объектом преступлений в сфере компьютерной

информации являются права и интересы физических и юридических лиц, общества и государства по поводу использования автоматизированных систем обработки данных. Непосредственным объектом отдельных преступлений в сфере компьютерной информации являются конкретные права и интересы по поводу использования таких систем (право владельца системы на неприкосновенность информации, содержащейся в системе, интерес относительно правильной эксплуатации системы).

Компьютерные преступления, посягая на основной объект, всегда посягают и на дополнительный объект, поскольку поражают блага более конкретного свойства: личные права и неприкосновенность частной сферы, имущественные права и интересы, общественную и государственную безопасность и конституционный строй. Эти подлежащие правовой охране интересы личности, общества и государства являются дополнительным объектом компьютерных преступлений. Отсутствие посягательства на эти общественные отношения (либо незначительность такого посягательства) исключает уголовную ответственность в силу ч.2 ст.14 УК.

Давайте рассмотрим такой пример. А., приходя в офис своего друга Р., использовал его компьютер, и в частности блок игровой информации (игровые программы), не ставя в известность об этом Р. Его действие - это практически кратковременное использование без разрешения чужого компьютера, являющееся неправомерным доступом к компьютерной информации, и, несомненно, в полной мере отражает основной объект преступления, но не отражает дополнительного объекта преступления, т.е. не содержит конкретного признака состава преступления.

Глава 3 Принципы построения системы информационной безопасности

3.1 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.

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:

1) более широкое толкование традиционных норм;
2) 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 (агенству 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, неправомочно приобретавших 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 § 263а, 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.

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

[*] Лазарев А. Статья для хакера // весь компьютерный мир, 1997, №1. С.9.
[**] Фемида США не успевает // Компьютера, 1996, № 49. С.8.

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 – о 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).

Доктрина информационной безопасности Российской Федерации (далее – Доктрина) утверждена Президентом РФ 9 сентября 2000 г. Этот документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ (прил. №4).

Доктрина на многие годы вперед служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности РФ;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ;
- разработки целевых программ обеспечения информационной безопасности РФ;

Доктрина развивает Концепцию национальной безопасности РФ применительно к информационной сфере.

На основе первоочередных мероприятий, перечисленных в Доктрине, предлагается разработка соответствующей федеральной программы, а также ряда развивающих ее документов, утверждаемых Президентом РФ.

В 2002 г. принят Закон «Об электронной цифровой подписи», 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.
- осуществить мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органов 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.

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.

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).

1. 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.

2. 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.

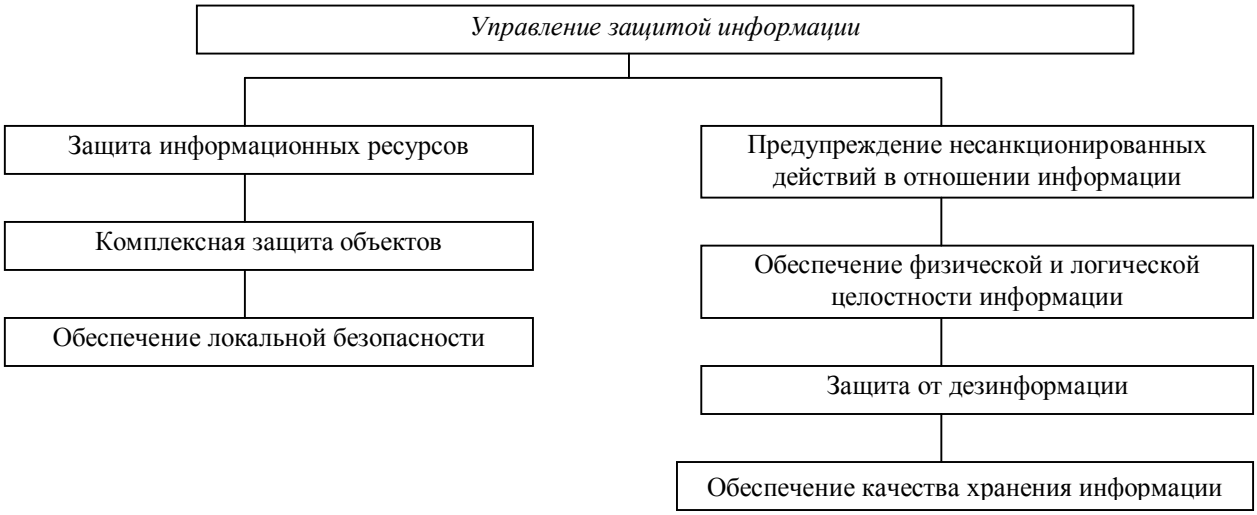

Рис.11

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, накапливанию 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 равномощности рубежей защиты. Равнопрочность подразумевает отсутствие незащищенных участков в рубежах защиты. Равномощность 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

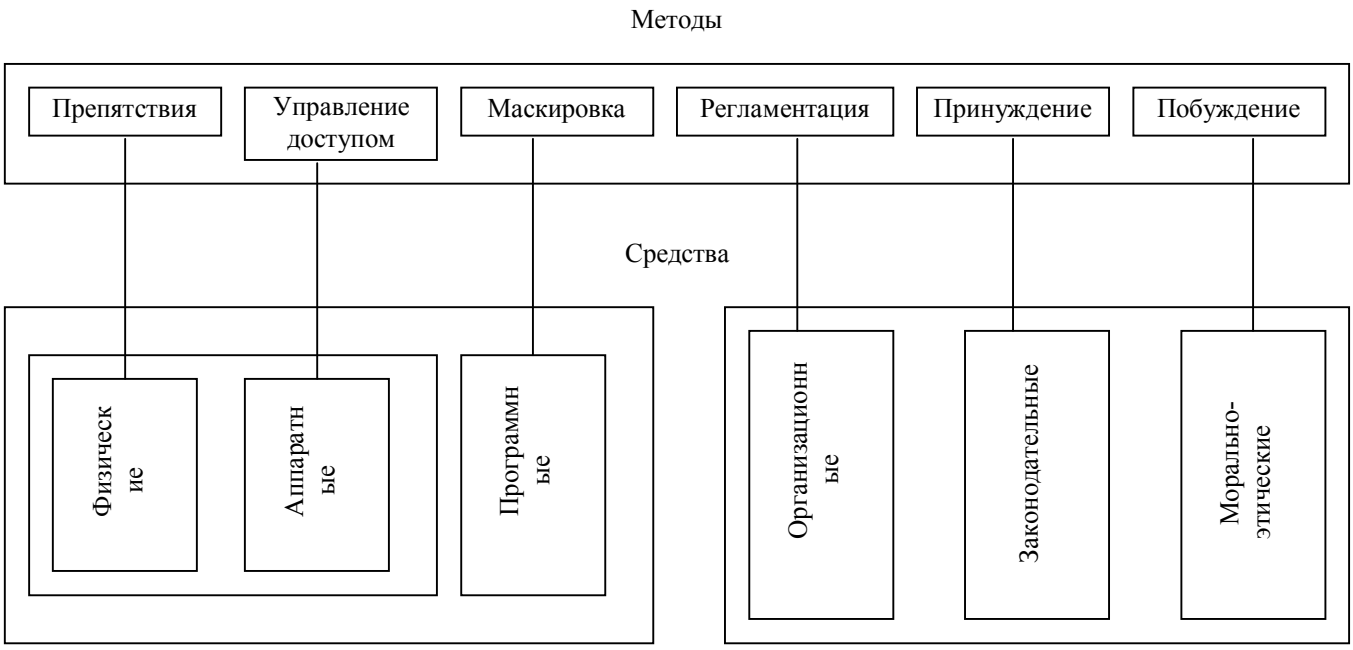

Рис. 12 Методы и средства информационной безопасности экономического объекта

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 криптограммы. 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 ассиметричного 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 подтверждать 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.

3.3 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 документированной 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).

Обеспечение информационной безопасности организации

Таблица 4

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;	Определение перечня документов Осуществление контроля за содержанием документов и степени конфиденциальности содержания Определение реальной степени конфиденциальности сведений, включенных в документ

	– необоснованной рассылки	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 (контролируемо) 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:

1. Выявление возможных каналов утечки.
2. Обнаружение реальных каналов.
3. Оценка опасности реальных каналов.
4. Локализация опасных каналов утечки информации.
5. 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:

1. Безопасных технических средств нет.
2. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.
3. Любой канал утечки информации может быть обнаружен и локализован. «На каждый яд есть противоядие».
4. 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:

1. На этапе проектирования (совершенствования) системы информационной безопасности:

– формирование требований к системе информационной безопасности;

– участие в разработке компонентов и системы информационной безопасности в целом.

2. 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 соблюдение 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).

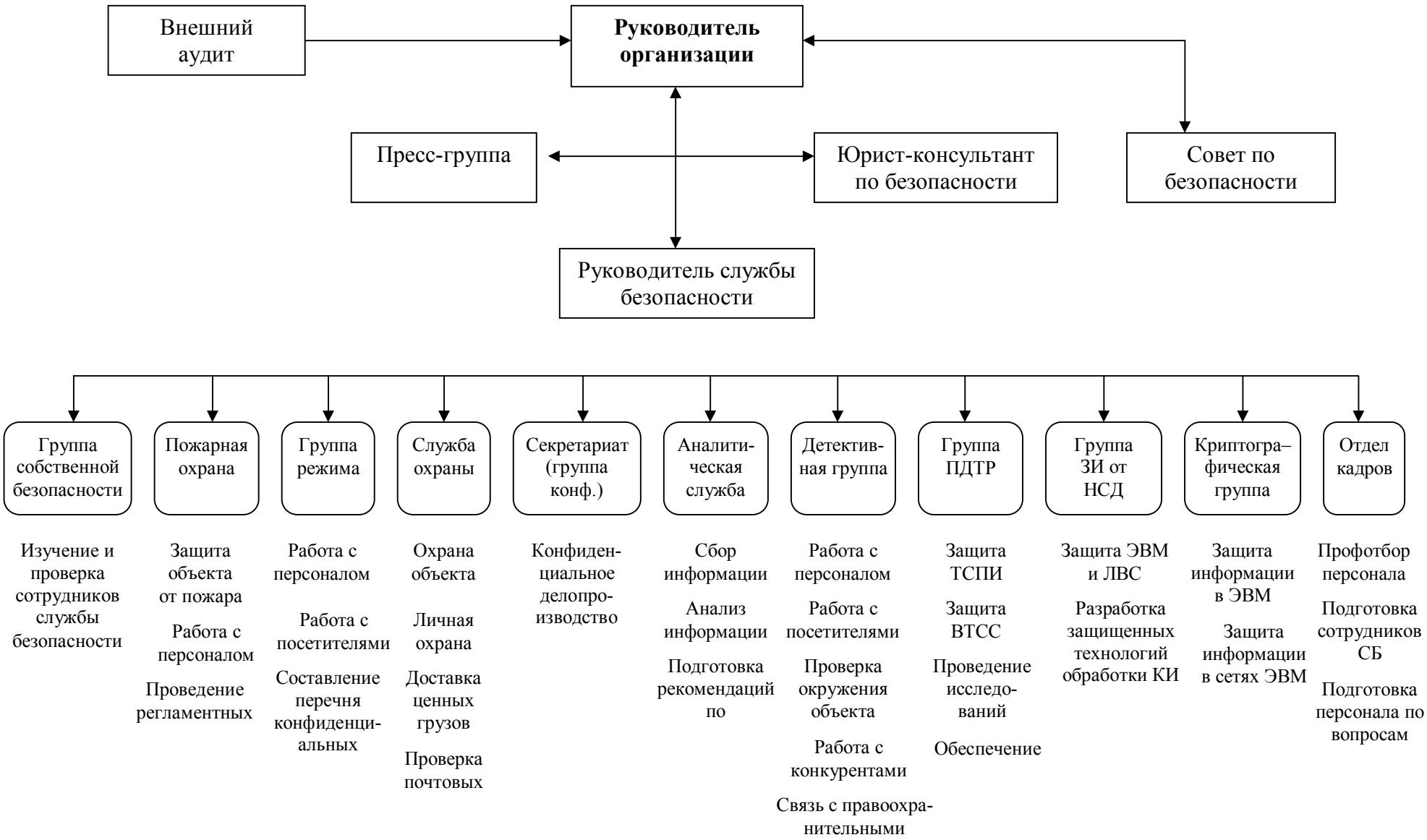

Рис. 14 Структура и задачи службы безопасности

3.4 Защита от компьютерных вирусов

Антивирусы – самый действенный способ борьбы с вирусами. Чтобы противостоять нашествию компьютерных вирусов, необходимо выбрать правильную защиту от них. Одним из способов защиты от вирусов является **резервное копирование**. Поэтому если вы желаете сохранить свои данные – своевременно производите резервное копирование, В случае потери данных, система может быть восстановлена. Другим способом защиты является **правильный выбор программного антивирусного средства**. Сейчас на рынке программного обеспечения представлен достаточно широкий спектр программ для лечения вирусов. Однако не стоит успокаиваться, даже имея какой-либо программный продукт. Появляются все новые и новые вирусы, и это требует периодического обновления антивирусного пакета.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусов;
- специальные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

- копирование информации – создание копий файлов и системных областей диска;
- средства разграничения доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователя.

Общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на три группы:

«сканеры» – антивирусные программы, которые наиболее полно и надежно определяют присутствие вируса, а затем лечат зараженные объекты, удаляя из них тело вируса и восстанавливая объект в первоначальное состояние. Эти программы имеют в своих базах данных от 6000 до 15000 масок вирусов плюс мощный эвристический механизм, который позволяет им находить неизвестные вирусы, вышедшие намного позже, чем сами антивирусные программы;

«ревизоры» – антивирусные программы, которые не имеют в своей базе масок вирусов; они их просто не знают. Но в своей базе данных они хранят наиболее полную информацию о файлах, хранящихся на данном компьютере или локальной сети. Их задача обнаружить вирус, а уже лечением пусть занимаются программы – «сканеры»;

«мониторы» – антивирусные программы, находящиеся в памяти и контролирующие все процессы, происходящие на компьютере. Эти программы не слишком популярны.

Можно привести и более детальную классификацию антивирусных программ:

Детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле па экран выводится соответствующее сообщение.

Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan McAfee Associates и Aidstest

позволяют обнаруживать около 1000, но всего их более пяти тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP, могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова – в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Большинство программ-детекторов имеют функцию «доктора», т.е. пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Большинство программ-докторов умеют «лечить» только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. По некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.

Программы ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей диском (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. **Доктора-ревизоры** – программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменении автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые использую «стандартные», известные на момент написания программы, механизмы заражения файлов.

Существуют также **Программы-фильтры**, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не «ловят» подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Программы-вакцины, или **Иммунизаторы**, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Если первые вирусы, появившиеся на заре компьютерной эры,

распространялись в основном через дискеты с программами, то сегодня они используют преимущественно Всемирную паутину. Причем шанс «подхватить инфекцию» есть не только при выкачивании мегабайтов данных, но и при обычном посещении web-страниц. Но слишком многие завсегдатаи Интернета не озабочены своей безопасностью. Между тем, никогда не следует забывать: чтобы обезопасить себя от вирусной инфекции необходимо придерживаться элементарнейших правил компьютерной гигиены.

В отличие от других стран, где ведущую роль играют глобальные поставщики антивирусов, в России преобладают отечественные разработчики и, прежде всего, «Лаборатория Касперского».

В Приложении № 7 представлена «Сводная таблица известных антивирусных программ» и их характеристики.

На российском рынке антивирусных программ работают три компании: «Лаборатория Касперского», Symantec и «Диалог - Наука».

Наибольшую популярность завоевал пакет AVP, разработанный лабораторией антивирусных систем Касперского. Это универсальный продукт, имеющий версии под самые различные операционные системы.

Антивирус Касперского (AVP) использует все современные типы антивирусной защиты: антивирусные сканнеры, мониторы, поведенческие блокираторы и ревизоры изменений. Различные версии продукта поддерживают все популярные операционные системы, почтовые шлюзы, межсетевые экраны (firewalls), web-серверы. Система позволяет контролировать все возможные пути проникновения вирусов на компьютер пользователя, включая Интернет, электронную почту и мобильные носители круга задач обеспечения безопасности, и обладает рядом специфических свойств.

Концепция AVP позволяет легко и регулярно обновлять антивирусные программы, путем замены антивирусных баз – набора файлов с расширением .AVC, которые на сегодняшний день позволяют обнаруживать и удалять более 50000 вирусов. Обновления к антивирусным базам выходят и доступны с сервера Лаборатории Касперского ежедневно.

Прежде чем переходить к описанию конкретных программных продуктов, предназначенных для защиты компьютеров от вирусов, хотелось бы отметить, что данную проблему нельзя рассматривать в отрыве от общей стратегии информационной безопасности. Здесь весьма уместно провести аналогии с традиционной медициной. Действительно, антивирусное программное обеспечение является лекарством, однако самый лучший способ быть здоровым – это избежать заражения. С этой точки зрения крайне важным является построение комплексной системы, которая бы позволила бы минимизировать возможные пути проникновения вирусов во внутреннюю сеть компании. Это тем более важно, что любое антивирусное программное обеспечение обеспечивает 100% лечение только уже известных вирусов. В то время как новые модификации и, особенно, новые типы вирусов с очень большой вероятностью остаются незамеченными. Частично данная проблема решается при помощи программ для контроля над целостностью данных (типа Kaspersky Inspector), однако они, как правило, лишь констатируют факт несанкционированного изменения файлов, а лечение возможно лишь после появления новых версий антивирусов.

Можно выделить основные источники проникновения вирусов в компьютерную сеть корпорации:

- с гибких носителей;
- с компакт- дисков;
- почты Internet;
- файлов, которые приходят из Internet;
- с рабочих станций;

- почты Intranet.

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!) несёт 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 некоей добавки к документу, который необходимо открыть. Некоторые последние «модели» вирусов вообще физически (т. е. в виде файлов) как бы не существуют: в компьютер передаются по сети определённые 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 создаётся никаких файлов и на жёсткий диск ничего не записывается.

Напомним в очередной раз некоторые аксиомы обращения с файлами (документами), получаемыми на съёмном носителе (дискета, диск CIJ-RO1 и т. п.) или по электронной почте.

- Даже просмотр содержимого вставленной в дисковод дискеты может вызвать заражение компьютера так называемым Boot-вирусом, находящимся в загрузочном секторе дискеты. Сегодня вирусы такого типа в мире встречаются не часто (программы и документы всё реже передаются на дискетах), однако в России иногда всплывают вирусы и двух-, и пятилетней «свежести». Соответственно любые приносимые дискеты, диски должны обязательно проверяться антивирусной программой.
- Не стоит спешить сразу открывать файл, полученный по электронной почте даже от знакомого адресата, но с необычным текстом письма, и тем более уж от незнакомого. Многие современные вирусы умеют сами себя рассылать по всем адресам из адресной книги (найденной в очередном компьютере), вставляя при этом в письмо определённый текст. Создатели вирусов справедливо полагают, что, получив письмо типа «Посмотри, какую замечательную картинку я нашёл в сети!» от хорошо известного корреспондента, человек, не задумываясь, щёлкнет мышкой по прикреплённому файлу. Вполне возможно, что одновременно с запуском программы, заражающей компьютер, вам действительно покажут картинку.
- Следует воздерживаться от «украшательства» своего компьютера всякими с виду безвредными «развлекалочками» (с гуляющими по экрану овечками, распускающимися цветочками, красочными фейерверками и т. п.) – такие небольшие забавные программки часто пишутся для того, чтобы замаскировать вирус. Воистину волк в овечьей шкуре! Например, по России уже второй год ходит небольшая

программа под названием «Новорусские Windows» – многие её поставили и через неделю-две удалили, не подозревая о том, что вирус уже успел похозяйничать в их компьютере. Программа, кстати, всего-навсего меняла названия кнопок в диалоговых окнах, превращая «Нет» в «Нафиг», а «Да» – в «Пофиг». Так что если вам дороги ваши данные и документы, не ставьте на свой компьютер подряд все программы непонятного происхождения и назначения.

- Офисные документы наиболее часто подвергаются заражению в силу интенсивного обмена ими, а также популярности пакета Microsoft Office и лёгкости встраивания в документ вредоносной макрокоманды. Любой пришедший извне офисный документ необходимо проверять антивирусной программой независимо от источника получения, так как автор может и не знать о заражённости своего компьютера. Кстати, весьма распространено заблуждение, что документ в формате RTF не может содержать вирус (в отличие от DOC), оно немало способствовало заражению тысяч компьютеров. Дело в том, что многие макровирусы умеют подменять в заражённом документе расширение *.doc на *.rtf, создавая у получателя документа иллюзию безопасности. Кстати, совсем недавно появился вирус, встроенный в документ формата PDF, что ещё некоторое время назад считалось неосуществимым.
- Не пользуйтесь «пиратскими» сборниками программного обеспечения.
- Самое важное: установите и регулярно обновляйте антивирусный комплект программ, так как, несмотря на развитый интеллект современных средств защиты, гарантированно будут определяться только вирусы, уже включённые в базу данных программы.[*]

[*] Потресов, С. Средство от случайных связей. Бухгалтер и компьютер №9(24) 2001г.

3.5 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. Чтобы этого избежать, ставились на бумаге признаки подлинности: подписи, печати и пр., что в полной мере не гарантировало от несанкционированного доступа к содержанию письма. 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.

Шифрование может быть симметричным и ассиметричным. 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 подписываться 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 подложны данных и пр., т.е. ЭЦП должна

[*] Аналоги в цифре. А. Волоховская. Ж. Бухгалтер и компьютер. №9(60). 2004

быть неотрекаемой. К тому же при рассылке неопределенному кругу лиц получать 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 ассиметричные 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 помешает ему отправлять сообщения от вашего имени.

Самый лучший и надежный способ распространения открытых ключей – воспользоваться услугами сертификационных центров. Сертификационный центр

* Козье Д. Электронная коммерция. Пер. с англ.: М., 1999. с. 68

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 5 проведено сравнение преимуществ и недостатков каждого типа шифрования.[*]

Таблица 5

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 информации (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 блокирован.

Плата со всеми перечисленными возможностями называется устройством криптографической защиты данных – УКЗД.

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность

[*] Козье Д. Электронная коммерция. Пер. с англ.: М., 1999. с. 68

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 распознания «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 велени администратора безопасности ограничивать возможность работы с внешними устройствами: дисководами, CD-ROM и т.д.

Пример 1. Система криптографической защиты информации (СКЗИ) «Верба - OW»

Используемые в СКЗИ "Верба - OW" методы шифрования гарантируют не только высокую секретность, но и эффективное обнаружение искажений или ошибок в передаваемой информации.

Ключ шифрования (ключ связи) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных. В данном случае термин "ключ" означает уникальный битовый шаблон.

При зашифровании сообщения криптографическое преобразование использует ключ. Он используется аналогично обычному ключу, которым запирают дверь, и закрывает сообщение от посторонних глаз. Для расшифрования сообщения нужен соответствующий ключ. Важно ограничить доступ к ключам шифрования, так как любой, кто обладает ключом шифрования, может прочитать зашифрованное сообщение.

В СКЗИ "Верба - OW" используется пара ключей: открытый и секретный ключи шифрования.

В СКЗИ "Верба - OW" используется алгоритм шифрования, основанный на принципе гаммирования, который подразумевает процесс наложения по определенному закону гаммы шифра на открытые данные.

СКЗИ "Верба - OW" является системой с открытым распределением ключей. Каждый пользователь вырабатывает свой секретный ключ, из которого затем с помощью некоторой процедуры формируется открытый ключ. Открытые ключи объединяются в справочник.

В СКЗИ "Верба - OW" ключ зашифрования совпадает с ключом расшифрования. При зашифровании сообщения *i*-ым абонентом для *j*-ого абонента общий секретный ключ связи вырабатывается на основе секретного ключа шифрования *i*-ого абонента и открытого ключа шифрования *j*-ого абонента. Соответственно, для расшифрования этого сообщения *j*-ым абонентом формируется секретный ключ связи на основе секретного ключа шифрования *j*-ого абонента и открытого ключа шифрования *i*-ого абонента. Таким образом, для обеспечения связи с другими абонентами каждому пользователю необходимо иметь:

– собственный секретный ключ шифрования;

– справочник открытых ключей шифрования пользователей сети конфиденциальной связи.

В СКЗИ "Верба - OW" реализована система электронной цифровой подписи на базе криптографического алгоритма, соответствующего ГОСТ Р34.10-94. Секретный ключ подписи используется для выработки электронной цифровой подписи. Только сохранение пользователем в тайне своего секретного ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

Открытый ключ подписи вычисляется как значение некоторой функции от секретного ключа, но знание открытого ключа не дает возможности определить секретный ключ. Открытый ключ может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего в виде отказа его от подписи документа.

При работе с СКЗИ "Верба - OW" каждый пользователь, обладающий правом подписи, самостоятельно формирует личные секретный и открытый ключи подписи. Открытые ключи подписи всех пользователей объединяются в справочники открытых ключей сети конфиденциальной связи.

Каждому пользователю, обладающему правом подписи, необходимо иметь:

– секретный ключ подписи;

– справочник открытых ключей подписи пользователей сети.

В СКЗИ "Верба - OW" реализована система электронной цифровой подписи на базе асимметричного криптографического алгоритма согласно ГОСТ Р34.10-94. Электронная цифровая подпись вырабатывается на основе электронного документа, требующего заверения, и секретного ключа. Согласно стандарту документ «сжимается» с помощью функции хэширования (ГОСТ Р34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»).

При проверке подписи проверяющий должен располагать открытым ключом пользователя, поставившего подпись. Проверяющий должен быть полностью уверен в подлинности открытого ключа (а именно в том, что имеющийся у него открытый ключ соответствует открытому ключу конкретного пользователя). Процедура проверки подписи состоит из вычисления хэш-значения документа и проверки некоторых соотношений, связывающих хэш-значение документа, подпись под этим документом и открытый ключ подписавшего пользователя. Документ считается подлинным, а подпись правильной, если эти соотношения выполняются. В противном случае подпись под документом считается недействительной.

Для разрешения споров между отправителем и получателем информации, связанных с возможностью искажения пересылаемого документа или открытого ключа проверки подписи, достоверная копия этого ключа может выдаваться третьей стороне и применяться им при возникновении конфликта между отправителем и получателем. Наличие у абонента секретного ключа не позволяет ему самому сменить свой номер в сети или выработать подпись под номером другого абонента.

Процедура проверки подписи состоит из вычисления хэш-значения документа и проверки некоторых соотношений, связывающих хэш-значение документа, подпись

под этим документом и открытый ключ подписавшего пользователя. Документ считается подлинным, а подпись правильной, если эти соотношения выполняются. В противном случае подпись под документом считается недействительной.

АРМ Администратора безопасности предназначен для работы с ключевой информацией. Он позволяет:

– на основе исходной ключевой информации, находящейся на лицензионной дискете вырабатывать рабочие ключи (секретные и открытые) шифрования пользователей;

– на основе ключей шифрования формировать секретные и открытые ключи ЭЦП;

– создавать рабочие копии ключевых дискет шифрования и ЭЦП;

– подготавливать ключи шифрования и секретные ключи ЭЦП для хранения на жестком диске.

В СКЗИ "Верба - OW" используются следующие типы носителей ключевой информации:

– ключевой диск для шифрования;

– ключевой диск для подписи;

– совмещенный ключевой диск (с ключами шифрования и подписи) и их рабочие копии.

При создании рабочих копий ключевых дисков необходимо использовать средства СКЗИ "Верба - OW". Полученный с помощью СКЗИ "Верба - OW" рабочий диск не является точной копией исходного, но полностью выполняет его функции. Нельзя создать рабочую копию исходного диска с ключевой информацией простым копированием файлов с исходного ключевого диска.

ПО "Верба - OW" предусматривает возможность хранения секретных ключей на жестком диске, что удобно при частом обращении к ключевой информации.

Смена ключей возможна в следующих ситуациях:

– плановая смена ключей;

– компрометация ключа;

– ввод в действие нового ключа;

– удаление ключа.

Плановую смену ключей рекомендуется производить не реже одного раза в год. При плановой смене ключей, при их компрометации и удалении абонента из сети конфиденциальной связи, все секретные ключи (шифрования и подписи) должны быть уничтожены, а выведенные из действия открытые ключи должны храниться в течение определенного «центром» времени для разбора конфликтных ситуаций. После уничтожения ключевой информации (при компрометации ключа) вводятся в действие резервные ключи. Все изменения должны немедленно отражаться в справочниках ключей и немедленно рассылаться всем абонентам сети.

Пример 2. Система защиты информации «Secret Net 4.0»

Система защиты информации Secret Net устанавливается на рабочем месте администратора безопасности и предоставляет ему следующие возможности:

- централизованное управление защитными механизмами клиентов Secret Net;
- контроль всех событий имеющих отношение к безопасности информационной системы;
- контроль действий сотрудников в ИС организации и оперативное реагирование на факты и попытки НСД;
- планирование запуска процедур копирования ЦБД;
- архивирования журналов регистрации.

Схема управления, реализованная в Secret Net, позволяет управлять информационной безопасностью в терминах реальной предметной области и в полной

мере обеспечить жесткое разделение полномочий администратора сети и администратора безопасности.

Система защиты информации Secret Net выпускается в автономном и сетевом вариантах.

Автономный вариант – состоит только из клиентской части Secret Net и предназначен для обеспечения защиты автономных компьютеров или рабочих станций и серверов сети, содержащих важную информацию.

Сетевой вариант – состоит из клиентской части, подсистемы управления, сервера безопасности и позволяет реализовать защиту, как всех компьютеров сети, так и только тех рабочих станций и серверов, которые ; хранят и обрабатывают важную информацию.

Безопасность рабочих станций и серверов сети обеспечивается с помощью всевозможных механизмов защиты:

- усиленная идентификация и аутентификация,
- полномочное и избирательное разграничение доступа,
- замкнутая программная среда,
- криптографическая защита данных,
- другие механизмы защиты.

Администратору безопасности предоставляется единое средство управления всеми защитными механизмами, позволяющее централизованно управлять и контролировать исполнение требований политики безопасности.

Вся информация о событиях в информационной системе, имеющих отношение к безопасности, регистрируется в едином журнале регистрации. О попытках свершения пользователями неправомерных действий администратор безопасности узнает немедленно.

Существуют средства генерации отчетов, предварительной обработки журналов регистрации, оперативного управления удаленными рабочими станциями.

Система Secret Net состоит из трех компонент:

– клиентская часть;

– сервер безопасности;

– подсистема управления.

Особенностью системы Secret Net является клиент-серверная архитектура, при которой серверная часть обеспечивает централизованное хранение и обработку данных системы защиты, а клиентская часть обеспечивает защиту ресурсов рабочей станции или сервера и хранение управляющей информации в собственной базе данных.

Клиентская часть системы защиты устанавливается на компьютер, содержащий важную информацию, будь то рабочая станция в сети или какой-либо сервер (в том числе и сервер безопасности).Основное назначение клиента Secret Net – защита ресурсов компьютера от несанкционированного доступа и разграничение прав зарегистрированных пользователей. Регистрация событий, происходящих на рабочей станции или сервере сети, передача информации на сервер безопасности. Выполнение централизованных и децентрализованных управляющих воздействий администратора безопасности.

Клиенты Secret Net оснащаются средствами аппаратной поддержки (для идентификации пользователей по электронным идентификаторам и управления загрузкой с внешних носителей).

Сервер безопасности. Сервер безопасности устанавливается на выделенный компьютер и обеспечивает решение следующих задач:

– ведение центральной базы данных системы защиты, функционирующую под управлением СУБД Oracle 8.0 Personal Edition и содержащую информацию, необходимую для работы системы защиты;

– сбор информации о происходящих событиях со всех клиентов Secret Net в

единый журнал регистрации и передача обработанной информации подсистеме управления;

– взаимодействие с подсистемой управления и передача управляющих команд администратора на клиентскую часть системы защиты.

Основными сферами применения системы Secret Net являются:

– защита информационных ресурсов;

– централизованное управление информационной безопасностью;

– контроль состояния информационной безопасности.

Система защиты информации Secret Net 4.0 сертифицирована Гостехкомиссией России по 3 классу защищенности. Это означает, что Secret Net 4.0 можно применять для защиты информации, содержащей сведения, составляющие государственную тайну.

Электронный замок «Соболь»/«Соболь-PCI» может применяться в составе системы защиты информации Secret Net для генерации ключей шифрования и электронно-цифровой подписи. Кроме того, при использовании электронного замка в составе Secret Net обеспечивается единое централизованное управление его возможностями. С помощью подсистемы управления Secret Net администратор безопасности имеет возможность управлять статусом персональных идентификаторов сотрудников: присваивать электронные идентификаторы, временно блокировать, делать их недействительными, что позволяет управлять доступом сотрудников к компьютерам автоматизированной системы организации.

Электронные замки «Соболь-PCI» и «Соболь» разработаны научно-инженерным предприятием «ИНФОРМЗАЩИТА» и предназначены для защиты ресурсов компьютера от несанкционированного доступа.

Электронные замки «Соболь» и «Соболь-PCI» сертифицированы Федеральным агентством правительственной связи и информации России. Сертификаты ФАПСИ № СФ/122-0305 и № СФ/022-0306 от 10.02.2000, а также и сертификат № СФ/527-0553 от 01.07.2002 позволяют применять данные средства для защиты информации, составляющую коммерческую или государственную тайну.

Электронный замок «Соболь»/Соболь-PCI» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети.

Система защиты электронный замок «Соболь»/«Соболь- PCI» обладает следующими возможностями:

– идентификация и аутентификация пользователей;

– регистрация попыток доступа к ПЭВМ;

– запрет загрузки ОС со съемных носителей.

Идентификация и аутентификация пользователей. Каждый пользователь компьютера регистрируется в системе электронный замок «Соболь»/«Соболь- PCI», установленной на данном компьютере. Регистрация пользователя осуществляется администратором и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора и назначении пароля.

Действие электронного замка «Соболь»/«Соболь- PCI» состоит в проверке персонального идентификатора и пароля пользователя при попытке входа в систему. В случае попытки входа в систему не зарегистрированного пользователя электронный замок «Соболь» регистрирует попытку несанкционированного доступа (НСД) и осуществляется аппаратная блокировка.

Регистрация попыток доступа к ПЭВМ. Электронный замок «Соболь»/«Соболь-PCI» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Электронный замок фиксирует в системном журнале вход пользователей, попытки входа, попытки НСД и другие события, связанные с безопасностью системы. В системном журнале хранится

следующая информация: дата и время события, имя пользователя и информация о типе события, *например*:

- факт входа пользователя;
- введение неправильного пароля;
- предъявление не зарегистрированного идентификатора пользователя;
- превышение числа попыток входа в систему.

Таким образом, электронный замок «Соболь» предоставляет информацию администратору о всех попытках доступа к ПЭВМ.

Контроль целостности программной среды и запрет загрузки со съемных носителей. Подсистема контроля целостности расширяет возможности электронного замка «Соболь»/«Соболь-PCI». Контроль целостности системных областей дисков и наиболее критичных файлов производится по алгоритму ГОСТ 28147-89. Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов.

Подсистема запрета загрузки с гибкого диска и CD ROM диска обеспечивает запрет загрузки операционной системы с этих съемных носителей для всех пользователей компьютера, кроме администратора. Администратор может разрешить отдельным пользователям компьютера выполнять загрузку операционной системы со съемных носителей.

Для настройки электронного замка «Соболь» администратор имеет возможность:

- определять минимальную длину пароля пользователя;
- определять предельное число неудачных входов пользователя;
- добавлять и удалять пользователей;
- блокировать работу пользователя на компьютере;
- создавать резервные копии персональных идентификаторов.

Возможности и преимущества электронного замка «Соболь»/ «Соболь-PCI»:

- самая низкая по сравнению с аналогичными продуктами цена – 190 долларов «Соболь» для стандарта ISA и 230 долларов «Соболь- PCI»;
- наличие датчика случайных чисел;
- простота установки, настройки и администрирования;
- современная элементная база, обеспечивающая высокую надежность и долговечность;
- возможность установки в любой IBM-совместимый персональный компьютер, имеющий свободный разъем стандарта ISA или PCI.

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 становиться 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 становиться 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, a 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 Proxy 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 немение, 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 Ithernet 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 подсетки 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, по-скольку 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 (Sycure 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 разобщенным офисам одной корпорации, а также партнерам, образующим виртуальное предприятие, безопасно обмениваться данными по Интернету.

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 мультипользовательских 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 производится 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:

1. Для определения, общих правил обработки информации в АИС, целей построения и функционирования системы защиты и подготовки сотрудников.
2. Для фиксирования на некоторый момент времени состава АИС, технологии обработки информации, средств защиты информации.
3. 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:

1. Политика безопасности.
2. Текущее состояние системы.
3. Рекомендации по реализации системы защиты.
4. Ответственность персонала.
5. Порядок ввода в действие средств защиты.
6. 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:

1. Цели, преследуемые реализацией системы защиты в вычислительной системе (например, защита данных компании от несанкционированного доступа, защита от утери данных и др.).

2. Меры ответственности средств защиты и нижний уровень гарантированной защиты (например, в работе небольших групп защищенных компьютеров, в обязанностях каждого из служащих и др.).

3. 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:

1. Пользователь персонального компьютера или терминала несет ответственность за физическую целостность компьютера (терминала) во время сеанса работы с АИС, а также за неразглашение собственного пароля.

2. Администратор баз данных несет ответственность за конфиденциальность информации в базах данных, ее логическую непротиворечивость и целостность.

3. 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:

1. 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.

2. Если избежать какого-либо нарушения невозможно, необходимо уменьшить вероятность его появления или смягчить последствия от него.

3. 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.

4. 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:

1. 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).

2.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.

3. 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.

4. 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.

5. 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:

1. 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.

2. 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 - непременное 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.

4.2 Политика 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 решении, 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.

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.

Последний принцип - всеобщая поддержка 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.

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 проникновении 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 достаточна 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.

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 опосредовано, 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 TCO, 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:

$$NP = \frac{CF_i}{(1+r)^n} - CF_0 \qquad (1)$$

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 TCO 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.

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 дисковода 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 угроз	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. обращаема 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.

В силу этих обстоятельств к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации.

В 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:

1. От чего надо защищать систему?
2. Что надо защищать в самой системе?
3. 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 и 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 и непрерывно.

В 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 и 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 и 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).

1. 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).

2. Защита от несанкционированного копирования и распространения программ и 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 комъюнити (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 к 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 оборотная 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 подвергнуться 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.

В 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 полуторамиллиардной 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.

В 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.

В 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, опасающихся 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.

В 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 отплате 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 смысл 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.

Основный 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 следующи:

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.

Заключение

Проблема информационной безопасности экономических объектов многоаспектна и нуждается в дальнейшей проработке.

В современном мире информатизация становится стратегическим национальным ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства повлекли помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной инфраструктуры, пропорционально растет потенциальная уязвимость экономики по отношению к информационным воздействиям.

Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. С позиций системного подхода к защите информации необходимо использовать весь арсенал имеющихся средств защиты во всех структурных элементах экономического объекта и на всех этапах технологического цикла обработки информации. Методы и средства защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам. Эффективность информационной безопасности означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз. Планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации. Необходима четкость в осуществлении полномочий и прав пользователей на доступ к определенным видам информации, в обеспечении контроля средств защиты и немедленного реагирования на их выход из строя.

Приложение 1

ФЕДЕРАЛЬНЫЙ ЗАКОН
от 20 февраля 1995 г. № 24–ФЗ
"Об информации, информатизации и защите информации"
Принят Государственной думой 25 января 1995 года

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Об участии России в международном информационном обмене см. Федеральный закон от 4 июля 1996 г. № 85-ФЗ.

Статья 1. *Сфера действия настоящего Федерального закона*

1. Настоящий Федеральный закон регулирует отношения, возникающие при:
формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;

создании и использовании информационных технологий и средств их обеспечения;
защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

2. Настоящий Федеральный закон не затрагивает отношений, регулируемых Законом Российской Федерации "Об авторском праве и смежных правах".

Статья 2. *Термины, используемые в настоящем Федеральном законе, их определения*

В настоящем Федеральном законе используются следующие понятия:
информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
информатизация – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;

документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
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;
информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
средства обеспечения автоматизированных информационных систем и их технологий – программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики: положения, уставы; должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;
собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;
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.

Статья 3. *Обязанности государства в сфере формирования информационных ресурсов и информатизации*

Об основах государственной политики в сфере информатизации см. Указ Президента РФ от 20 января 1994 г. № 170.

1. Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации.

2. Основными направлениями государственной политики в сфере информатизации являются:
обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы:
формирование и защита государственных информационных ресурсов;
создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;
создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;
обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;
содействие формированию рынка информационных ресурсов, услуг, информационных

систем, технологий, средств их обеспечения;
формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;
поддержка проектов и программ информатизации;
создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;
развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

ГЛАВА 2. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

Статья 4. *Основы правового режима информационных ресурсов*

1. Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

2. 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.

Статья 5. *Документирование информации*

1. Документирование информации является обязательным условием включения информации в информационные ресурсы. Документирование информации осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов, безопасность Российской Федерации.

2. Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством Российской Федерации.

3. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.
Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.
4. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Статья 6. *Информационные ресурсы как элемент состава имущества и объект права собственности*

1. Информационные ресурсы могут быть и негосударственными и как элемент состава

имущества находиться в собственности граждан, органов государственной власти, органов местного самоуправления, организаций общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются гражданским законодательством Российской Федерации.

2. Физические и юридические лица являются собственниками тех документов, массивов документом, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

3. Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных законом способов.
Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне. Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.
4. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо от их организационно-правовой формы и форм собственности, а также гражданами на основании статьи 8 настоящего Федерального закона, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

5. Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

6. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.

См. Положение о порядке учета архивных документов при приватизации государственного и муниципального имущества, утвержденное распоряжением Госкомимущества РФ от 22 октября 1996 г. № 1131-р, приказом Росархива от 6 ноября 1996 г. № 54.

7. Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право:
назначить лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими:

устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

определять условия распоряжения документами при их копировании и распространении.
8. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и

режим производной продукции, создаваемой в этом случае, регулируются договором.

Статья 7. ***Государственные информационные ресурсы***

1. Государственные информационные ресурсы Российской Федерации формируются в соответствии со сферами ведения как:

федеральные информационные ресурсы;

информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации (далее – информационные ресурсы совместного ведения);
информационные ресурсы субъектов Российской Федерации.

2. Формирование государственных информационных ресурсов в соответствии с пунктом 1 статьи 8 настоящего Федерального закона осуществляется гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениями.

Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации формируют государственные информационные ресурсы, находящиеся в их ведении, и обеспечивают их использование в соответствии с установленной компетенцией.

3. Деятельность органов государственной власти и организаций по формированию федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации финансируется из федерального бюджета и бюджетов субъектов Российской Федерации по статье расходов "Информатика" ("Информационное обеспечение").

4. Организации, которые специализируются на формировании федеральных информационных ресурсов и (или) информационных ресурсов совместного ведения на основе договора, обязаны получить лицензию на этот вид деятельности в органах государственной власти. Порядок лицензирования определяется законодательством Российской Федерации.

Статья 8. ***Обязательное представление документированной информации для формирования государственных информационных ресурсов***

1. Граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов.

Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство Российской Федерации.

2. Порядок и условия обязательного представления документированной информации доводятся до сведения граждан и организаций.

Порядок обязательного представления (получения) информации, отнесенной к государственной тайне, и конфиденциальной информации устанавливается и осуществляется в соответствии с законодательством об этих категориях информации.

3. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).

Необеспечение регистрационными органами регистрируемых юридических лиц перечнем представляемых в обязательном порядке документов с адресами их представления не является основанием для отказа в регистрации. Должностные лица регистрационных органов, виновные в необеспечении регистрируемых юридических лиц перечнями представляемых в обязательном порядке документов с адресами их представления привлекаются к дисциплинарной ответственности вплоть до снятия с должности.

4. Документы, принадлежащие физическим и юридическим лицам, могут включаться по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

Статья 9. ***Отнесение информационных ресурсов к общероссийскому национальному достоянию***

1. Отдельные объекты федеральных информационных ресурсов могут быть объявлены общероссийским национальным достоянием.

2. Отнесение конкретных объектов федеральных информационных ресурсов к общероссийскому национальному достоянию и определение их правового режима устанавливаются Федеральным законом.

Статья 10. ***Информационные ресурсы по категориям доступа***

1. Государственные информационные ресурсы Российской Федерации являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

О степенях секретности сведений см.: Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне", постановление Правительства РФ от 4 сентября 1995 г. № 870.

2. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

3. Запрещено относить к информации с ограниченным доступом:

законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением отнесенных к государственной тайне;

документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

4. Отнесение информации к государственной тайне осуществляется в соответствии с

Законом Российской Федерации "О государственной тайне".
5. Отнесение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации, за исключением случаев, предусмотренных статьей 11 настоящего Федерального закона.

Статья 11. ***Информация о гражданах (персональные данные)***

1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне Федерального закона. Персональные данные относятся к категории конфиденциальной информации.

Согласно Федеральному закону от 15 ноября 1997 г. № 143-ФЗ сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными.

О сборе, хранении, использовании и распространении информации о частной жизни см. Конституцию РФ от 12 декабря 1993 г.

См. Временный перечень сведений, составляющих конфиденциальную информацию в Пенсионном фонде Российской Федерации, утвержденный постановлением Правления ПФР от 30 августа 1996 г. № 123.
Перечень сведений конфиденциального характера утвержден Указом Президента РФ от 6 марта 1997 г. № 188.

Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

2. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
4. Подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных. Порядок лицензирования определяется законодательством Российской Федерации.
5. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 настоящего Федерального закона и законодательства о персональных данных.

ГЛАВА 3. ПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

Статья 12. *Реализация права на доступ к информации из информационных ресурсов*

1. Пользователи – граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения – обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцами этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

2. Владельцы информационных ресурсов обеспечивают пользователей (потребителей) информацией из информационных ресурсов на основе законодательства, уставов указанных органов и организаций, положений о них, а также договоров на услуги по информационному обеспечению.

См. Федеральный закон от 19 июля 1998 г. № 113-ФЗ "О гидрометеорологической службе" и Положение об информационных услугах в области гидрометеорологии и мониторинга загрязнения окружающей природной среды, утвержденное постановлением Правительства РФ от 15 ноября 1997 г. № 1425.

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации.

Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов.

3. Порядок получения пользователем информации (указание места, времени, ответственных должностных лиц, необходимых процедур) определяет собственник или владелец информационных ресурсов с соблюдением требований, установленных настоящим Федеральным законом.

Перечни информации и услуг по информационному обеспечению, сведения о порядке и условиях доступа к информационным ресурсам владельцы информационных ресурсов и информационных систем предоставляют пользователям бесплатно.

4. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, обеспечивают условия для оперативного и полного предоставления пользователю документированной информации в соответствии с обязанностями, установленными уставами (положениями) этих органов и организаций.

5. Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные вид и массивы информации, в соответствии с их компетенцией, либо непосредственно ее собственником в соответствии с законодательством.

Статья 13. Гарантии предоставления информации

1. Органы государственной власти и органы местного самоуправления создают доступные для каждого информационные ресурсы по вопросам деятельности этих органов и подведомственных им организаций, а также в пределах своей компетенции осуществляют массовое информационное обеспечение пользователей по вопросам прав, свобод и обязанностей граждан, их безопасности и другим вопросам, представляющим общественный интерес.
2. Отказ в доступе к информационным ресурсам, предусмотренным в пункте 1 настоящей статьи, может быть обжалован в суде.

3. Комитет при Президенте Российской Федерации по политике информатизации организует регистрацию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения права граждан на доступ к информации.

О государственном учете и регистрации баз и банков данных см. постановление Правительства РФ от 28 февраля 1996 г. № 226.

4. Перечень информационных услуг, предоставляемых пользователям из государственных информационных ресурсов бесплатно или за плату, не возмещающую в полном размере расходы на услуги, устанавливает Правительство Российской Федерации.

Расходы на указанные услуги компенсируются из средств федерального бюджета и бюджетов субъектов Российской Федерации.

Статья 14. *Доступ граждан и организаций к информации о них*

1. Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных федеральными законами.

2. Владелец документированной информации о гражданах обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается. Ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации.
3. Субъекты, представляющие информацию о себе для комплектования информационных ресурсов на основании статей 7 и 8 настоящего Федерального закона, имеют право бесплатно пользоваться этой информацией.
4. Отказ владельца информационных ресурсов субъекту в доступе к информации о нем может быть обжалован в судебном порядке.

Статья 15. *Обязанности и ответственность владельца информационных ресурсов*

1. Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных законодательством Российской Федерации или собственником этих информационных ресурсов, в соответствии с законодательством.

2. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

ГЛАВА 4. ИНФОРМАТИЗАЦИЯ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ТЕХНОЛОГИИ И СРЕДСТВА ИХ ОБЕСПЕЧЕНИЯ

Статья 16. *Разработка и производство информационных систем, технологий и средств их обеспечения*

1. Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

2. Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

3. Государство создает условия для проведения научно-исследовательских и опытно-конструкторских работ в области разработки и производства информационных систем, технологий и средств их обеспечения.

Правительство Российской Федерации определяет приоритетные направления развития информатизации и устанавливает порядок их финансирования.

4. Разработка и эксплуатация федеральных информационных систем финансируются из средств федерального бюджета по статье расходов "Информатика" ("Информационное обеспечение").

5. Органы государственной статистики совместно с Комитетом при Президенте Российской Федерации по политике информатизации устанавливают правила учета и анализа состояния отрасли экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

Статья 17. *Право собственности на информационные системы, технологии и средства их обеспечения*

1. Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства.

2. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

3. Информационные системы, технологии и средства их обеспечения включаются в состав имущества субъекта, осуществляющего права собственника или владельца этих объектов. Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков.

Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

Статья 18. *Право авторства и право собственности на информационные системы, технологии и средства их обеспечения*

Право авторства и право собственности на информационные системы, технологии и

средства их обеспечения могут принадлежать разным лицам.

О защите авторских и смежных прав см. также Закон РФ от 9 июля 1993 г. М 5351-1 "Об авторских правах".

Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством Российской Федерации.

Статья 19. *Сертификация информационных систем, технологий, средств их обеспечения и лицензирование деятельности по формированию и использованию информационных ресурсов*

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".
2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.
3. Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.
4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

ГЛАВА 5. ЗАЩИТА ИНФОРМАЦИИ И ПРАВ СУБЪЕКТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ИНФОРМАТИЗАЦИИ

Статья 20. *Цели защиты*

Целями защиты являются:

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;
предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Статья 21. ***Защита информации***

1. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:
в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
в отношении персональных данных – Федеральным законом.
2. Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации.

3. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации.

4. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.
5. Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.
6. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

О защите информации, которой обмениваются Российская Федерация и НАТО, см. постановление Правительства РФ от 3 марта 1997 г. № 242

Статья 22. ***Права и обязанности субъектов в области защиты информации***

1. Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.
2. Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных

систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Статья 23. *Защита прав субъектов в сфере информационных процессов и информатизации*

1. Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.
2. Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.
3. За правонарушения при работе с документированной информацией органы государственной власти организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и субъектов Российской Федерации.

Для рассмотрения конфликтных ситуаций и защиты прав участников в сфере формирования использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения могут создаваться временные и постоянные третейские суды.

Третейский суд рассматривает конфликты и споры сторон в порядке, установленном законодательством о третейских судах.

4. Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств и обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

Статья 24. *Защита права на доступ к информации*

1. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке. Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли-продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

2. Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях

необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.
3. Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Статья 25. ***Вступление в силу настоящего Федерального закона***

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Предложить Президенту Российской Федерации привести в соответствие с настоящим Федеральным законом изданные им правовые акты.

3. Поручить Правительству Российской Федерации: привести в соответствие с настоящим Федеральным законом изданные им правовые акты; подготовить и внести в Государственную думу в трехмесячный срок в установленном порядке предложения о внесении изменений и дополнений в законодательство Российской Федерации в связи с принятием настоящего Федерального закона; принять нормативные правовые акты, обеспечивающие реализацию настоящего Федерального закона.

Президент Российской Федерации *Б. Ельцин*

Москва, Кремль
20 февраля 1995 года № 24-ФЗ

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА от 6 марта 1997 г. № 188

В целях дальнейшего совершенствования порядка опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти постановляю:
Утвердить прилагаемый Перечень сведений конфиденциального характера.

Президент Российской Федерации
Б. ЕЛЬЦИН

Утвержден
Указом Президента
Российской Федерации
от 6 марта 1997 г. № 188

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Приложение 3

ДОКТРИНА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

(Утверждена Президентом Российской Федерации 9 сентября 2000 года)

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая 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.

Настоящая Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения

информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий

для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих с научно-технического и духовного потенциала Российской Федерации

обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту чести и своего доброго имени;

укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

гарантировать свободу массовой информации и запрет цензуры;

не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и

иностранных граждан;

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Для достижения этого требуется:

развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

В этих целях 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 Российской Федерации, 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 и 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 Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и

общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию. духовному возрождению России могут являться:

принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;

противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

противоправные сбор и использование информации;

нарушения технологии обработки информации;

внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

компрометация ключей и средств криптографической защиты информации;

утечка информации по техническим каналам;

внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

использование несертифицированных отечественных и зарубежных

информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

несанкционированный доступ к информации, находящейся в банках и базах данных;

нарушение законных ограничений на распространение информации.

3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

Стремление ряда стран к доминированию и ущемлению интересов России в мировом и информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

Обострение международной конкуренции за обладание информационными технологиями и ресурсами;

деятельность международных террористических организаций;

Увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию создания конкурентоспособных российских технологий

Деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств

Разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получения несанкционированного доступа к ним.

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере;

недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

недостаточная экономическая мощь государства;

снижение эффективности системы образования и воспитания, недостаточное

количество квалифицированных кадров в области обеспечения информационной безопасности;

недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации

конкурентоспособных российских информационных агентств и средств массовой информации.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы. Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией ной политики;

развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления,

оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;

разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;

разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;

совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;

установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;

координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации,

развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономическою развития России и реальности угроз применения «информационного оружия»;

разработка и создание механизмов формирования и реализации государственной информационной политики России;

разработка! методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются:

внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации;

законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;

создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются.

создание и совершенствование системы обеспечения информационной безопасности Российской Федерации,

усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

разработка, использование и совершенствование средств защиты информации и

методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;

формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

В сфере экономики. Обеспечение информационной безопасности Российской Федерации в сфере экономики играет ключевую роль в обеспечении национальной безопасности Российской Федерации

Воздействию угроз информационной безопасности Российской Федерации в

сфере экономики наиболее подвержены:

система государственной статистики;

кредитно-финансовая система;

информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

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.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур - производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости России от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

Основными мерами по обеспечению информационной безопасности Российской Федерации 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 передами экономической информации.

В сфере внутренней политики. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

конституционные права и свободы человека и гражданина;

конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

В сфере внешней политики. К наиболее важным объектам обеспечения информационной безопасности Российской Федерации в сфере внешней политики относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации

при международных организациях,

информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

распространение за рубежом дезинформации о внешней политике Российской Федерации;

нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

информационно-пропагандистская деятельность политических сил общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

недостаточная информированность населения о внешнеполитической деятельности Российской Федерации.

Основными мероприятиями по обеспечению информационной безопасности Российской Федерации в сфере внешней политики являются:

разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Российской Федерации;

разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Российской Федерации;

совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

совершенствование информационного обеспечения субъектов Российской

Федерации по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

В области науки и техники. Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

научно-технические кадры и система их подготовки;

системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими).

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств - участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

сохраняющуюся сложную экономическую ситуацию в России, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

неспособность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;

серьезные проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;

сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Российской Федерации в области науки и техники - это совершенствование

законодательства Российской Федерации, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Российской Федерации в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

В сфере духовной жизни. Обеспечение информационной безопасности Российской Федерации в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния всех народов России, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Российской Федерации, обеспечения обороноспособности и безопасности государства.

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;

свобода массовой информации;

неприкосновенность частной жизни, личная и семейная тайна;

русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств - участников Содружества Независимых Государств;

языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;

объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве,

ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

неспособность современного гражданского общества России обеспечить

формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:

развитие в России основ гражданского общества;

создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу;

совершенствование законодательства Российской Федерации, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей Российской Федерации;

формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности федеральных органов государственной власти и общественных объединений, обеспечение достоверности сведении о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей Российской Федерации, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах. Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств зашиты информации и контроля их эффективности;

привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

лицензирование деятельности организаций в области защиты информации;

аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

введение территориальных, частотных, энергетических, пространственных и

временных ограничений в режимах использования технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны. К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Российской Федерации в сфере обороны, являются:

все виды разведывательной деятельности зарубежных государств;

информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;

преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны являются:

систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;

проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;

постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;

совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах. К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасное для указанных объектов, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического статистического характера;

отказ технических средств и сбои программного обеспечения в и формационных и телекоммуникационных системах;

преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

Наряду с широко используемыми общими методами и средства; защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;

повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций. Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях: к приведению в движение больших масс людей, испытывающих психический стресс;

к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;

повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;

прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;

разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Международное сотрудничество Российской Федерации в области об печения информационной безопасности - неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Особенность международного сотрудничества Российской Федерации в области

обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики, противодействия укреплению роли России как одного из влиятельных центр формирующегося многополярного мира, усиления технологического отрыва ведущих держав мира и наращивания их возможностей для здания «информационного оружия». Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

запрещение разработки, распространения и применения «информационного оружия»;

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами - участниками Содружества Независимых Государств.

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

III. ОСНОВНЫЕ ПОЛОЖЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПЕРВООЧЕРЕДНЫЕ МЕРОПРИЯТИЯ ПО ЕЕ РЕАЛИЗАЦИИ

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах:

соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;

приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;

организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;

поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

формулирует и реализует государственную информационную политику России;

организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;

способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации. Это предполагает:

оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

создание организационно-правовых механизмов обеспечения информационной безопасности;

определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства Российской Федерации в данной сфере;

создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;

разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;

совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации.

Правовое обеспечение информационной безопасности Российской Федерации должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Разработка механизмов правового обеспечения информационной безопасности Российской Федерации включает в себя мероприятия по информатизации правовой сферы в целом.

В целях выявления и согласования интересов федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и других субъектов отношений в. информационной сфере, выработки необходимых решений государство поддерживает формирование общественных советов, комитетов и комиссий с широким представительством общественных объединений и содействует организации их эффективной работы.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации

Первоочередными мероприятиями по реализации государственной политики

обеспечения информационной безопасности Российской Федерации являются:

разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;

разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;

принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;

развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;

гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

IV. ОРГАНИЗАЦИОННАЯ ОСНОВА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

10. Основные функции системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии; создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимают соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством. Российской Федерации формирует, реорганизует и упраздняет подчиненные органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации настоящей Доктрины.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения

информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

* * *

Реализация первоочередных мероприятий по обеспечению информационной безопасности Российской Федерации, перечисленных в настоящей Доктрине, предполагает разработку соответствующей федеральной программы. Конкретизация некоторых положений настоящей Доктрины применительно к отдельным сферам деятельности общества и государства может быть осуществлена в соответствующих документах, утверждаемых Президентом Российской Федерации.

Приложение 4

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РСФСР

О ПЕРЕЧНЕ СВЕДЕНИЙ, КОТОРЫЕ НЕ МОГУТ СОСТАВЛЯТЬ КОММЕРЧЕСКУЮ ТАЙНУ от 5 декабря 1991 г. № 35

В целях обеспечения деятельности государственной налоговой службы правоохранительных и контролирующих органов, а также предупреждения злоупотреблений в процессе приватизации Правительство РСФСР постановляет:

1. Установить, что коммерческую тайну предприятия и предпринимателя не могут составлять:

учредительные документы (решение о создании предприятия или до-договор учредителей) и Устав;

документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);

сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

документы о платежеспособности;

сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

документы об уплате налогов и обязательных платежах;

сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

2. Запретить государственным и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

о размерах имущества предприятия и его денежных средствах;

о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;

о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;

о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

3. Предприятия и лица, занимающиеся предпринимательской деятельностью, руководители государственных и муниципальных предприятий обязаны представлять сведения, перечисленные в пунктах 1 и 2 настоящего Постановления, по требованию органов власти, управления, контролирующих и правоохранительных органов, других юридических лиц, имеющих на это право в соответствии с законодательством РСФСР, а также трудового коллектива предприятия.

4. Действие настоящего Постановления не распространяется на сведения, относимые в соответствии с международными договорами к коммерческой тайне, а также на сведения о деятельности предприятия, которые в соответствии с действующим

законодательством составляют государственную тайну.

Б. ЕЛЬЦИН

Приложение 5

«УТВЕРЖДАЮ»
Руководитель аппарата
Государственной думы
Н.Н. Трошкин
2.03.1999 г.

ОСНОВНЫЕ НАПРАВЛЕНИЯ обеспечения надежности обработки, хранения и передачи информации в компьютерной сети Государственной думы Федерального собрания Российской Федерации

1. Введение

Назначением Основных направлений является выработка организационных и технологических мер по обеспечению надежности (безопасности) обработки, хранения и передачи информации.
Настоящие Основные направления определяют способы взаимодействия пользователей компьютерной сети и должностных лиц, обеспечивающих ее функционирование, а также процедуры, предотвращающие или реагирующие на нарушения безопасности.
В Основных направлениях сформулированы обязанности и ответственность пользователей компьютерной сети и должностных лиц, участвующих во взаимодействии.
Основные направления являются основой для иных нормативных документов, регламентирующих порядок функционирования компьютерной сети.
Положения Основных направлений распространяются на всех пользователей: депутатов Государственной думы и их помощников, работников аппарата, а также представителей внешних организаций, подключенных к компьютерной сети (в том числе и с помощью средств удаленного доступа) в установленном порядке. Требования Основных направлений распространяются также на представителей всех внешних организаций, обслуживающих отдельные элементы компьютерной сети Государственной думы на договорной основе или на основе иных документов, регламентирующих распределение обязанностей.

2. Обязанности и ответственность

За реализацию Основных направлений и иных нормативных документов, разработанных на их основе (далее требований безопасности) в Государственной думе отвечают:
– *руководитель структурного подразделения*. Он отвечает за доведение требований безопасности до пользователей структурного подразделения и организацию работ по их выполнению;

– *координатор безопасности* (начальник отдела компьютерной сети и систем передачи данных Управления информационно-технологического обеспечения, назначается руководителем аппарата Государственной думы). Он отвечает за реализацию и развитие Основных направлений, разработку на их основе иных нормативных документов, координацию работ и контроль за выполнением требований безопасности системным администратором компьютерной сети, администраторами локальных вычислительных сетей и информационных технологий и пользователями;

– *системный администратор компьютерной сети* (работник отдела компьютерной

сети и систем передачи данных УИТО, назначается руководителем аппарата Государственной думы по представлению начальника УИТО и подчиняется непосредственно координатору безопасности). Он осуществляет свою деятельность в соответствии с "Положением о службе главного администратора компьютерной сети Государственной думы" и отвечает за выполнение требований безопасности в рамках всей компьютерной сети;
– *администратор локальной вычислительной сети* (ЛВС) *структурного подразделения* (работник аппарата структурного подразделения, назначается руководителем аппарата Государственной думы по представлению руководителя структурного подразделения). Он осуществляет свою деятельность в соответствии с "Положением об администраторе локальной вычислительной сети структурного подразделения Государственной думы" и отвечает за выполнение требований безопасности в рамках ЛВС структурного подразделения. В каждом структурном подразделении может функционировать несколько ЛВС;
– *администратор информационной технологии* (ИТ) (работник аппарата структурного подразделения, назначается руководителем структурного подразделения). Он осуществляет свою деятельность в соответствии с нормативными документами, разрабатываемыми при внедрении ИТ в структурном подразделении, и отвечает за выполнение требований безопасности в рамках ИТ. В каждой ЛВС может функционировать несколько ИТ;
– *пользователь*. Он отвечает за выполнение требований безопасности в рамках используемых им средств информатизации, подключенных к компьютерной сети (в том числе и с помощью средств удаленного доступа) в установленном порядке.

2.1. Руководитель структурного подразделения обязан:

– доводить до пользователей структурного подразделения требования безопасности и требования иных нормативных документов по вопросам информационной безопасности, постоянно держать в поле зрения вопросы безопасности;
– обеспечивать, чтобы каждый компьютер в структурном подразделении имел пользователя, ответственного за выполнение требований безопасности;
– представлять для назначения в установленном порядке администраторов ЛВС структурного подразделения;
– назначать администраторов ИТ, функционирующих в рамках ЛВС структурного подразделения;
– организовывать обучение пользователей мерам безопасности;
– информировать администраторов ЛВС и ИТ структурного подразделения об изменении статуса каждого пользователя (переход на другую работу, увольнение и т.п.);
– обеспечивать контроль за соблюдением работниками структурного подразделения физической защиты технических средств.

2.2. Координатор безопасности обязан:

– оказывать помощь руководителям структурных подразделений в понимании и реализации требований безопасности;

– осуществлять контроль за состоянием дел по выполнению требований безопасности в структурных подразделениях;

– принимать участие в разработке нормативных документов, регламентирующих распределение обязанностей между аппаратом Государственной думы и внешними организациями, обслуживающими отдельные элементы компьютерной сети, и регламентов выполнения работ;

– взаимодействовать с отделом по защите государственной тайны, ФАПСИ (в случае необходимости) и другими организациями по проблемам безопасности;
– руководить работой по анализу угроз в компьютерной сети, их последствий, выбору защитных мер;
– разрабатывать планы восстановления работоспособности компьютерной сети в целом после аварий и иных критических ситуаций;
– готовить ежегодные отчеты;
– требовать от системного администратора компьютерной сети, администраторов ЛВС, ИТ структурных подразделений и пользователей безусловного выполнения требований безопасности.
– готовить предложения по развитию Основных направлений.

2.3. Системный администратор компьютерной сети обязан:

– осуществлять оперативный контроль за соблюдением требований безопасности в рамках всей компьютерной сети;
– при выявлении нарушений требований безопасности, самостоятельно или во взаимодействии с администраторами ЛВС структурных подразделений, установить причины и принять меры по их устранению, доложить координатору безопасности;

– проводить анализ рисков в компьютерной сети в целом, оценивать размеры возможного ущерба, выбирать эффективные меры защиты;
– учитывать, анализировать случаи нарушения требований безопасности;
– информировать администраторов ЛВС структурных подразделений о нарушениях требований безопасности, оказывать помощь в выборе эффективных мер зашиты;
– периодически проводить проверку надежности защиты компьютерной сети, не допускать получения привилегий неавторизированными пользователями;
– организовывать регулярные учебно-методические занятия с администраторами ЛВС структурных подразделений по вопросам выполнения требований безопасности;
– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
– требовать от пользователей и администраторов ЛВС и ИТ структурных подразделений безусловного выполнения требований безопасности.

2.4. Администратор ЛВС структурного подразделения обязан:

– осуществлять оперативный контроль за соблюдением требований безопасности в рамках ЛВС структурного полразделения;
– при выявлении нарушений требований безопасности, самостоятельно (или во взаимодействии с системным администратором компьютерной сети) установить причины и принять меры по их устранению, доложить системному администратору компьютерной сети и руководителю структурного подразделения;
– проводить анализ рисков в ЛВС структурного подразделения, оценивать размеры возможного ущерба, выбирать эффективные меры защиты;
– ежедневно анализировать регистрационную информацию;
– учитывать, анализировать случаи нарушения требований безопасности;
– информировать администраторов ИТ о нарушениях требований безопасности, оказывать помощь в выборе эффективных мер защиты;
– периодически проводить проверку надежности защиты ЛВС структурного подразделения, не допускать получения привилегий неавторизированными пользователями;
– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
– требовать от пользователей и администраторов ИТ структурного подразделения

безусловного выполнения требований безопасности.

2.5. Администратор ИТ обязан:

– управлять правами доступа пользователей к ИТ;
– выделять пользователям имена и начальные пароли только после заполнения регистрационных форм;
– регулярно выполнять резервное копирование информации, обрабатываемой ИТ;
– выполнять мероприятия антивирусной защиты программных средств ИТ;
– осуществлять оперативный контроль за соблюдением требований безопасности в рамках ИТ;
– при выявлении нарушений требований безопасности, самостоятельно (или во взаимодействии с администратором ЛВС структурного подразделения) установить причины и принять меры по их устранению, доложить администратору ЛВС структурного подразделения;
– проводить анализ рисков в рамках ИТ, оценивать размеры возможного ущерба, выбирать эффективные меры защиты;
– ежедневно анализировать регистрационную информацию;
– учитывать, анализировать случаи нарушения требований безопасности;
– периодически проводить проверку надежности защиты ИТ, не допускать получения привилегий неавторизированными пользователями;
– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
– требовать от пользователей безусловного выполнения требований безопасности.

2.6. Пользователь обязан:

– знать и соблюдать требования безопасности, выполнять процедуры безопасности и требования иных нормативных документов, регламентирующих порядок функционирования компьютерной сети;
– выполнять процедуры безопасности для защиты пользовательской информации, расположенной на рабочей станции или сервере ЛВС структурного подразделения;
– информировать администраторов ЛВС и ИТ структурных подразделений о нарушениях требований безопасности и иных нештатных ситуациях;
– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

2.7. Ответственность

Нарушение требований безопасности может подвергнуть компьютерную сеть и циркулирующую в ней информацию недопустимому риску. В связи с этим нарушения требований безопасности со стороны пользователей и должностных лиц, обеспечивающих функционирование компьютерной сети, будут рассматриваться руководством Государственной думы и ее аппарата для принятия мер в установленном порядке.

3. Направления обеспечения безопасности

3.1. Безопасность технических средств

3.1.1. Сохранность технических средств

Защищаемые технические средства компьютерной сети - комплекты оборудования, входящие в состав серверов ЛВС структурных подразделений, рабочих станций, активного и пассивного сетевого оборудования.

Сохранность серверов ЛВС структурных подразделений, активного и пассивного сетевого оборудования обеспечивается администраторами ЛВС структурных подразделений, специалистами УИТО и подразделениями ФАПСИ в соответствии с установленным распределением обязанностей.
Сохранность рабочих станций обеспечивается пользователями.

3.1.2. Учет технических средств

В компьютерной сети могут быть использованы только учтенные технические средства, переданные пользователям в соответствии с "Порядком установки и сопровождения средств информатизации в Государственной думе". Обо всех изменениях в составе технических средств руководители структурных подразделений должны информировать соответствующие службы.
Личные технические средства пользователей могут использоваться в компьютерной сети только после постановки их на учет и техническое обслуживание в Управлении делами Государственной думы.

3.1.3. Установка и перемещение технических средств

Вся деятельность по установке и перемещению технических средств выполняется в соответствии с "Порядком установки и сопровождения средств информатизации в Государственной думе".
Установка и перемещение технических средств в категорированных помещениях выполняется после согласования с отделом по защите государственной тайны аппарата Государственной думы.

3.1.4. Сервисное обслуживание технических средств

Сервисное обслуживание, ремонт и восстановление работоспособности технических средств компьютерной сети осуществляется Управлением делами Государственной думы, УИТО и ФАПСИ в соответствии с утвержденным распределением обязанностей. ФАПСИ осуществляет свою деятельность на основании договора и может привлекать для решения этих задач другие внешние организации.

3.2. Безопасность программных средств

3.2.1. Программные средства компьютерной сети

В компьютерной сети разрешено использовать только лицензионные типовые программные средства и средства, разработанные в Государственной думе. Иные программные средства не сопровождаются УИТО.
Программным средством, разработанным в Государственной думе, считается средство, разработанное работниками аппарата Государственной думы или лицами, работающими в ее интересах на основании договоров или соглашений. Такое программное средство ограничено внутренним использованием.
Установка и сопровождение программных средств осуществляется в соответствии с "Порядком установки и сопровождения средств информатизации в Государственной думе".

3.2.2. Учет и хранение программных средств

Учет и хранение всех программных средств, используемых в компьютерной сети и технической документации к ним осуществляется в соответствии с "Порядком учета и хранения программных средств в Государственной думе".

3.2.3. Антивирусная безопасность программных средств

Вся деятельность по выполнению мероприятий антивирусной защиты программных средств компьютерной сети организуется и осуществляется пользователями и должностными лицами, обеспечивающими ей функционирование, в соответствии с "Порядком проведения антивирусных мероприятий в компьютерной сети Государственной думы".

3.3. Безопасность телекоммуникаций

3.3.1. Компьютерная сеть

Изменение конфигурации компьютерной сети не может проводиться без предварительного согласования с координатором по безопасности и системным администратором компьютерной сети.
Все вновь разрабатываемые ЛВС и ИТ структурных подразделений должны учитывать требования безопасности, их подключение в компьютерную сеть должно быть согласовано с координатором безопасности и системным администратором компьютерной сети.
Перед объединением с сетью новые ЛВС и ИТ структурных подразделений должны быть проверены на совместимость с компьютерной сетью, приняты по акту и обеспечены соответствующей нормативной документацией.
Самостоятельное подключение и перемещение рабочих станций пользователями в компьютерной сети запрещено. Такие действия автоматически фиксируются и блокируются активным сетевым оборудованием. Для возобновления работы с ресурсами компьютерной сети пользователю необходимо обратиться к администратору ЛВС структурного подразделения и системному администратору компьютерной сети Государственной думы.

3.3.2. Асинхронный доступ

Внутренние и внешние модемы (факс-модемы) запрещено использовать на рабочих станциях компьютерной сети. Они могут устанавливаться только на компьютерах (в том числе и портативных), не включенных в компьютерную сеть.
Исключительные случаи санкционируются координатором безопасности. В этих случаях модемы должны использоваться только для выхода и должны быть выключены всегда, когда не используются.
Рекомендованными средствами асинхронного доступа являются серверы доступа и модемный пул, входящие в состав компьютерной сети.

3.3.3. Доступ к внешним информационным ресурсам

Доступ к внешним информационным ресурсам должен устанавливаться таким образом, чтобы исключить, прямо или косвенно, риски в компьютерной сети.
Соединения компьютерной сети с другими сетями должны согласовываться с координатором по безопасности и утверждаться руководителем аппарата Государственной думы.

3.4. Процедуры обеспечения безопасности

3.4.1. Копирование и восстановление

Для защиты от потери вся информация, которая хранится на магнитных носителях технических средств компьютерной сети или переносится на магнитных носителях, должна копироваться пользователями и должностными лицами, обеспечивающими функционирование компьютерной сети, и храниться в защищенном месте.
Все пользователи должны быть обучены процедурам копирования и восстановления информации.
Должно быть предусмотрено копирование документации.

3.4.2. Контроль доступа

Доступ пользователей к ЛВС и ИТ структурных подразделений должен осуществляться через уникальные имена пользователей (одно имя для доступа ко всем ЛВС и ИТ), защищенные индивидуальными паролями.
Пользователи должны самостоятельно использовать только случайные пароли, регулярно менять их, не записывать пароли на бумаге, не сообщать их другим лицам.
Вся информация об изменениях статуса депутатов Государственной думы, их помощников и работников аппарата должна передаваться из Управления кадров и государственной службы координатору безопасности для оперативного управления правами доступа.

3.4.3. Протоколирование и аудит

В системных журналах должен осуществляться сбор информации о доступе к ЛВС и ИТ структурных подразделений. Накопленная информация должна регулярно анализироваться системным администратором компьютерной сети, администраторами ЛВС и ИТ структурных подразделений.

3.4.4. Компьютерные носители

При санкционированной передаче рабочей станции и портативного компьютера другому пользователю информация на магнитных носителях (ЖМД и ГМД) должна быть предварительно уничтожена пользователем или специалистами, осуществляющими установку и сопровождение средств информатизации.

4. Обучение

Пользователи и должностные лица, обеспечивающие функционирование компьютерной сети, должны быть обучены процедурам безопасности и ознакомлены с требованиями нормативных документов.
Управление кадров и государственной службы совместно с УИТО организует обучение и переподготовку работников аппарата по письменным заявкам руководителей структурных подразделений.

5. Контактные телефоны

По вопросам, относящимся к проблемам обеспечения безопасности обработки, хранения и передачи информации в компьютерной сети Государственной думы, следует обращаться к координатору безопасности (тел. 292-7844) и системному администратору компьютерной сети (тел. 292-1878).

Приложение 6

Глоссарий

Авторизация	предоставление или отказ в доступе к различным ресурсам или службам. Большинство компьютерных систем безопасности используют двухшаговый процесс: аутентификация, т.е. проверка, является ли пользователь тем, за кого он себя выдаёт, а затем авторизация, которая позволяет пользователю получить доступ к ресурсам в зависимости от его полномочий.
Алгоритм	точное предписание порядка выполнения операций для решения задачи; удовлетворяет требованиям определенности и однозначности (не допускать произвола в операциях), массовости (быть универсалы применимым для всех задач данного класса, хотя начальные условия задач можно варьировать в известных пределах) и результативности (приводить к решению за конечное число операций); гарантирует, что если задача имеет решение, то, осуществляя заданную последовательность действий, решение будет найдено.
Аппаратно-программные средства защиты	средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы
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.
Атака	действие некоторого субъекта компьютерной системы (пользователя, программы, процесса и т.д.), использующего уязвимость компьютерной системы для достижения целей, выходящих за пределы авторизации данного субъекта в компьютерной системе. Если, например, пользователь не имеет права на чтение некоторых данных, хранимых в компьютерной системе, а ему очень хочется, и поэтому он предпринимает ряд известных ему нестандартных манипуляций, обеспечивающих доступ к этим данным (в случае отсутствия или недостаточно надёжной работы средств безопасности) либо завершившихся неудачей (в случае надёжной работы средств безопасности), этот пользователь (иногда его называют «захватчиком») предпринимает в отношении компьютерной системы атаку.
Аутентификация	процесс подтверждения подлинности личности пользователя, для чего могут использоваться пароли, специальные карточки или электронная цифровая подпись.
Банковская тайна	сведения о банковском счете, банковском вкладе, операциях по счету о клиентах банка.
Безопасное	общецелевые (исполняемые образы, утилиты либо средства

программное обеспечение	разработки программного обеспечения) и прикладные программы и средства, осуществляющие безопасную обработку данных в компьютерной системе и безопасно использующие ресурсы системы.
Безопасность	состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.
Безопасность автоматизированных банковских систем (АБС)	это ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на АБС. Защита – это своего рода соревнование обороны и нападения: кто больше знает, предусматривает действенные меры, тот и выигрывает.
Безопасность информационной системы	совокупность элементов, необходимых для обеспечения адекватной защиты компьютерной системы, включая аппаратные/ программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удалённых компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.
Безопасность организации	стабильно прогнозируемое во времени состояние организации окружения, при котором возможно выполнение целевой функции (миссии) организации без перерывов и нарушений
Биометрический контроль доступа	автоматизированный метод, с помощью которого путём проверки (исследования) уникальных физиологических особенностей или поведенческих характеристик человека осуществляется идентификация личности. Такие физиологические особенности, как папилярный узор пальца, геометрия ладони или рисунок (модель) радужной оболочки глаза, являются постоянными физическими характеристиками человека. Данный тип измерений (проверки) практически неизменен, так же как и сами физиологические характеристики. Поведенческие же характеристики, такие как подпись, голос или клавиатурный почерк, находятся под влиянием как управляемых действий, так и менее управляемых психологических факторов. Поскольку поведенческие характеристики могут изменяться с течением времени, зарегистрированный биометрический образец должен обновляться при каждом его использовании. Хотя биометрия, основанная на поведенческих характеристиках, менее дорога и представляет меньшую угрозу для пользователей, физиологические черты позволяют осуществить большую точность идентификации личности и её безопасность. В любом случае, оба метода обеспечивают значительно более высокий уровень идентификации, чем сами по себе пароли или карты.
Брандмауэр (межсетевой экран)	программный и/или аппаратный барьер между двумя сетями, позволяющий установить только авторизованные

	межсетевые соединения. Брандмауэр защищает соединяемую с Интернетом корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации. Система может быть создана на базе программного, аппаратного обеспечения или комбинации того и другого.
Верификация	использование теста или имитированной среды для выявления идентичности двух уровней спецификаций системы, например политики безопасности в спецификации высшего уровня (исходном коде) и объектном коде.
Вирус	программа, модифицирующая другие программы. В контексте проблем безопасности этот термин обычно используется в отношении программ, злонамеренно внедряемых в систему с целью нанесения вреда и разрушения. Вирусная программа распространяется за счёт самокопирования и подсоединения копий к другим программам. Когда в системе происходит определённое событие, на которое настроен вирус, вирус начинает выполнять свою целевую функцию.
Государственная тайна	защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывателыюй и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.
Гриф конфиденциальности	реквизит, свидетельствующий о степени конфиденциальности сведений, содержащихся в их носителе, проставляемые на самом носителе (или) в сопроводительной документации на него
Гриф секретности	реквизит, свидетельствующий о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе (или) в сопроводительной документации на него
Дезинформация	способ маскирования, заключающийся в преднамеренно распространении ложных сведений о лицах, объектах, события: явлениях и процессах или имитации их деятельности
Деятельность	всякого рода практическая активность, направленная на достижение определенной цели
Доверенная вычислительная база	термин, относящийся к аппаратным, фирменным программным и просто программным механизмам защиты в компьютерной системе, обеспечивающим реализацию в этой системе избранной политики безопасности.
Доверенная компьютерная система	система, допускающая ведение безопасной обработки несортированного потока критичной информации за счёт использования достаточных аппаратных и программных средств обеспечения безопасности.
Документ	материальный объект с зафиксированной на нем информацией в вид текста, звукозаписи или изображения, предназначенный для передач во времени и пространстве в целях хранения и общественного использования. Свойство: наличие реквизитов.
Документация	Совокупность документов, оформленная по единым правилам. Подразделяется на нормативно-справочную,

	конструкторскую, проектную, проектно-сметную, техническую, технико-экономическую, эксплуатационную и т.п.
Документированная информация	Зафиксированная на материальном носителе информация реквизитами, позволяющая его идентифицировать.
Доступность информации	является ведущим аспектом информационной безопасности. Информационные системы создаются или приобретаются прежде всего для получения определённых информационных услуг. Если получение этих услуг становится невозможным, это наносит ущерб всем субъектам информационных отношений. Особенно ярко важность доступности как аспекта информационной безопасности проявляется в разного рода системах управления производством, транспортом. Менее критичными к отказам в доступе являются различные справочно- информационные услуги, которыми пользуется большое количество людей: продажа билетов, банковские операции, различного рода справки. Однако длительная недоступность ресурсов подобного рода может повлечь весьма неприятные последствия, как в моральном, так и в материальном плане.
Доступность ресурса системы	свойство ресурса быть доступным для использования авторизованными субъектами системы в любое время.
Жизненно важные интересы	Совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества, государства.
Жизненный цикл	модель создания и использования системы информационной безопасности, отражающей ее различные состояния, начиная с момента возникновения необходимости в системе и закапчивая моментом ее полного выхода из употребления.
Задачи информационной безопасности	состоят в обеспечении комбинации доступности, целостности и конфиденциальности информации определяются в ряде международных и российских руководящих документов. В целом под этим термином подразумевается: • возможность за приемлемое время получить требуемую информационную услугу, а также предотвращение несанкционированного отказа в получении информации; • предотвращение несанкционированной модификации или разрушения информации; предотвращение несанкционированного ознакомления с информацией.
Законодательные средства	правовые акты страны, которые регламентируют правила использования, обработки, и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил
Закрытые данные	данные, доступные ограниченному кругу пользователей.
Защита информации (защита данных, Data protection)	совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на неё угроз естественного или искусственного

характера.

Злоумышленник (ЗЛ)	лицо, пытающееся посредством использования несовершенства правовых, организационных или технических средств обеспечения информационной безопасности оказать неправомерное и несанкционированное воздействие на (получить, изменить или ограничить в доступе защищаемую информацию) информацию организации.
Идентификация	процесс анализа персональных, технических или организационных характеристик или кодов для получения (предоставления) доступа к компьютерным ресурсам.
Имитозащита	защита систем передачи и хранения информации от навязывания ложных данных.
Информационная безопасность	состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере (среде)
Информационная война	информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.
Информационная неопределенность	несоответствие фактического и желаемого состояний информированности сотрудников об окружающей действительности, которое не позволяет решать задачи предметной деятельности
Информационная потребность	определенное состояние субъекта предметной деятельности, которое возникает в связи с необходимостью получения сведений, обеспечивающих решение предметных задач
Информационная преступность	проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, т.е. деятельность, проводимая в политических целях.
Информационная сфера (среда)	сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации
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; • вмешательства 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.
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.
Информация	1) общенаучное понятие, включающее обмен сведениями между людьми; 2) с точки зрения принятия решений информацией являются данные, оказывающие влияние на поведение системы, используемые в процессе принятия решений или в связи с осуществлением тех или иных действии; 3) сведения (отображение) о событии или состоянии реальной действительности, позволяющие принимать решения, ведущие к достижению цели предметной деятельности.
Источник информации	материальный объект, носитель определенных сведений, представляющих конкретный интерес для злоумышленника
Канал утечки информации	физический путь от источника КИ к злоумышленнику, посредством которого возможно нарушение конфиденциальности
Коммерческая (служебная) тайна	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.
Компьютерная безопасность	состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами. Безопасность обеспечивается путём создания вокруг компьютера и оборудования защитной зоны, в которой работает только авторизованный персонал, а также использования специального программного обеспечения и встроенных в операционные процедуры механизмов защиты.
Контроль безопасности (аудит безопасности)	независимое изучение системных записей и действий: - для проверки адекватности системных средств управления; - для обеспечения их соответствия установленной политике и рабочим процедурам; для обнаружения брешей в безопасности и выдачи рекомендаций по изменению управления, политики и процедур.
Конфиденциальная информация	документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Конфиденциальность компьютерной информации	это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т.д.).
Концепция системы информационной безопасности	системно взаимосвязанная совокупность структурных решений, реализующих требуемое качество информационной безопасности.
Криптографическая защита	защита информационных процессов от целенаправленных попыток отклонить их от нормальных условий протекания.
Криптографическая система, криптосистема	набор криптографических преобразований или алгоритмов, предназначенных для работы в единой технологической цепочке с целью решения определённой задачи защиты информационного процесса.
Криптографические средства	средства защиты с помощью преобразования информации (шифрование). Шифрованием называется некоторое обратимое однозначное преобразование данных, делающее их непонятными для неавторизованных лиц. Никто, кроме хозяина данных и лиц, которым разрешен доступ к этим данным, не должен знать, во-первых, самого алгоритма преобразования данных, а, во-вторых, управляющих данных для такого алгоритма – так называемых ключей. Шифрование делает почти бессмысленным простой доступ к данным: ведь, не зная ключа, захватчик может годами биться над украденной абракадаброй, но так и не понять смысла данных.
Логическая бомба компьютерного вируса	участок программы, который реализует некоторые действия при наступлении определённых условий. Этим условием может быть, например, наступление какой-то даты или появление какого-то имени файла.
Люком компьютерного вируса	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 неописанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности, выход в привилегированный режим).
Маскировка	метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.
Микрофонный эффект	появление в цепях радиоэлектронной аппаратуры посторонних (паразитных) электрических сигналов, обусловленных механическим воздействием, в том числе и звуковой волны.
Наблюдение	постоянное или выборочное активное и целенаправленное исследование предметов, явлений или людей в естественных условиях или с помощью технических средств с последующим обобщением и анализом данных наблюдения.
Незаконное подключение	контактное или бесконтактное подсоединение к различного рода линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них тем или иным путем.
Несанкционированн	преднамеренные, противоправные действия

ый доступ (НСД) к информации	злоумышленников с целью нарушения информационной безопасности.
Носители сведений, составляющих государственную тайну	материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.
Обеспечение безопасности	проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз.
Обеспечение информационной безопасности	регулярная деятельность по созданию и поддержанию заданного уровня информационной безопасности.
Объектами посягательств	могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением. В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория не имеет особого смысла. Если компьютер - только объект посягательства, то квалификация правонарушения может быть произведена по существующим нормам права. Если же – только инструмент, то достаточен только такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ. Каждый сбой работы компьютерной сети это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, «безбумажного» документооборота и других, серьёзный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.
Операционная безопасность данных	защита данных от модификации, разрушения или разглашения (случайных, неавторизованных либо преднамеренных) во время выполнения операций ввода, обработки или вывода.
Организационное обеспечение информационной	регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и

безопасности	несанкционированный доступ к КИ становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.
Организационные мероприятия	совокупность процессов или действий, ведущих к образованию и совершенствованию взаимосвязей между частями целого.
Организационные средства	организационно-технические и организационно-правовые мероприятия по поведению персонала.
Организационные средства обеспечения информационной безопасности	упорядоченная совокупность организационных решений, регламентирующих на правовой основе: создание и функционирование системы информационной безопасности, взаимоотношения сотрудников и подразделений организации между собой и со сторонними организациями, общую организацию работ в сфере информационной безопасности.
Оргштатный элемент	это «обезличенный» пользователь системы, для которого провидится работа по управлению доступом к операциям и объектам системы. Затем реальному пользователю выдаётся право быть представленным в системе в виде оргштатного элемента.
Основные объекты безопасности	личность – права и свободы; общество – материальные и духовные ценности; государство – конституционный строй, суверенитет, территориальная целостность.
Открытое опубликование конфиденциальных сведений	публикация материалов в открытой печати, передача по радио и телевидению, оглашение на международных и внутрироссийских съездах, конференциях, совещаниях, симпозиумах, при публичной защите диссертаций и других публичных выступлениях, свободная рассылка, вывоз материалов за границу или передача их в любой форме иностранным фирмам, организациям или отдельным лицам вне сферы прямых служебных обязанностей.
Перехват	получение разведывательной информации за счет приема сигналом электромагнитной энергии пассивными средствами приема, расположенными, как правило, на достаточно безопасном расстоянии от источника конфиденциальной информации.
Перечень сведений, составляющих служебную или коммерческую тайну	Документ, содержащий сведения, не являющиеся секретными, но связанными с производственной, управленческой, финансовой и другой деятельностью организации, разглашение или утечка которых может нанести ущерб ее интересам, а также сведения, содержащие деловую информацию, имеющую фактическую или потенциальную ценность для организации в связи с ее конфиденциальным характером.
Персональные данные	сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.
Побуждение	метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счёт соблюдения сложившихся моральных и этических норм.
Правовое обеспечение защиты информации	совокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы

	их деятельности в системе защиты информации.
Преобразователь	прибор, который трансформирует изменение одной физической величины в изменение другой. В терминах электроники это означает преобразование неэлектрической величины в электрический сигнал и наоборот.
Препятствие	метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).
Принуждение	метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
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.
Процесс обеспечения информационной безопасности	совокупность логически упорядоченных, взаимосвязанных и организованных процедур безопасности, ведущая к достижению цели обеспечения информационной безопасности.
Разглашение	противоправные, умышленные или неосторожные действия сотрудников организации, приведшие к не вызванному служебной необходимостью, оглашению конфиденциальных сведений, которые в установленном порядке были доверены им по работе, а также передача таких сведений по открытым техническим каналам или обработка их на некатегорированных ЭВМ.
Регламентация	метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.
Система защиты данных	комплекс программных, технических, криптографических и организационных средств, обеспечивающих защиту данных от несанкционированного использования, а также преднамеренного или случайного их разрушения и искажения.
Система информационной безопасности	организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации - от нарушения конфиденциальности, целостности и доступа
Системный аналитик	специалист, описывающий прикладные проблемы, определяющий спецификации системы, дающий рекомендации по изменениям оборудования, проектирующий процедуры обработки данных и методы верификации

	предполагаемых структур данных.
Скрытый канал	канал коммуникации, позволяющий процессу передавать информацию путём, нарушающим политику безопасности, реализуемую в данной системе.
След контроля	записи о транзакциях, выполняемых в системе, которые (записи) в совокупности документируют ход обработки информации в системе, что, в свою очередь, позволяет проследить (провести трассировку) его вперед – от исходных транзакций до создаваемых в процессе их работы записей и/или отчётов, а также назад – от конечных записей/ отчётов до исходных транзакций. Последовательность записей, составляющих след контроля, позволяет определить источники возникновения транзакций в системе и последовательность их выполнения системой.
Служба безопасности	система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности информации.
Средства защиты информации	Средства защиты информации: - технические, криптографические, программные и другие средства, предназначенные для защиты конфиденциальной информации; - средства реализации средств защиты информации; средства контроля эффективности защиты информации.
Стратегическое планирование СИБ	1) методология анализа, разработки и сопровождения сложных СИБ, определяющая подсистемы, компоненты и способы их соединения, задающая ограничения, при которых система должна разрабатываться и функционировать, выбирающая наиболее эффективное сочетание людей и технических средств для реализации системы; 2) деятельность, осуществляемую для выработки решений по трансформации начального состояния СИБ к требуемому состоянию, при ограничениях на время и ресурсы.
Субъект обеспечения безопасности	1) основной – государство, осуществляющее в этой области через органы законодательной, исполнительной и судебной властей; 2) граждане, общественные организации в соответствии с законодательством.
Троянский конь	вид компьютерного вируса, функции, реализуемые программой, но не описанные в документации. Человек, знающий эту функцию, может заставить работать программу непредсказуемым для окружающих способом.
Угроза	условия, представляющие потенциальную возможность нанесения ущерба компьютерной системе. Атаки – частный вид угроз, так же как стихийные бедствия , человеческие ошибки, программные сбои и т.д.
Угроза безопасности	Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.
Угроза безопасности организации	потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить устойчивость, развитие или привести к прекращению деятельности организации.

Угрозы доступности данных	возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации.
Угрозы конфиденциальности данных и программ	реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи. Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки.
Угрозы отказа от выполнения транзакций	возникают в том случае, когда легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность.
Угрозы целостности данных, программ, аппаратуры.	Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении и модификации записей о состоянии счетов, изменении порядка расположения данных.
Управление в терминологии безопасности	защитный механизм (действие, устройство, процедура, технология и т.д.), уменьшающий уязвимость компьютерной системы.
Управление доступом	метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты: 1. идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора); 2. аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору; 3. проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту); 4. разрешение и создание условий работы в пределах установленного регламента; 5. регистрацию обращений к защищаемым ресурсам; реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.
Утечка информации	неконтролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым они были доверены.
Уязвимость	некоторая слабость системы безопасности, которая может послужить причиной нанесения компьютерным системам ущерба.
Физические средства защиты	предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.
Хищение	умышленное, противоправное тайное завладение чужим

имуществом, средствами, документами, информацией.

Целостность информации	немаловажный аспект информационной безопасности, обеспечивающий предотвращение несанкционированных изменений и разрушений информации. Примерами нарушения целостности могут служить различные, совершенные при помощи вычислительных систем, кражи в банках, подделка кредитных карточек, изменения информации в различных информационных системах.
Целостность ресурса системы	свойство ресурса быть неизменным в семантическом смысле при функционировании системы.
Целостность системы	состояние системы, в котором существует полная гарантия того, что при любых условиях компьютерная система базируется на логически завершённых аппаратных и программных средствах, обеспечивающих работу защитных механизмов, логическую корректность и достоверность операционной системы и целостность данных.
Червь	программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе. В отличие от вирусов червь обычно не искажает файлы данных и программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.
Экспозиция	форма возможной потери или ущерба для компьютерной системы. Например, экспозициями считаются неавторизованный доступ к данным или противодействие авторизованному использованию компьютерной системы.
Электронное устройство защиты	электронное устройство в составе компьютера, предназначенное для защиты программ и данных от несанкционированного доступа. Электронное устройство защиты выполняет функции замка, ответчика и т.п.
“Rainbow series” (Радужная серия)	опубликованные стандарты безопасности, используемые Министерством обороны США, названные каждый по цвету обложки. Например, в «красной книге» описываются вопросы безопасности в сетях, в «жёлтой книге»- безопасность паролей, в «оранжевой книге» («Department of Defence Trusted Computer System Evaluation Criteria» DOD 5200.28 – STD («критерий оценивания безопасности компьютерных систем министерства обороны»)) дается стандарт оценивания безопасности компьютерных систем, устанавливающий четыре иерархические класса – A, B, C и D – определенных уровней доверенности (иными словами, уверенности в безопасности) для конкретных приложений, разрабатываемых и используемых в интересах правительства, - доверенных компьютерных систем т.д.
Risk analysis (Анализ риска)	процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчётов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.
Risk assessment (Оценка риска)	метод анализа угроз и слабых сторон, известных и предполагаемых, позволяющий определить размер ожидаемого ущерба и степень его приемлемости для работы

	системы.
Secure operating system (безопасная операционная система)	операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Приложение 7

Антивирус Касперского Personal 5.0 Разработчик:

«Лаборатория Касперского»

«Антивирус Касперского Personal 5.0» – новая разработка «Лаборатории Касперского», воплощающая результаты многолетних исследований ведущих экспертов в области защиты от вредоносных программ. Продукт сочетает уникальную функциональность, новый пользовательский интерфейс и высокий уровень защиты от вирусов. Программный комплекс позволяет организовать полномасштабную систему антивирусной защиты персонального компьютера. «Антивирус Касперского Personal 5.0» охватывает все возможные источники проникновения вирусной угрозы – съемные и постоянные файловые носители, электронную почту и протоколы Интернета.

Наиболее характерным отличием нового антивируса является пользовательский интерфейс. Он позволяет без труда управлять всем встроенным арсеналом средств защиты от вирусов при помощи уникальной системы «Экспертный Совет». При возникновении нештатной ситуации «Экспертный Совет», выполненный в виде набора рекомендаций по настройке и использованию программы, в большинстве случаев позволит владельцу компьютера самостоятельно разрешить затруднение. В главном окне программы всегда доступны встроенные указания по выполнению тех или иных действий и обоснования для их совершения.

Выполненный в стиле Windows XP, пользовательский интерфейс «Антивируса Касперского» отличается простотой, интуитивной понятностью и привлекательным дизайном. Все технические подробности защиты адаптированы для понимания даже начинающими пользователями и реализованы в 3-компонентном графическом меню. Меню позволяет одновременно управлять всеми элементами программы из единого центра.

Использование «Антивируса Касперского» обеспечивает полное восстановление работоспособности системы при вирусной атаке. В то же время функция антивирусной проверки и лечения электронной почты позволяет очистить от вирусов входящую и исходящую корреспонденцию в режиме реального времени. В случае необходимости пользователю также доступны проверка и лечение почтовых баз различных почтовых систем. Защиту компьютера от самых свежих вредоносных кодов обеспечит автоматическая процедура обновлений антивирусных баз данных, выпускаемых экспертами «Лаборатории Касперского» круглосуточно с трехчасовым интервалом.

Сводная таблица антивирусных программ

	Имя	AIDSTEST	DR. WEB	AVSP	ADINF	MSAV
	Версия	1723	4.0	2.95	12.00	DOS 7.10
ИП	Фильтр	-	-	+	-	-
ИП	Доктор	+	+	+	-	+
ИП	Ревизор	-	-	+	+	+
ИП	Детектор	+	+	+	-	+
	Количество вирусов	9000	7100	276*	-	2546
	Поддержка мыши	-	+	+	+	+
	Оконный интерфейс	-	+	+	+	+
	Обнаружение Stealth-вирусов	-	-	+	+	+
	Обнаружение неизвестных вирусов	-	+	+	+	+
	Время работы при задании соответствующих режимов**	/g /s	/a/s2/v/o/u	Качество*** /все файлы	По умолчанию	По умолчанию с контрольными суммами
		2,5 мин.	23 мин.	4 мин./11 мин.	1 мин.	1 мин. 20 сек.

*– имеется возможность самостоятельного пополнения данных о вирусах;
** – данные о быстродействии приведены для машины 486DX2-66 с жестким диском 270 Mb, заполненным на 97%
*** – файлы с расширениями *.com, *.exe, *.ov, *.bin, *.sys.

Сводная таблица антивирусных программ

Название антивирусной программы	Общие характеристики	Положительные качества	Недостатки
AIDSTEST	Самая известная антивирусная программа, совмещающая в себе функции детектора и доктора Д.Н. Лозинского. В России практически на каждом IBM – совместимом персональном компьютере есть одна из версий этой программы.	При запуске Aidstest проверяет оперативную память на наличие известных ему вирусов и обезвреживает их. Может создавать отчет о работе.	После окончания обезвреживания вируса следует обязательно перезагрузить ПЭВМ. Возможны случаи ложной тревоги, например, при сжатии антивируса упаковщиком. Программа не имеет графического интерфейса и режимы ее работы задаются с помощью ключей.
DOCTOR WEB	Dr. Web также. Как и Aidstest относится к классу детекторов докторов, но в отличие от последнего имеет так называемый «эвристический анализатор» – алгоритм, позволяющий обнаруживать неизвестные вирусы.	Пользователь может указать программе тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. Как и Aidstest, Dr.	При сканировании памяти нет стопроцентной гарантии, что антивирус обнаружит все вирусы, находящиеся там. Тестирование винчестера Dr. Web-ом занимает намного больше времени, чем Aidstest-ом.

		Web может создавать отчет о работе.	
AVSP (Antivirus Software Protection)	Эта программа сочетает в себе и детектор, и доктор, и ревизор, и даже некоторые функции резидентского фильтра.	Антивирус может лечить как известные, так и неизвестные вирусы. К тому же AVSP может лечить самомодифицирующиеся и Stealth-вирусы (невидимки). Очень удобна контекстная система подсказок, которая дает пояснения к каждому пункту меню. При комплексной проверке AVSP выводит также имена файлов, в которых произошли изменения, а также так называемую карту изменений.	Вместе с вирусами драйвер отключает и некоторые другие резидентные программы. Останавливается на файлах, у которых странное время создания.
Microsoft Antivirus	Этот антивирус может работать в режимах детектора-доктора и ревизора. MSAV имеет дружественный интерфейс в стиле MS Windows, естественно, поддерживается мышь.	Хорошо реализована контекстная помощь: подсказка есть практически к любому пункту меню. К любой ситуации. Универсально реализован доступ к пунктам меню: для этого можно использовать клавиши управления курсором, ключевые клавиши. В главном меню можно сменить диск (Select new drive), выбрать между проверкой без удаления вирусов (Detect) и с их удалением (Detect&Clean).	Серьезным неудобством при использовании программы является то, что она сохраняет таблицы с данными о файлах не в одном файле, а разбрасывает их по всем директориям.
Advanced Diskinfoscope	ADinf относится к классу программ-ревизоров.	Антивирус имеет высокую скорость работы, способен с успехом противостоять вирусам, находящимся в памяти. Он позволяет контролировать диск, читая его по секторам через BIOS и не используя системные прерывания DOS, которые может перехватить вирус.	Для лечения зараженных файлов применяется модуль ADinf CureModule, не входящий в пакет ADinf и поставляющийся отдельно.

Приложение 9

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 зашиты 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 проводится 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 состояние «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)*.

Приложение 10

10 января 2002 года N 1-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Принят
Государственной Думой
13 декабря 2001 года

Одобрен
Советом Федерации
26 декабря 2001 года

Глава I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цель и сфера применения настоящего Федерального закона

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско - правовых сделок и в других предусмотренных законодательством Российской Федерации случаях.

Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом Российской Федерации, Федеральным законом "Об информации, информатизации и защите информации", Федеральным законом "О связи", другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также осуществляется соглашением сторон.

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

электронный документ - документ, в котором информация представлена в электронно - цифровой форме;

электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной

цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

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;

пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Глава II. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

1. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

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;

подтверждена подлинность электронной цифровой подписи в электронном документе;

электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2. Участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Статья 5. Использование средств электронной цифровой подписи

1. Создание ключей электронных цифровых подписей осуществляется для использования в:

информационной системе общего пользования ее участником или по его обращению удостоверяющим центром;

корпоративной информационной системе в порядке, установленном в этой системе.

2. При создании ключей электронных цифровых подписей для использования в информационной системе общего пользования должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей несертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством Российской Федерации.

3. Использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается.

4. Сертификация средств электронной цифровой подписи осуществляется в соответствии с законодательством Российской Федерации о сертификации продукции и услуг.

Статья 6. Сертификат ключа подписи

1. Сертификат ключа подписи должен содержать следующие сведения:

уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;

открытый ключ электронной цифровой подписи;

наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;

наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре

1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не

менее установленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством Российской Федерации.

3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Глава III. УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

Статья 8. Статус удостоверяющего центра

1. Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Требования, предъявляемые к материальным и финансовым возможностям удостоверяющих центров, определяются Правительством Российской Федерации по представлению уполномоченного федерального органа исполнительной власти.

Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы.

2. Деятельность удостоверяющего центра подлежит лицензированию в соответствии с законодательством Российской Федерации о лицензировании отдельных видов деятельности.

Статья 9. Деятельность удостоверяющего центра

1. Удостоверяющий центр:

изготавливает сертификаты ключей подписей;

создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;

проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

2. Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

3. При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в удостоверяющем центре.

4. Услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Статья 10. Отношения между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти

1. Удостоверяющий центр до начала использования электронной цифровой подписи уполномоченного лица удостоверяющего центра для заверения от имени удостоверяющего центра сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица удостоверяющего центра в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью удостоверяющего центра.

2. Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц удостоверяющих центров.

3. Электронные цифровые подписи уполномоченных лиц удостоверяющих центров могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих электронных цифровых подписей для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4. Уполномоченный федеральный орган исполнительной власти:

осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Статья 11. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

вносить сертификат ключа подписи в реестр сертификатов ключей подписей;

обеспечивать выдачу сертификата ключа подписи обратившимся к нему участникам информационных систем;

приостанавливать действие сертификата ключа подписи по обращению его владельца;

уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Статья 12. Обязательства владельца сертификата ключа подписи

1. Владелец сертификата ключа подписи обязан:

не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

хранить в тайне закрытый ключ электронной цифровой подписи;

немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Статья 13. Приостановление действия сертификата ключа подписи

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

3. Действие сертификата ключа подписи по указанию полномочного лица (органа) приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица (органа). В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4. В соответствии с указанием полномочного лица (органа) о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание о приостановлении действия сертификата ключа подписи.

Статья 14. Аннулирование сертификата ключа подписи

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

по истечении срока его действия;

при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

в случае, если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

по заявлению в письменной форме владельца сертификата ключа подписи;

в иных установленных нормативными правовыми актами или соглашением сторон случаях.

2. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

Статья 15. Прекращение деятельности удостоверяющего центра

1. Деятельность удостоверяющего центра, выдающего сертификаты ключей подписей для использования в информационных системах общего пользования, может быть прекращена в порядке, установленном гражданским законодательством.

2. В случае прекращения деятельности удостоверяющего центра, указанного в пункте 1 настоящей статьи, сертификаты ключей подписей, выданные этим удостоверяющим центром, могут быть переданы другому удостоверяющему центру по согласованию с владельцами сертификатов ключей подписей.

Сертификаты ключей подписей, не переданные в другой удостоверяющий центр, аннулируются и передаются на хранение в соответствии со статьей 7 настоящего Федерального закона уполномоченному федеральному органу исполнительной власти.

3. Деятельность удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, прекращается по решению владельца этой системы, а также по договоренности участников этой системы в связи с передачей обязательств данного удостоверяющего центра другому удостоверяющему центру или в связи с ликвидацией корпоративной информационной системы.

Глава IV. ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Статья 16. Использование электронной цифровой подписи в сфере государственного управления

1. Федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, а также организации, участвующие в документообороте с указанными органами, используют для подписания своих электронных документов электронные цифровые подписи уполномоченных лиц указанных органов, организаций.

2. Сертификаты ключей подписей уполномоченных лиц федеральных органов государственной власти включаются в реестр сертификатов ключей подписей, который ведется уполномоченным федеральным органом исполнительной власти, и выдаются пользователям сертификатов ключей подписей из этого реестра в порядке, установленном настоящим Федеральным законом для удостоверяющих центров.

3. Порядок организации выдачи сертификатов ключей подписей уполномоченных лиц органов государственной власти субъектов Российской Федерации и уполномоченных лиц органов местного самоуправления устанавливается нормативными правовыми актами соответствующих органов.

Статья 17. Использование электронной цифровой подписи в корпоративной информационной системе

1. Корпоративная информационная система, предоставляющая участникам информационной системы общего пользования услуги удостоверяющего центра корпоративной информационной системы, должна соответствовать требованиям, установленным настоящим Федеральным законом для информационных систем общего пользования.

2. Порядок использования электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

3. Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Статья 18. Признание иностранного сертификата ключа подписи

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Российской Федерации в случае выполнения установленных законодательством Российской Федерации процедур признания юридического значения иностранных документов.

Статья 19. Случаи замещения печатей

1. Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

2. В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Глава V. ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

Статья 20. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом

1. Нормативные правовые акты Российской Федерации подлежат приведению в соответствие с настоящим Федеральным законом в течение трех месяцев со дня вступления в силу настоящего Федерального закона.

2. Учредительные документы удостоверяющих центров, выдающих сертификаты ключей подписей для использования в информационных системах общего пользования, подлежат приведению в соответствие с настоящим Федеральным законом в течение шести месяцев со дня вступления в силу настоящего Федерального закона.

Статья 21. Переходные положения

Удостоверяющие центры, создаваемые после вступления в силу настоящего Федерального закона до начала ведения уполномоченным федеральным органом исполнительной власти реестра сертификатов ключей подписей, должны отвечать требованиям настоящего Федерального закона, за исключением требования предварительно представлять сертификаты ключей подписей своих уполномоченных лиц уполномоченному федеральному органу исполнительной власти. Соответствующие сертификаты должны быть представлены указанному органу не позднее чем через три месяца со дня вступления в силу настоящего Федерального закона.

Президент
Российской Федерации
В.ПУТИН

Москва, Кремль
10 января 2002 года
N 1-ФЗ

Список литературы

1. Абрамов, А.В. Новое в финансовой индустрии: информатизация банковских технологий. – СПБ: Питер, 1997

2. Автоматизированные информационные технологии в банковской деятельности / под ред. проф. Г.А. Титоренко. – М.: Финстатинформ, 1997

3. Автоматизированные информационные технологии в экономике: Учебник / Под ред. проф. Г.А. Титоренко. – М.: ЮНИТИ, 2000

4. Агеев, А. С., сост. Организация и современные методы защиты информации: Метод. пособие для рук. и сотрудников служб безопасности Агеев А. С. и др.; Под общ. ред. С. А. Диева, А. Г. Шаваева . – М.: Концерн"Банк. Деловой Центр", 1998

5. Аглицкий, И. Состояние и перспективы информационного обеспечения российских банков. – Банковские технологии, 1997

6. Аджиев, В. Мифы о безопасности программного обеспечения: уроки знаменитых катастроф. – Открытые системы, 199. №6

7. Алексеев, В.И. ,сост. Информационная безопасность муниципальных образований Учеб. пособие Ассоц. экон. взаимодействия обл. Центр.-Черноозем. региона Рос. Федерации "Черноземье" и др.; [Алексеев В. И. и др.]. – Воронеж: Изд-во Воронеж. гос. техн. ун-та, 1998

8. Алексеев, В.М. Международные критерии оценки безопасности информационных технологий и их практическое применение: Учеб. пособие / В. М. Алексеев, В. В. Андрианов, С. Л. Зефиров ; М-во образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 2002

9. Алексеев, В.М. Нормативное обеспечение защиты информации от несанкционированного доступа: Учеб. пособие В. М. Алексеев; М-во образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 2002

10. Алексеев, В.М. Обеспечение информационной безопасности при разработке программных средств: Учеб. пособие В.М. Алексеев, В.Г. Каминский, А.С. Овчаров; М-во общ. и проф образования Рос. Федерации. Пенз. гос. ун-т. – Пенза: Изд-во Пенз. гос. ун-та, 1999

11. Алешин, Л.И. Защита информации и информационная безопасность: Курс лекций Л. И. Алешин; Моск. гос. ун-т культуры. – М.: Моск. гос. ун-т культуры, 1999

12. Банки и банковские операции. Учебник / Под ред. Е.Ф. Жукова. – М.: Банки и биржи, ЮНИТИ, 1997

13. Ахраменка, Н.Ф. и др. Преступление и наказание в платежной системе с электронными документами// Управление защитой информации, 1998

14. Барсуков, В.С. Безопасность: технологии, средства, услуги. – М.: Кудиц – Образ, 2001

15. Батурин, Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991

16. Батурин, Ю.М., Жодзишский, А.М. Компьютерная преступность и компьютерная безопасность. М.: Юр.лит., 1991

17. Бахметьев, А.В. Социальные факторы формирования информационного общества / Бахметьев А.В.; Ин-т социал.-полит. исслед. РАН, Фонд поддержки ученых "Науч. перспектива". – М.: Ин-т социал.-полит. исслед.: Фонд поддержки учен.

18. Безруков, Н.Н. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в М5-005. К., 1989

19. Безруков, Н.Н. Компьютерные вирусы. – М.: Наука, 2000

20. Безруков, Н.Н."Классификация компьютерных вирусов и методы защиты от них". – Москва, СП "ICE", 2003

21. Белов, В.Н. Правонарушения, связанные с использованием ЭВМ // Проблемы совершенствования советского законодательства: Труды ВНИ-ИСЭ. Вып. 5. М., 1976

22. Бетелин, В.Б., ред. Вопросы кибернетики. Информационная безопасность. Операционные системы реального времени. Базы данных / Рос. акад. наук. Науч. совет по комплекс. пробл. "Кибернетика". Науч.-исслед. ин-т систем. исслед.; Под ред. В. Б. Бетелина. – М.: НИИ систем. исслед. РАН и др., 1999

23. Браун, С. "Мозаика" и "Всемирная паутина" для доступа к Internet: Пер. с англ. – М.: Мир: СК Пресс, 1999

24. Быков, В.А. Электронный бизнес и безопасность / В. А. Быков. – М.: Радио и связь, 2000

25. Варфоломеев, А.А. Информационная безопасность. Математические основы криптологии: [Учеб. пособие] / А. А. Варфоломеев, В. М. Фомичев ; Моск. гос. инж.-физ. ин-т (техн. ун-т), [Фак. кибернетики]. Ч. 1. – М.: МИФИ, 1995

26. Ведомости РФ. 1992. № 42, ст. 2325

27. Вехов, В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П. Смарогинского. М.: Право и Закон, 1996

28. Водженкин, Б.В. Пояснительная записка к Модельному Уголовному кодексу для государств – участников СНГ // Правоведение. 1996. № 1

29. Волобуев, С.В. Введение в информационную безопасность: Учеб. пособие по курсу "Методы и средства защиты информ." : Для студентов специальностей 220100, 220200, 071900, 552800 С.В. Волобуев; М-во образования Рос. Федерации. Обн. ин-т атом. энергетики. Фак. Кибернетики. – Обнинск: Обн. ин-т атом. энергетики, 2001

30. Волобуев, С.В. Информационная безопасность автоматизированных систем: Учеб. пособие по курсу "Методы и средства защиты информ." С.В. Волобуев; М-во образования Рос. Федерации. Обн. ин-т атом. энергетики. Фак. Кибернетики. – Обнинск: Обн. ин-т атом. энергетики, 2001

31. Всероссийская научно-практическая конференция "Информационная безопасность в системе высшей школы", 28-29 нояб. 2000 г., НГТУ, Новосибирск, Россия: ИБВШ 2000. – Новосибирск, 2001

32. Вус, М.А. ,сост. Проблемы инфомрмационной безопасности: Сб. рефератов студен. науч. работ С.-Петерб. семинар "Информационная безопасность99"; [Сост. - М.А. Вус]. – Спб., 1999

33. Выступление министра внутренних дел РФ "Об экстренных мерах по усилению борьбы с преступностью и личной безопасности граждан РФ" на заседании Государственной думы от 16.1 1.94 г. // Щит и меч. 1994. № 44

34. Гайкович, Ю.В, Першин, А.С. Безопасность электронных банковских систем. – М.: Единая Европа, 1994

35. Галатенко, В.А. Информационная безопасность: практический подход В. А. Галатенко; Под ред. В. Б. Бетелина; Рос. акад. наук, Науч.-исслед. ин-т систем. исслед. – М.: Наука, 1998

36. Галатенко, В.А.. Основы информационной безопасности: Курс лекций: Для студентов вузов, обучающихся по специальности 351400 "Приклад. информатика" В.А. Галатенко; Под ред. В.Б. Бетелина. – М.: Интернет-Ун-т информ. технологий, 2003

37. Геннадиева, Е.Г. Теоретические основы информатики и информационная безопасность: [Учебник] [Геннадиева Е.Г., Дорохов Ф.М., Касилов А.Н. и др.]; Под ред. В.А. Минаева, В.Н. Саблина. – М.: Радио и связь, 2000

38. Гика, Себастиан Нарчис. Сокрытие информации в графических файлах формата BMP Дис. … канд. техн. наук: 05.13.19 – СПб., 2001

39. Гика, Себастиан Нарчис. Сокрытие информации в графических файлах формата BMP: Автореф. дис. ... канд. техн. наук: 05.13.19 С.-Петерб. гос. ин-т точ. механики и оптики. – СПб., 2001

40. Гилстер, П. Новый навигатор Internet: Пер с англ. – Киев: Диалектика, 2002

41. Гринсберг, А.С. и др. Защита информационных ресурсов государственного управления. – М.: ЮНИТИ, 2003

42. Голубев, В.В. Управление безопасностью. – С-Петербург: Питер, 2004

43. Горбатов, В.С. Информационная безопасность. Основы правовой защиты: [Учеб. пособие] В. С. Горбатов, Т. А. Кондратьева; Центр. банк Рос. Федерации, Моск. гос. инж.-физ. ин-т (техн. ун-т). – М.: МИФИ(ТУ), 1995

44. Горлова, И.И., ред. Информационная свобода и информационная безопасность: Материалы междунар. науч. конф., Краснодар, 30-31 окт. 2001 г. [Науч. ред.: Н.И. Горлова и др.]. – Краснодар, 2001

45. Горохов, П.К. Информационная безопасность Англо-рус. слов. П. К. Горохов Information security. – М.: Радио и связь, 1995

46. Государственный стандарт (ГОСТ) 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования" // Бюллет. норм. акт. мин. и ведомств СССР. М., 1989

47. Гуц, Н.Д. Алгоритмы защиты информации на основе управляемых перестановочных операций: Автореф. дис. ... канд. техн. наук: 05.13.19 Санкт-Петербургский гос. ин-т точной механики и оптики. – СПб., 2001

48. Гуц, Н.Д. Алгоритмы защиты информации на основе управляемых перестановочных операций Дис. … канд. техн. наук: 05.13.19 – СПб., 2001

49. Демин, В.С. и др. Автоматизированные банковские системы. – М: Менатеп-Информ, 1997

50. Демин, А.И. Информационная теория экономики. – М.: Проспект, 2002

51. Джонсон, Джордж. Распределенные системы в многофилиальной структуре. – PC Magazine/Russian Edition, 1998., №10

52. Дмитриевский, Н.Н. Информационная безопасность. Борьба с компьютерными вирусами и другими вредоносными программами [Учеб. пособие] Н. Н. Дмитриевский; Моск. инж.-физ. ин-т. – М.: МИФИ, 1993

53. Догадов, А.А. Разработка аппаратно-программного комплекса для автоматизированного обнаружения устройств перехвата акустической информации: Автореф. дис. ... канд. техн. наук: 05.13.19 Моск. инж.-физ. ин-т. – М., 2001

54. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000

55. Женило, В.Р. Специальная техника и информационная безопасность: Учебник [Авт. учеб.: Женило В. Р., Кириллычев А. Н., Кирин В. И. и др.]; Под ред. В. И. Кирина; Акад. управления МВД России. – М.: Акад. упр. МВД России, 2000

56. Жигулин, Г.П. Метод и модель ресурсов поля угроз системы защиты информации сетевых автоматизированных систем : Автореф. дис. ... канд. техн. наук: 05.13.19 С.-Петерб. гос. ин-т точ. механики и оптики (техн. ун-т). – СПб., 2001

57. Жуков, А.В., ред. Информационная безопасность России в условиях глобального информационного общества: Сб. материалов Всерос. конф. Под общ. ред. Жукова А.В. – М., 2001

58. Завгородний, В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001

59. Закон Российской Федерации "Об информации, информатизации и защите информации" // Собр. закон. РФ. № 8. 20 февр. 1995. Ст. 21

60. Закон РФ “О правовой охране программ для ЭВМ и баз данных” // Ведомости РФ. 1992. № 42

61. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. М., 1988. № 10

62. Законодательные меры по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах (по материалам зарубежной печати). 1984. № 6.

63. Законодательство в борьбе с компьютерными преступлениями // Проблемы преступности в капиталистических странах. М., 1989. № 8

64. Законопроекты по борьбе с компьютерной преступностью // Проблемы преступности в капиталистических странах. 1988. № 7

65. Заратуйченко, О.В. Концепции построения и реализации информационных систем в банках. — СУБД, 1996, №4

66. Захаров, М.Ю. Информационная безопасность социума Социально-философское исследование: Дис. … д-ра филос. наук: 09.00.11 – Ростов н/Д, 1998

67. Захаров, М.Ю. Информационная безопасность социума: социально-философское исследование: Автореф. дис. ... д-ра филос. наук: 09.00.11 Ростовский гос. ун-т. – Ростов-на-Дону, 1998

68. Защита информации в информационно-вычислительных системах и сетях // Экономика и жизнь. №30 2001

69. Збруева, Н.А. Информационная безопасность личности, культурологический аспект Дис. … канд. культурол. наук: 24.00.01 – М., 2001

70. Збруева, Н.А. Информационная безопасность личности. Культурологический аспект: Автореф. дис. ... канд. культурологических наук: 24.00.01 Гос. акад. славянской культуры. – М., 2001

71. Здравомыслов, Б.В. Уголовное право РФ. Особенная часть // М.: Юрист, 1996

72. Зегжда, Д.П. ,авт. Информационная безопасность. Защита информации от компьютерных вирусов в сетях ЭВМ Учеб. пособие С. В. Молотков, Д. П. Зегжда, Ю. И. Мазничка, В. А. Петров; [Под ред. А. А. Малюка]; Моск. инж.-физ. ин-т. – М.: МИФИ, 1993

73. Зубик, В.Б. и др. Экономическая безопасность предприятия (фирмы). Минск: Высшая школа, 1998

74. Иванов, А.З. Алгоритмы криптографических преобразований: Учеб. пособие по курсу "Информационная безопасность компьютерных систем" для студентов, обучающихся по спец. 210100 "Управление и информатика в технических системах". – М.: Изд-во МЭИ, 2003

75. Изотов, Б.В. Модели управляемых подстановочных операций и синтез блочных алгоритмов защиты информации: Автореф. дис. ... канд. техн. наук: 05.13.19 Санкт-Петербургский гос. ин-т точной механики и оптики. – СПб., 2001

76. Изотов, Б.В. Модели управляемых подстановочных операций и синтез блочных алгоритмов защиты информации Дис. … канд. техн. наук: 05.13.19 – СПб., 2001

77. Ильюшенко, В. Н., ред. Проблемы информационной безопасности общества и личности: Материалы Первой межрегион. науч.-практ. конф. 24-26 мая 2000 г. г. Томск [Отв. ред.: В. Н. Ильюшенко, А. П. Бацула]. – Томск: Том. гос. ун-т систем упр. и радиоэлектроники

78. Ильюшенко, В.Н. Информационная безопасность общества: Учеб. пособие В. Н. Ильюшенко; М-во общ. и проф. образования РФ. Том. гос. ун-т систем упр. и радиоэлектрон. – Томск, 1998

79. Информатика / Под ред. Проф. Н.В. Макаровой. – М.: Фин. и стат., 1997

80. Информационная безопасность в Санкт-Петербурге: Рабочие материалы семинара гор. Администрации 14 мая 1997 г. СПб.: Высш. адм. шк. Правительства. – СПб., 1997

81. Информационная безопасность в учебных планах вузов России: Материалы межвуз. семинара 26-27 нояб. 1997 г. – СПб., 1997

82. Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов: Межвуз. сб. Саратов: СЮИ МВД России, 2003

83. Информационная безопасность России в условиях глобального информационного общества: 3-я Всерос. конф., Москва, 7-8 февр. 2002 г.: Сб. материалов. – М.: Ред. журн. "Бизнес + Безопасность", 2002

84. Информационная безопасность России в условиях глобального информационного общества "ИНФОФОРУМ-5": Сб. материалов 5-й Всерос. конф., Москва, 4-5 февр. 2003 г. – М.: ООО Ред. журн. Бизнес и Безопасность России, 2003

85. Информационная безопасность: Сб. метод. материалов М-во образования Рос. Федерации [и др.]. – М.: ЦНИИАТОМИНФОРМ, 2003

86. Информационные технологии // Экономика и жизнь. №25, 2001

87. Информационные технологии в маркетинге: Учебник для вузов / Г.А. Титоренко, Г.А. Макарова, Д.М. Дайтбегов и др.; Под. ред. проф. Г.А. Титоренко – М.: 2003

88. Информационные технологии в экономике и управлении: Учебник / Козырев А.А.– М.: Изд-во Михайлова В.А., 2005

89. Информационные технологии управления: Учебн. пособие для вузов / Под ред. проф. Г.А.Титоренко. – М.: ЮНИТИ-ДАНА, 2002

90. Калужин, Р.В. Адаптивное сжатие акустических сигналов и речи в автоматизированных системах защиты и обработки оперативно-розыскной информации: Автореф. дис. ... канд. техн. наук: 05.13.19 Моск. ин-т МВД РФ. – М., 2001

91. Компьютерная “фомка” // Комсомольская правда. 1994. № 82, Мошенники “засветились” на дисплее // Комсомольская правда. 1994. № 74

92. Касперский, Е. Компьютерные вирусы в М5-В05. М., 1992

93. Керашев, А.Т. Информационная безопасность в системе национальной безопасности на Северном Кавказе / А.Т. Керашев; М-во образования Рос. Федерации. Адыг. гос. ун-т. – Майкоп: Адыг. гос. ун-т, 1999

94. Керашев, А.Т. Информационная безопасность и информационная политика в структурогенезе межнациональных отношений: На примере Северного Кавказа: Автореф. дис. ... д-ра полит. наук : 23.00.02 – М., 1999

95. Керашев, А.Т. Информационная безопасность и информационная политика в структурогенезе межнациональных отношений на примере Северного Кавказа: Дис. … д-ра политол. наук: 23.00.04 – М., 1999

96. Кирин, В. И., ред. Информатизация и информационная безопасность правоохранительных органов: XII Междунар. науч. конф., 20-21 мая 2003 г.:[Сб. тр.] [Редкол.: Кирин В. И. (отв. ред.) и др.]. – М.: Акад. упр. МВД России, 2003

97. Кириченко, А. Вирусы научились размножаться по своим законам //Деловые люди. 1995. № 2

98. Кирсанов, К.А. Информационная безопасность: Учеб. пособие К. А. Кирсанов, А. В. Малявина, Н. В. Попов; Моск. акад. экономики и права. – М.: МАЭП, 2000

99. Климова, В. В. ,сост. Современный бизнес: этика, культура, безопасность: Ретросп. библиогр. указ… М-во науки и технологий РФ. ГПНТБ России. – М.: Репрогр. центр ГПНТБ России, 1997

100. Козлов, С.Б., Иванов, Е.В. Предпринимательство и безопасность. М., 1991

101. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – Телеком, 2002

102. Колобов, О.А., Ясенев, В.Н.Информационная безопасность и антитеррористическая деятельность современного государства. Уч. пособие – Н. Новгород, ННГУ, 2001

103. Комментарий к УК РФ / Под общ. ред. Ю.Н. Скуратова и И.Н. Лебедева. М., 1996

104. Комментарий к УК РФ. М.: Институт государства и права Российской академии наук. 1997

105. Компьютеризация банковской деятельности / Под ред. Прф. Г.А. Титоренко. М.: Финстатинформ, 1997

106. Карпычев, В.Ю. Основы информационной безопасности: Учеб. пособие, Н.Новгород.: изд-во ННГУ, 2001

107. Компьютерная преступность в Великобритании // Проблемы преступности в капиталистических странах. М.: ВИНИТИ, 1990. № 8

108. Компьютерные вирусы: что это такое и как с ними бороться: Касперский Е.В.– М: СК Пресс, 2004

109. Компьютерная преступность и информационная безопасность/Под общей ред. А.П. Леонова. – Минск: АРИЛ, 2000

110. Компьютерные преступления и их профилактика // Проблемы преступности в капиталистических странах. М., 1981. № 6

111. Конеев, И.Р. Информационная безопасность предприятия: [Информ. безопасность. Классификация атак. Методика упр. рисками. Криптограф. средства и механизмы] Искандер Конеев, Андрей Беляев. – СПб.: БХВ-Петербург, 2003

112. Коротков, Э.Ю. Разработка интеллектуальной системы анализа и повышения защищенности корпоративной сети от несанкционированного доступа: Автореф. дис. ... канд. техн. наук: 05.13.01, 05.13.19 С.-Петерб. гос. электротехн. ун-т. – СПб., 2001

113. Косоплечев, Н.П., Григорян, В.А., Федулов, И.В. Система мер предупреждения преступности. М., 1988

114. Кравченко, В. Как защитить телефон от подслушивания // МН Коллекция. 1995. №2

115. Кребер, Г. Категория условия и ее соотношение с категорией причины. М., 1961

116. Крылов, В.В. Информационные компьютерные преступления. – М. ИНФРА-М: Норма, 1997

117. Крысин, А. ,сост. Информационная безопасность: Практ. рук. [А. Крысин]. – М.: Спаррк; Киев: Век, 2003

118. Крысин, В.А. Безопасность предпринимательской деятельности. – М:Финансы и статистика, 1996

119. Кудрявцев, В.Н. Причины правонарушений. М., 1976

120. Кузнецова, Н.Ф. Проблемы криминологической детерминации. М., 1984

121. Кураков, Л.П. Информация как объект правовой защиты Л. П. Кураков, С. Н. Смирнов. – М.: Гелиос, 1998

122. Курбатов, В.И. Стратегия делового успеха», Москва, Дашков и Ко, 2002 г.

123. Курушин, В.Д. Компьютерные преступления и информационная безопасность Справочник В. Д. Курушин, В. А. Минаев. – М.: Новый юрист, 1998

124. Лазарев, И.А. Информация и безопасность. – М.: НГЦНТИ, 1997

125. Линьков, И.И. и др. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. – М: ПИТ, 1998

126. Литвинов, Б.Ю. Локальные сети и компьютерные вирусы. – Киев, 1993

127. Лопатин, В.Н. Информационная безопасность в системе государственного управления Теорет. и орг.-правовые проблемы : Дис. … канд. юрид. наук: 12.00.02 – СПб., 1997

128. Леонов, А.П. Безопасность автоматизированных банковских и офисных систем. Минск: НКП Беларуси, 1996

129. Лопатин, В.Н. Информационная безопасность России Дис. … д-ра юрид. наук: 12.00.01 – СПб., 2000

130. Лукашин, В.И. Информационная безопасность: Учеб.-практ. пособие для системы высш. и доп. образования В. И. Лукашин. – М.: Моск. гос. ун-т экономики, статистики и информатики

131. Лучин, И.Н., Желдаков А.А., Кузнецов Н.А. Взламывание парольной защиты // Информатизация правоохранительных систем. М., 1996

132. Мак-Клар, Стюарт. Хакинг в Web. Атаки и защита Стюарт Мак-Клар, Саумил Шах, Шрирай Шах; [Пер. с англ. Е.Н. Василенко [и др.] Пер.:.- Boston etc.: Addison-Wesley, [200?] 0-201-76176-9 – М. [и др.]: Вильямс, 2003

133. Малюк, А.А. Теоретические основы формализации прогнозной оценки уровня безопасности информации в системах обработки данных А. А. Малюк; Моск. гос. инженер.-физ. ин-т (техн. ун-т). – М.: МИФИ, 1998

134. Маркин, С.И. Информационная безопасность: Учеб. пособие С.И. Маркин; М-во образования Рос. Федерации. Тамб. гос. ун-т им. Г. Р. Державина. – Тамбов: Изд-во ТГУ, 2001

135. Мартынов, А.И. Модель и метод трассировки поля угроз безопасности при проектировании систем защиты телекоммуникаций: Автореф. дис. ... канд. техн. наук: 05.13.19 С.-Петерб. гос. ин-т точ. механики и оптики. – СПб., 2001

136. Материалы Второй межведомственной конференции "Научно-техническое и информационное обеспечение деятельности спецслужб", [4-6 февр. 1998 г.]. – М.: УМО по образованию в обл. информ. безопасности

137. Мельников, В.В. Защита информации в компьютерных системах: – М.: Финансы и статистика. Электроинформ, 2004

138. Мельников, В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003

139. Мельников, П.П. Защита информации в автоматизированных системах финансовых и коммерческих организаций Учеб. пособие П. П. Мельников; Финансовая акад. при Правительстве Рос. Федерации, Каф. вычисл. техники. – М.: ФА, 1998

140. Меры по защите программного обеспечения в странах ЕЭС // Борьба с преступностью за рубежом. М.: ВИНИТИ. 1992. № 8

141. Милославская, Н.Г. Интрасети: доступ в Internet, защита = Intranets: Internet access, security: Учеб. пособие для студентов вузов, обучающихся по специальности "Комплекс. обеспечение информ. безопасности автоматизир. систем" Н.Г. Милославская, А.И. Толстой Intranets: Internet access, security. – М.: ЮНИТИ, 2000

142. Минаев, В.А., ред. Компьютерные технологии в криминалистике и информационная безопасность Тр. акад. Акад. упр. МВД России; [Редкол.: В. А. Минаев (отв. ред.) и др.]. – М.: Акад. упр. МВД РФ, 1997

143. Митрохина, Е.Ю. Информационная безопасность личности как социологическая проблема: Автореф. дис. ... канд. социол. наук: 22.00.06 Ин-т социально-политич. исслед. – М., 1999

144. Митрохина, Е.Ю. Информационная безопасность личности как социологическая проблема Дис. … канд. социол. наук: 22.00.06 – М., 1999

145. Михайлов, С.Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции [Учеб. пособие] С. Ф. Михайлов, В. А. Петров, Ю. А. Тимофеев; Центр. банк Рос. Федерации (Банк России), Моск. гос. инж.-физ. ин-т (техн. ун-т). – М.: МИФИ(ТУ), 1995

146. Михайлов, С.Ф. Петров, В.А., Тимофеев, Ю.А. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. – М.: МИФИ, 2000

147. Московский университет и развитие криптографии в России: Материалы Конф. в МГУ, 17-18 окт. 2002 г. – М.: МЦНМО, 2003

148. Мостовой, Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. – №8. 2000

149. Мур, Г. Глобальный информационный рынок. – Материалы агентства VDM-News, мониторинг иностранной прессы, 14.01.99

150. Мячев, А.А., Степанов, В.Н., Щербо, В.К. Интерфейсы систем обработки данных: Справочник. М.: Радио и связь, 1989

151. Научно-практический комментарий к УК РФ. Н. Новгород: Номос, 1996

152. Некоторые проблемы борьбы с компьютерными преступлениями// Проблемы преступности в капиталистических странах. 1990. № 7

153. Никифоров, С.Г. Исследование устойчивости автоматизированных систем охраны предприятий к несанкционированным действиям: Автореф. дис. ... канд. техн. наук: 05.13.06, 05.13.19 С.-Петерб. гос. электротехн. ун-т (ЛЭТИ). – СПб., 2001

154. Оголюк, А.А. Метод и механизмы защиты информационных систем уровневым контролем списков санкционированных событий: Автореф. дис. ... канд. техн. наук: 05.13.19 С.-Петерб. гос. ин-т точ. механики и оптики (техн. ун-т). – СПб., 2002

155. Орлов, В.А. Системы безопасности. – М.: Инфра - М, 2004

156. Отавин, А.Д. Интеграционный подход к построению защищенных распределенных вычислительных систем: Автореф. дис. ... канд. техн. наук: 05.13.19 С.-Петерб. гос. техн. ун-т. – СПб., 2001

157. Партыка, Т. Л., Попов И.И.. Информационная безопасность. М Форум инфра-м, 2004

158. Партыка, Т.Л. Информационная безопасность: Учеб. пособие для студентов учреждений сред. проф. образования, обучающихся по специальностям информатики и вычисл. техники Т. Л. Партыка, И. И. Попов. – М.: Форум : Инфра-М, 2002

159. Першиков, В.И., Савинков В.М. Толковый словарь по информатике. М., 1991

160. Петренко, С.А. Аудит безопасности Intranet: Информ. технологии для инженеров Петренко С.А., Петренко А.А. – М.: Компания АйТи : ДМК Пресс, 2002

161. Петров В.А., Пискарев, С.А., Шеин, А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. – М., 1998

162. Полевой, Н.С. Правовая информатика и кибернетика: Учебник. М.: Юр. лит., 1993.

163. Попов, В.Б. Основы компьютерных технологий / В.Б. Попов. – М.: Финансы и статистика, 2002

164. Попов, С.А. Информация и безопасность: Учеб. пособие : Специальность: 071900 Информ. системы на трансп. 220700 Комплекс. обеспечение информ. безопасности автоматизир. систем Попов С.А., Францев Р.Э., Коршунов И.Л.; М-во трансп. Рос. Федерации. С.-Петерб. гос. ун-т вод. Коммуникаций. – СПб.: С.-Петерб. гос. ун-т вод. коммуникаций, 2000

165. Предотвращение компьютерных преступлений // Проблемы преступности в капиталистических странах. М.: ВИНИТИ, 1986. № 4

166. Приложение к журналу "Юридический бюллетень предпринимателя". М., 1996.

167. Приходько, А.Я. Словарь-справочник по информационной безопасности / А. Я. Приходько. – М.: СИНТЕГ, 2001

168. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом. М.: ВИНИТИ. 1992. № 4

169. Просихин, В.П. Методология построения архитектуры безопасности распределенных компьютерных систем: Автореф. дис. ... д-ра техн. наук : 05.13.19 Петербургский гос. ун-т телекоммуникации им. проф. М. А. Бонч-Бруевича. – СПб., 2001

170. Просихин, В.П. Методология построения архитектуры безопасности распределенных компьютерных систем Дис. … д-ра техн. наук: 05.13.19 – СПб., 2001

171. Проскурин, В.Г. Защита в операционных системах: Програм.-аппарат. средства обеспечения информ. безопасности : Учеб. пособие для студентов вузов, обучающихся по

специальностям "Защищ. телекоммуникац. системы", "Орг. и технология защиты информ.", "Комплекс. обеспечение информ. безопасности автоматизир. систем" В.Г. Проскур. – М.: Радио и связь, 2000

172. Пэрри, У. ЭВМ и организация бухгалтерского учета, пер с англ. – М.: Финансы и статистика, 1986

173. Работа с ПК / Под ред. А. Тихонова; Игоров Б. А. Пер. с англ. – М.: БИНОМ, 2000

174. Разбирин, С.А. Информационная безопасность фирмы: (Организац.-правовой аспект) Сергей Разбирин. – Липецк: Изд-во ЛЭГИ, 2000

175. Различные аспекты компьютерной преступности // Проблемы преступности в капиталистических странах. М.: ВИНИТИ, 1987. № 3

176. Рарог, А.И. Уголовное право России // Институт межд. права и экон. М.: 1996

177. Ржавский, К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учеб. пособие для студентов вузов, обучающихся по специальностям "Автоматизир. системы обраб. информ.", "Комплекс. обеспечение информ. безопасности автоматизир. систем" К.В. Ржавский. – Волгоград: Изд-во Волгогр. гос. ун-та, 2002

178. Рогозин, В.Ю. Преступления в сфере компьютерной информации, информационная безопасность и средства защиты компьютерной информации: Лекция В. Ю. Рогозин; М-во внутр. дел Рос. Федерации. Волгогр. юрид. ин-т. – Волгоград: Волгогр. юрид. ин-т МВД России, 2000

179. Россия на пороге информационного общества: Материала Семинара 22 апр. 1997 г. в рамках Науч. конф. Фак. журналистики СПбГУ "Средства массовой информации в соврем. мире". – СПб., 1997

180. Ростовцев, А.Г. Методология проектирования алгоритмов аутентификации для критических информационно-телекоммуникационных систем: Автореф. дис. ... д-ра техн. наук: 05.13.19 С.-Петерб. гос. техн. ун-т. – СПб., 2001

181. Рудакова, О.С. Банковские электронные услуги. – М.: ЮНИТИ, 1997

182. Румянцев, А. Банкоматный вор работал под колпаком // Известия. 1995. № 235

183. Садердинов, А.А., Трайнев, В.А., Федулов, А.А. Информационная безопасность предприятия: Учебное пособие. 2-е изд. – М.: Издательско-торговая корпорация «Дашков и К°», 2004

184. Санкин, Л.А. , ред. Информационное право: информационная культура и информационная безопасность: Материалы Всерос. науч.-практ. конф., 17-19 окт. 2002 г. [Сост.: Л. А. Санкин [и др.]. – СПб.: СПбГУП, 2002

185. Сахаров, А.В. Информационная безопасность организационно-технических систем: Автореф. дис. ... д-ра техн. наук: 05.27.05, 05.12.21 Моск. гос. авиац. ин-т. – М., 2000

186. Сахаров, А.В. Информационная безопасность организационно-технических систем Дис. … д-ра техн. наук: 05.27.05, 05.12.21 – М., 2000

187. Селиванов, Н.А. Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8.

188. Семеновых, В.А. Некоторые вопросы информационно-аналитической работы в банке. – Материалы Семинара «Практические вопросы информационно-аналитической работы в коммерческом банке», 24-26.03.98

189. Симаков, В.В., Балакирев, С.В. Многоканальный цифровой комплекс регистрации и обработки аудиоинформации // Информатизация правоохранительных систем. М.: Академия МВД России, 1996

190. Системы безопасности: Межотраслевой темат. кат. – М.: Groteck, 2001

191. Смирнов, М.И.,. Трубилин, И.Т, Лойко, В.И., Барановская, Т.П. Автоматизированные информационные технологии в экономике. – М.: Финансы и статистика, 2000

192. Смолинов, С.В. Информационная безопасность военнослужащих США в 50-90-е гг. XX века По опыту локальных войн и военных конфликтов: Дис. … канд. ист. наук: 07.00.03 – М. 2000

193. Смолинов, С.В. Информационная безопасность военнослужащих США в 50-90-е гг. XX века: По опыту локальных войн и военных конфликтов: Автореф. дис. ... канд. ист. наук: 07.00.03 – М., 2000

194. Снытников, А.А. Лицензирование и сертификация в области защиты информации [Учеб. пособие] А. А. Снытников. – М.: Гелиос АРВ, 2003

195. Соколов, А.В., Шаньгин, В.Ф Защита информации в распределенных корпоративных сетях и системах, ДМК Пресс, 2002

196. Спесивцев, А.В., Вегнер, В.А., Крутяков, А.Ю. и др. Защита информации в персональных ЭВМ. М.: Радио и связь, 1992

197. Специальная техника и информационная безопасность: Учебник / [Авт. Учеб.: Женило В. Р., Кириллычев А. Н., Кирин В. И. и др.]; Под ред. В. И. Кирина; Акад. управления МВД России. Т. 1., 2000

198. Степанов, Е.А. Информационная безопасность и защита информации: Учеб. пособие для студентов вузов, обучающихся по специальности "Документоведение и документац. обеспечение упр." Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2001

199. Столингс, В. Основы защиты сетей. Приложения и стандарты, пер. с англ. – М.: Диалектика - Вильямс, 2002

200. Тарасов, П.И. Диасофт предлагает комплексные решения для банков. — Мир ПК, 1998, №5

201. Титоренко, Г.А. Автоматизированные информационные технологии в экономике. – М.: Юнити, 2004

202. Титоренко, Г.А. и др. Компьютеризация банковской деятельности. – М.: Финстатинформ. 1997

203. Тихомиров, Л.И. Основы построения информационных систем нефтяной отрасли с использованием информационно-безопасных интернет- и интранет-технологий : На примере ЗАО "Лукойл-Пермь": Автореф. дис. ... канд. техн. наук: 05.13.01, 05.13.19 Гос. НИИ управляющих машин и систем. – Пермь, 2001

204. Торокин, А.А. Основы инженерно-технической защиты информации". – Издательство «Ось-89», 1999

205. Тушнолобов, И.Б., Урусов Д.П., Ярцев В.И. Распределенные сети. – СПБ: Питер, 1998

206. Уголовное право России. Учебник. М.: ИМП, 1996

207. Уголовный кодекс Российской Федерации от 13.06.1996 года № 63-ФЗ с изменениями и дополнениями.

208. Устинов, В.С. Криминология // СПб.: ВШ МВД РФ, 1995

209. Устинов, Г.Н. Основы информационной безопасности систем м сетей передачи данных: Учеб. пособие для студентов по специальностям 200900 и 550400 и аспирантов ВУЗов Г.Н. Устинов. – М.: СИНТЕГ, 2000

210. Уфимцев, Ю.С. ,сост. Информационная безопасность России Моск. акад. экономики и права; [Ю.С. Уфимцев и др.]. – М.: Экзамен, 2003

211. Файтс, Ф., Джонстон, П. Компьютерный вирус: проблемы и прогноз. М.: Кратц, 1993

212. Федоров, В. Компьютерные преступления: выявление, расследование и профилактика // Законность. 1994. № 6

213. Фигурнов, В.Э. IBM PC для пользователей. М.: ИНФРА–М, 1996

214. Фисун, А. П. Информация и информационная безопасность: Учеб. пособие для курсантов и слушателей образоват. учреждений высш. проф. образования МВД России юрид. профиля [Фисун А. П., Касилов А. Н., Дорохов Ф. М. и др.]; Под ред. В. А. Минаева, А. П. Фисуна; Дальневост. юрид. ин-т МВД России. – Хабаровск: Дальневост. юрид. ин-т МВД России, 2002

215. Фомичев, В.М. «Дискретная математика и криптология». – М.: Диалог-МИФИ, 2003 г.

216. Ходжаев, А.Г. Оценка стойкости систем защиты информации и скоростные алгоритмы преобразования данных в системах Дис. … канд. техн. наук: 05.13.19 – М., 2001

217. Ходжаев, А.Г. Оценка стойкости систем защиты информации и скоростные алгоритмы преобразования данных в системах: Автореф. дис. ... канд. техн. наук: 05.13.19 Моск. гос. акад. приборостроения и информатики. – М., 2001

218. Хорев, А.А. «Антивирусные программы». – М.: МО РФ, 2002

219. Царегородцев, А.В. Информационная безопасность в распределенных управляющих системах: Монография А. В. Царегородцев. – М.: Изд-во Рос. ун-та дружбы народов, 2003

220. Цветков, В.Я. Технологии и системы информационной безопасности: Аналит. обзор В.Я. Цветков; М-во пром-сти, науки и технологий Рос. Федерации. Всерос. науч.-техн. информ. Центр. – М.: ВНТИЦ, 2001

221. Цыганков, В.Д. Психотроника и безопасность России. – М.: СИНТЕГ, 2003

222. Черешкин, Д.С. Методика оценки рисков нарушения информационной безопасности в автоматизированных информационных системах / Д.С. Черешкин, А.А. Кононов, Е.Г. Новицкий. В.Н. Цыгичко; Ин-т систем. анализа РАН. – М.: ИСА РАН, 1999

223. Черкасов, В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 1994

224. Чугуев, А.Д., Захарин, С.И. Вирусный бизнес криминальной среды как социальная база для развития преступной деятельности по созданию вирусов // Подготовка специалистов в условиях изменяющейся структуры преступности и обновляющегося законодательства России. Волгоград: ВСШ МВД РФ, 1994

225. Шаковец, А.Н. Основы защиты компьютерной информации и информационная безопасность: Лекция А.Н. Шаковец, Н.В. Рымарева; М-во внутрен. дел России, Дальневосточ. юрид. ин-т. – Хабаровск: Дальневосточ. юрид. ин-т МВД РФ, 2003

226. Шаньгин, В.Ф. Защита информации и информационная безопасность: Учеб. пособие : [В 2 ч.] / В. Ф. Шаньгин; М-во общ. и проф. образования Рос. Федерации. Моск. гос. ин-т электрон. техники (Техн. ун-т). Ч. 2., 2000

227. Швец, Д.Ю. Информационная безопасность России и современные международные отношения / Д. Ю. Швец. – М.: Мир безопасности, 2001

228. Шийко, А.С. Политика борьбы с компьютерной преступностью как угрозой информационной безопасности России: Автореф. дис. ... канд. полит. наук : 20.01.02 Рос. акад. гос. службы при Президенте РФ. – М., 2001

229. Шишкин, А.Д. Программирование на языке Си: Учеб. пособие А.Д. Шишкин; М-во образования Рос. Федерации. Рос. гос. гидрометеорол. ун-т. – СПб.: РГГМУ, 2003

230. Шнайер, Б. Информационная безопасность и прикладная криптология. – Издательство Триумф, 2003

231. Шумилов, Н.И. Криминалистические аспекты информационной безопасности Дис. … канд. юрид. наук: 12.00.09 – СПб., 1997

232. Экономическая информатика и вычислительная техника / Под ред. В.П. Косарева, А.Ю. Королева. – М.: Финансы и статистика, 1999

233. Экономическая информатика и вычислительная техника: Учебник / Титоренко Г.А., Черняк Н.Г., Еремин Л.В. и др.; Под ред. В.П.Косарева, А.Ю.Королева – М.: Финансы и статистика, 2002

234. Экономическая информатика. Учебник / Под ред. В.П. Косарева и Л.В. Еремина. – М.: Финансы и Статистика, 2002.

235. Экономическая эффективность систем информационной безопасности. Чеботарь П.П. – Молдовская экономическая академия, 2003

236. Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учеб. для студентов вузов ж.-д. трансп. В. В. Яковлев, А. А. Корниенко. – М., 2002

237. Ярочкин, В.И. Информационная безопасность. – М.: Мир, 2003

238. Ярочкин, В.И. Информационная безопасность: Учеб. для студентов вузов, обучающихся по гуманитар. и соц.-экон. Специальностям. – М.: Фонд "Мир", 2003: Акад. Проект

239. Ясенев, В.Н. Автоматизированные информационные системы в экономике и обеспечение их безопасности: Учебное пособие. – Н.Новгород, 2002

240. Ясенев, В.Н. Компьютеризация бухгалтерского учета. – Н.Новгород: изд-во ННГУ, 1995

241. Ясенев, В.Н. Экономическая информатика и вычислительная техника. – Н.Новгород, ННГУ, 1996

242. Ястребов, Д.А. Информационная безопасность: термины и определения / Д. А. Ястребов. – М.: ТИССО, 2002

243. Ярочкин, В.И. Информационная безопасность: Учеб. для студентов вузов. – М.: Гаудеамус, 2 изд., 2004

244. Computer Fraud. 1987. 9. № 12

245. Criminology. 1988. 26. № 1

246. Novell NetWare. Руководство пользователя, 1998

247. http://demo.cintech.ua

248. http://marketsurveys.ru

249. http://www.cislink.com

250. http://www.client.uniastrum.ru

251. http://www.duma.gov.ru

252. http://www.infin.ru

253. http://www.intertrust.ru
254. http://www.maprf.ru
255. http://www.sbcinfo.ru
256. http://www.softlab.ru
257. http://www.strongdisk.ru
258. http://zakon.kuban.ru/uk/uk_gl28.htm

Вячеслав Николаевич **Ясенев**

В.Н. Ясенев

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИЧЕСКИХ СИСТЕМАХ

Учебно-методическое пособие

Государственное образовательное учреждение высшего профессионального образования
«Нижегородский государственный университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23.

Подписано печать 14.02.2006. Формат 60x84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл.печ.л.9,0.
Заказ №235. Тираж 700 экз.

Отпечатано в типографии Нижегородского государственного университета
Им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37
Лицензия ПД№ 18-0099 от 14.05.01