МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

Информационная безопасность

Учебное пособие
под общей редакцией проф. Ясенева В.Н.

Рекомендовано ученым советом института экономики и предпринимательства для студентов ННГУ, обучающихся по направлению подготовки 38.03.01 «Экономика»

Нижний Новгород
2017

УДК 311 (075.8)
ББК У051

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

Рецензенты:
Зав. Кафедрой «Экономики и экономической безопасности»
Нижегородской правовой академии
Академик финансовой академии «Элита» проф., д.э.н. Чеботарев В.С.
Зав.кафедрой «Финансы и кредит» проф., д.э.н. Яшина Н.И.

В настоящем пособии изложены материалы для самостоятельной работы студентов бакалавриата, включающие краткое изложение основных тем дисциплины, контрольные вопросы, тесты и задания для студентов.

Учебное пособие предназначено для студентов бакалавриата, обучающихся по направлению38.03.01 «Экономика» в Институте экономики и предпринимательства ННГУ им. Н.И. Лобачевского.

Ответственный за выпуск:
председатель методической комиссии ИЭП ННГУ,
к.э.н., доцент Летягина Е.Н.

УДК 311 (075.8)
ББК У051

СОДЕРЖАНИЕ

Предисловие……..……..4
Тема 1. Теоретические аспекты информационной безопасности экономических систем……..6
Контрольные вопросы и тесты……...17
Тема 2. Понятие информационных угроз и их виды……20
Контрольные вопросы и тесты……...52
Тема 3.Государственное регулирование информационной безопасности…….54
Контрольные вопросы и тесты……...76
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности…….79
Контрольные вопросы и тесты……...98
Тема 5. Организация системы защиты информации……..101
Контрольные вопросы и тесты…….149
Тема 6. Менеджмент и аудит систем информационной безопасности……...153
Контрольные вопросы и тесты…….188
7. Учебно-методическое обеспечение самостоятельной работы обучающихся…….191
Список использованных источников…….195

Предисловие

Дисциплина «Информационная безопасность» относится к базовой части учебного плана по ряду направлений 38.03.01 «Экономика», обязательна для освоения на 1–м курсе во 2–м семестре. Основное назначение данной дисциплины состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

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

В ходе изучения дисциплины студенты должны комплексно применять знания, навыки и умения, полученные при изучении «Информатики».

Минимальный уровень освоения содержания дисциплины предполагает:

- Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;
- Уяснение вопросов обеспечения информационной проблем создания (концептуального проектирования) систем информационной безопасности;
- Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ.

Содержательные аспекты дисциплины «Информационная безопасность» логически связаны с такими учебными дисциплинами как: «Информатика», «Информационные системы в экономике», «Менеджмент», «Маркетинг», «Финансы», «Бухгалтерский учет» и др.

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

Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, лабораторных занятий и самостоятельной работы, должны всесторонне использоваться студентами на завершающем этапе обучения в бакалавриате, при обучении в магистратуре, а также в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

Реализация компетентностного подхода при изучении дисциплины «Информационная безопасность» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр по актуальным проблемам, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

Практические занятия проводятся в компьютерных классах с применением специализированных информационных систем, комплексов и технологий бизнес-индустрии.

Тематика практических заданий ориентирована на рассмотрение аналитических типовых и исследовательских задач финансово-экономического характера.

В ходе самостоятельной работы, при подготовке к плановым занятиям и экзамену студенты анализируют поставленные преподавателем задачи с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет.

Тема 1. Теоретические аспекты информационной безопасности экономических систем

1. Основные понятия информационной безопасности экономического объекта.
2. Экономическая информация как товар и объект безопасности
   Контрольные вопросы и тесты

1.Основные понятия информационной безопасности экономического объекта

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.

Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации. Под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются.

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. 1 Структура понятия «Информационная безопасность»

Понятие информационной безопасности в узком смысле этого слова подразумевает:

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

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

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

К объектам информационной безопасности на предприятии относят:

❖ информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;

❖ средства и системы информатизации - средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

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

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

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

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или 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 имеет:

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.

2.Экономическая информация как товар и объект безопасности

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.

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-Предприятие" 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.

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.

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.

Персональные данные

1) Персональные данные – любая информация, относящаяся к физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

2) Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) Фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) Наименование (фамилия, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) Цель обработки персональных данных;

4) Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способом обработки персональных данных;

6) Срок, в течение которого действует согласие, а также порядок его отказа.

Контрольные вопросы по теме 1

1. Назовите особенности современного информационного общества.
2. Какие элементы информационной инфраструктуры Вы знаете?
3. Что понимается под угрозой безопасности информации?
4. Дайте определение информационной безопасности на предприятии.
5. Назовите объекты информационной безопасности на предприятии.
6. Какие обеспечивающие подсистемы включает система защиты информации?
7. Назовите особенности экономической информации.
8. В чем отличия понятий информационный ресурс, продукт и услуга?
9. Как определяется цена информационного продукта?
10. Что такое конфиденциальность, целостность и доступность информации?
11. Какая информация компании не может быть отнесена к коммерческой тайне?
12. Что такое персональные данные?

Тесты к теме №1

1. Информационная война – это…

А. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

2. Информационная безопасность – это…

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. надежность работы компьютера;

В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;

Б. средства вычислительной и организационной техники;

В. Конституция России.

5. Обеспечение безопасности информации – это…

А. одноразовое мероприятие;

Б. комплексное использование всего арсенала имеющихся средств защиты;

В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;

В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности – это?

А. антивирусные программы;

Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;

В. комплекс математических методов, связанных с оценкой опасности технических средств.

8.Информационное обеспечение информационной безопасности – это?

А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

Б. антивирусные программы;

В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. совокупность средств;

В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

А. раскрытие конфиденциальной информации;

Б. нарушение принципов экономической безопасности;

В. отказ от обслуживания.

11. Информационное оружие – это?

А. комплекс технических средств, методов и технологий, направленных против управленческих систем;

Б. нормативно-правовая база по информационной безопасности;

В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности – это..?

А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;

Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;

В. широкое использование технических средств защиты информации.

13.Экономическая информация является товаром?

А. да;

Б. нет;

В. кроме конфиденциальных сведений.

14. К числу особенностей информации как товара НЕ относятся:

А. сохраняемость;

Б. несамостоятельность;

В. самостоятельность.

15 .Информация может составлять коммерческую тайну, если:

А. к ней нет свободного доступа на законном основании;

Б. содержится в учредительных документах;

В. содержится в бухгалтерском балансах.

16. Не являются коммерческой тайной?

А. сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;

Б. сведения о научных разработках;

В. сведения о персонале предприятия.

17. Конфиденциальность компьютерной информацией – это?

А. предотвращение проникновения компьютерных вирусов в память ПЭВМ;

Б. свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;

В. безопасное программное обеспечение.

18. Банковская тайна – это..?

А. информация о банковском счете, вкладе, операциях по счету, о клиентах банка;

Б. информация о сотрудниках банка;

В. информация о режиме работы банка.

19. Объектами профессиональной тайны НЕ являются:

А. тайна страхования;

Б. врачебная тайна;

В. бухгалтерский баланс.

Тема 2. Понятие информационных угроз и их виды

1. Информационные угрозы, их виды, причины.
2. Компьютерные преступления, их виды.

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.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

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.

Классификация информационных угроз представлены на рис.2, 3.

Рис.2. Типы информационных угроз

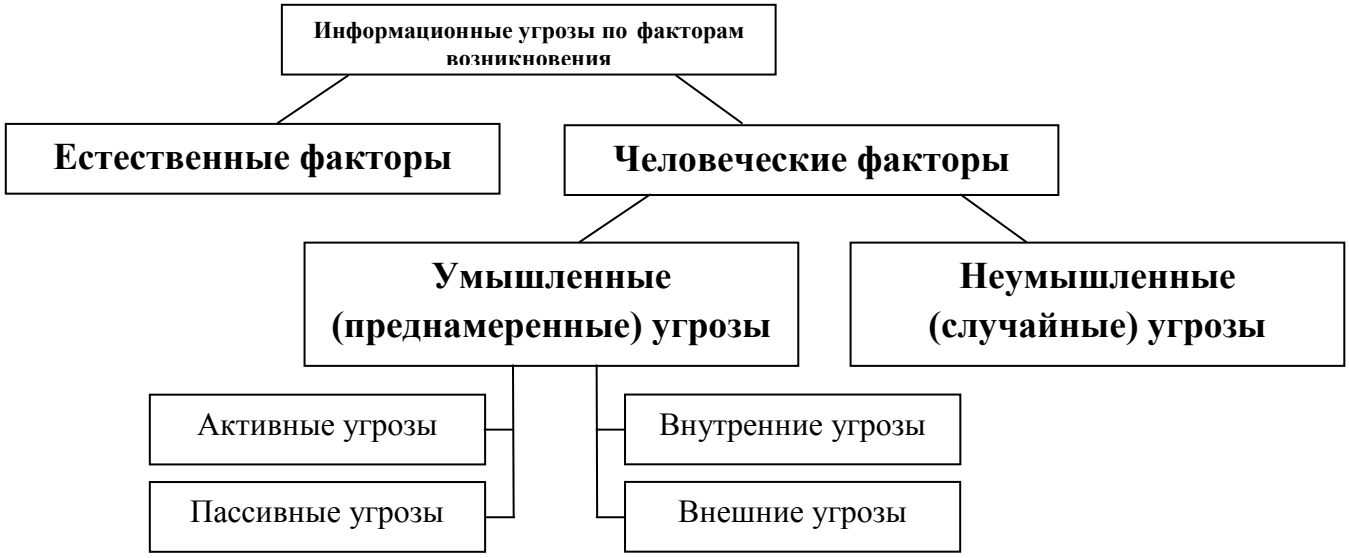


Рис.3. Классификация информационных угроз по факторам возникновения

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 пр01раммы 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 но 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. 4).

Рис. 4. Действия и события, нарушающие информационную безопасность

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

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;

- несанкционированного доступа к конфиденциальной информации различными способами.

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

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

По физической природе возможны следующие средства переноса информации:

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

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

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

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

К факторам утечки могут, например, относиться:

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

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.5.

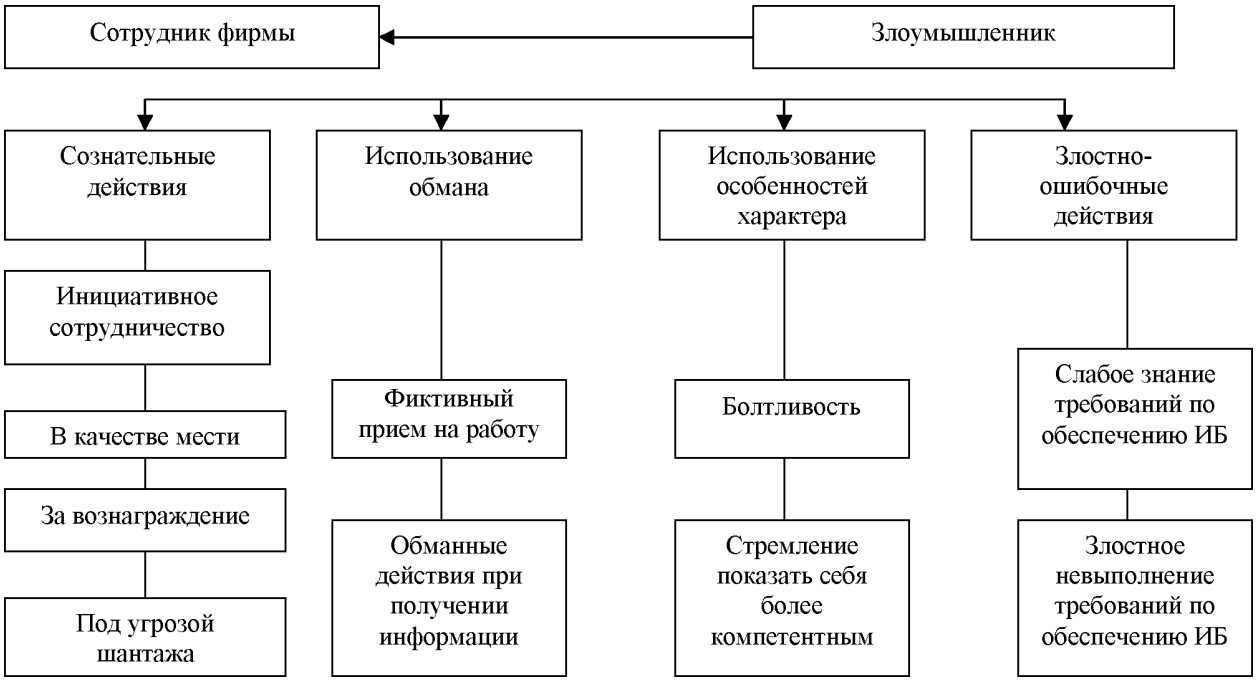


Рис. 5. Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались. Типы и субъекты информационных угроз представлены в табл.1.

Таблица 1

Типы и субъекты угроз

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

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

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

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

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

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

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

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

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

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

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

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

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.

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

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

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

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

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

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

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

- транспорт.

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

- несанкционированные внешние воздействия из Internetна 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 Internetили 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 Internetили 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 средствзащиты 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 снарушением конфиденциальности информации, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

4. По причине появления используемой ошибки защиты.

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

Такая ошибка может быть обусловлена одной из следующих причин:

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

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

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

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

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

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

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом.

Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных и программе, в частности «маскарад», при котором пользователь присваивает себе каким-либо образом полномочия другого пользователя выдавая себя за него.

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

Воздействию могут подвергаться следующие компоненты:

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

- объекты системы - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевыеустройства, 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.

2.Компьютерные преступления и их виды

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

Сетью Интернет в совокупности со своими внутренними информационными сетями пользуются все банки и корпорации, аккумулирующие на своих счетах крупные денежные средства, лакомый кусок для разного рода компьютерных мошенников. Число преступных посягательств на имущество, совершаемых путём злоупотребления доверием или обманом, продолжает расти. В качестве статистических данных приведём отчёт Центра статистической информации Главного информационно-аналитического центра МВД России: в Российской Федерации за 2015 год было зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159.1 - 159.6 УК РФ (по сравнению с прошедшим годом, это больше на 25 процентов, в 2014 году было зарегистрировано 160214 подобных преступлений). При этом небывалыми темпами растёт число мошенничеств в сфере компьютерной информации (995 зарегистрированных преступлений в 2014 году против 5443 в 2015 году). Раскрываемость же подобных деяний оставляет желать лучшего: в 2015 году она находилась на уровне 7,4 %. По итогам четырёх месяцев 2016 года негативная тенденция остаётся: зарегистрировано 1789 мошенничеств в сфере компьютерной информации (на 143,7% больше). В числе лидеров по количеству данных преступлений: Тюменская область (333 зарегистрированных преступления), Удмуртия (298), Республика Коми (223) . Раскрыто всего 72 преступления (на 5,3% меньше по сравнению с аналогичным периодом 2015 года). Низкая раскрываемость данного вида преступлений обусловлена достаточно высоким уровнем подготовки злоумышленников. Обычно они имеют как профессиональное образование, так и необходимую техническую аппаратуру, существенно облегчающую сокрытие следов при совершении компьютерных мошенничеств.

Увеличение числа киберпреступлений объясняют рост потребности владельцев информационных ресурсов (предприятий, организаций, государственных ведомств) в реализации систематических, всеобъемлющих мер по обеспечению информационной безопасности. Все негативные воздействия на объекты информационной безопасности можно разделить на три вида: нарушение конфиденциальности информации; разрушение (утеря, необратимое изменение) информации; недоступность информационных ресурсов - возникновение ситуаций, когда пользователи (все или их часть) на некоторый период времени теряют возможность доступа к необходимым данным (или информационным системам)[37].

На практике основными наиболее распространенными способами нарушения информационной безопасности являются: получение несанкционированного доступа к личной и конфиденциальной информации и их модификация, несанкционированное использование информационных ресурсов с целью получения выгоды или нанесения ущерба, кража электронных денег, осуществление атак типа «отказ в обслуживании» - распространение вирусов и других вредоносных программ, осуществляющих различные негативные воздействия.

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.

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.

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

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 более общем виде способы совершения КП можно классифицировать на:

- несанкционированный доступ;

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

Несанкционированный доступ включает:

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

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

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

- документы, содержащие интересующую их информацию;
- технические носители;
- информацию, обрабатываемую в информационных системах.

Под модификацией информации понимается внесение в нее любых изменений, 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.

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:

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 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.

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

- *Физические злоупотребления,* которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.

- *Операционные злоупотребления,* представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.

- *Программные злоупотребления,* которые включают в себя: различные способы изменения системы математического обеспечения («логическая бомба»– введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; «троянский конь»– включение в обычную программу своего задания).

- *Электронные злоупотребления,* которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

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

• *Методы перехвата.*

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

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

• Методы несанкционированного доступа.

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. 2) [58].

Таблица 2

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

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

«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.

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

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

Методики несанкционированного доступа сводится к двум разновидностям:

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

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

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

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

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;

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

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

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

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

Уивинг – одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе «запутывания следов». Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети – Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы.

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

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

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

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

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

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

«Логическая бомба»– тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

«Временная бомба»– разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

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

Типологизация компьютерных преступников представлена на рис.6.

Рис. 6. 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.

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	Руково-дитель	Прог раммист	Инженер (техник)	Пользо-ватель	Конкурент
Изменение кодов	+		+			
Копирование файлов	+		+			
Уничтожение файлов	+	+	+		+	+
Присвоение программ			+	+		+
Шпионаж	+	+	+			+
Установка			+	+		+
Саботаж	+		+	+		+
Продажа данных	+	+	+		+	
Воровство		+	+		+	+

Субъектов компьютерных преступлений с точки зрения профессиональной подготовленности принято подразделять на лиц, совершающих преступления:

а) «нетехнические»;

б) «технические», требующие минимума специальных знаний;

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

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

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

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

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

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

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

- корысть;
- ошибка пользователей и программистов неумышленного характера;

безответственность в организации системы информационной безопасности;

- самоутверждение путем демонстрации своего превосходства;
- месть за какие-либо действия администрации;
- недостатки созданных информационных систем и технологий.

Полагается, что преступления в сфере компьютерной информации являются «беловоротничковыми преступлениями» («БП»– это такие правонарушения, при совершении которых имеет место нанесение ущерба торговле, нарушение страховых и валютных правил, взяточничество и т.п.). В 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.

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.

История компьютерных вирусов представлена на рис.7.

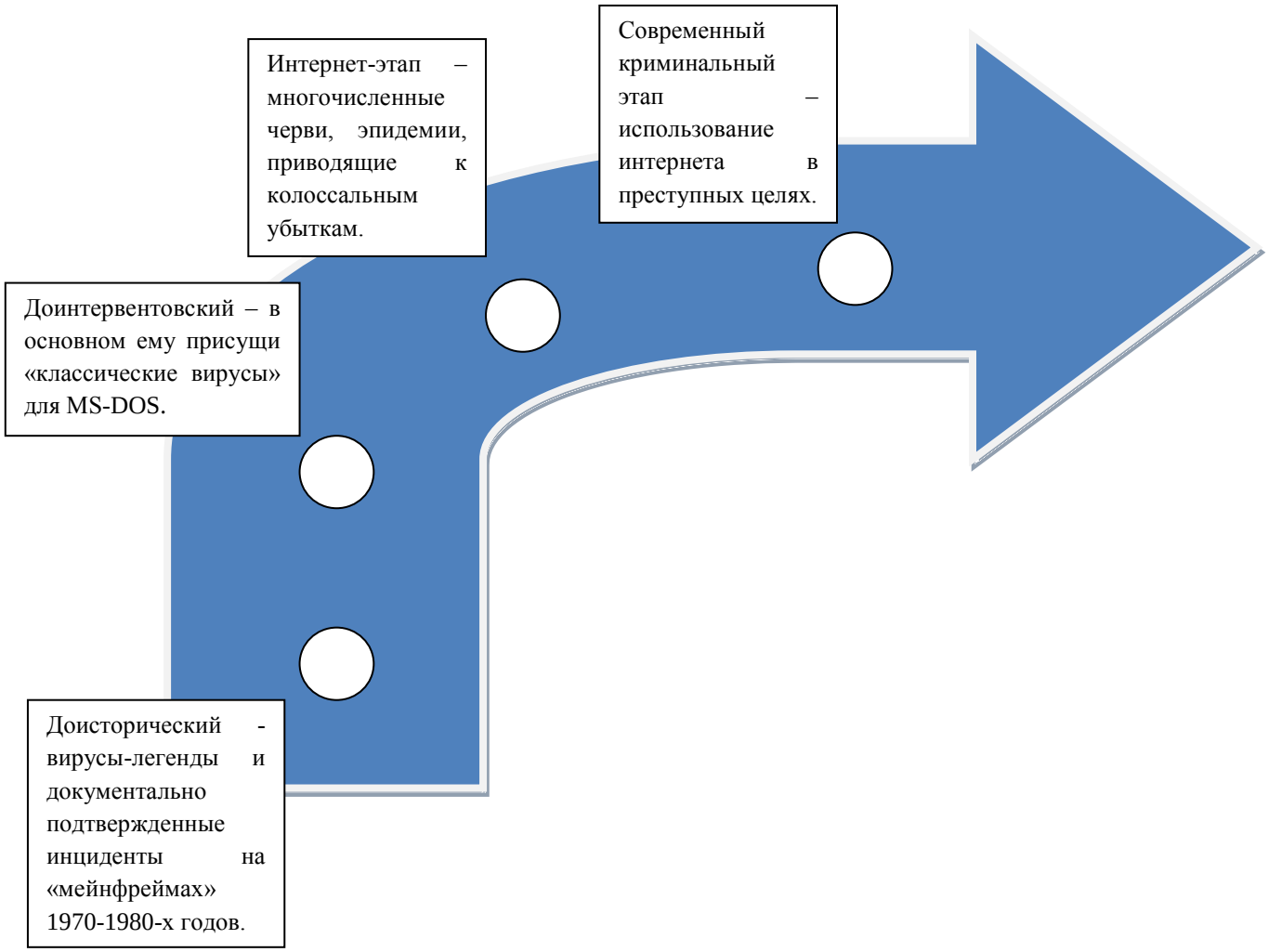


Рис. 7. История компьютерных вирусов.

Классификация способов несанкционированного копирования представлены на рис.8.

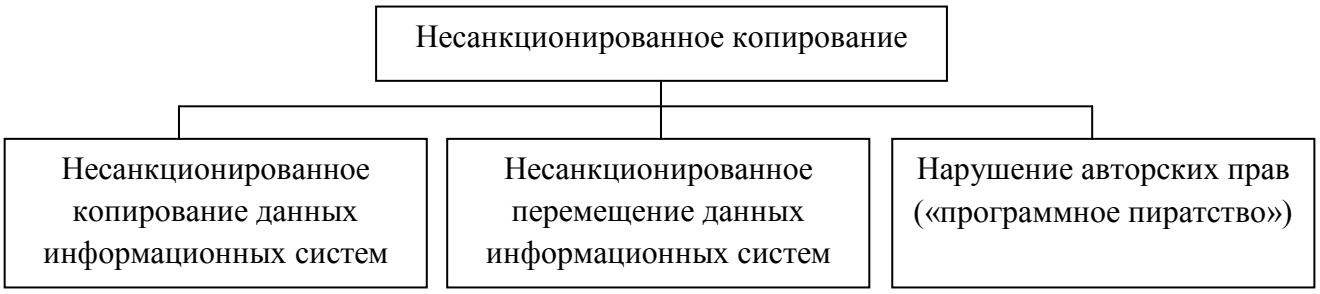


Рис. 8. Несанкционированное копирование информации

В последнее время к этим особенностям, характерным для вирусов компьютерных, 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.

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

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

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

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

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

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

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

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

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

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

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

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить

такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов и пр.

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

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.

«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.

«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 ниже.

Классификация компьютерных вирусов по среде обитания:

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

Классификация компьютерных вирусов по способам 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

С учетом особенностей алгоритма вируса выделяют:

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;

- сообщение, требующее выплаты компенсации за восстановление файлов компьютеров (вирусы-вымогатели).

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 и может быть прекращена (вирусы-вымогатели);
- некоторые файлы оказываются испорченными и т.д.

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

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

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

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

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

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

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

В настоящий момент известно два семейства MMS-червей:

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

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

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

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

Справочник угроз при работе в интернет

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих программ было самораспространение; некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы – типичные проявления кибервандализма.

В чем разница между вирусом и червем?

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

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

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

Что такое рекламные системы (adware)?

Понятие «adware» включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без

ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.
Устаревшие, не обновленные вовремя версии веб-браузеров могут быть уязвимыми для хакерских инструментов, скачивающих рекламные программы на ваш компьютер.

Контрольные вопросы к теме 2

1. Назовите информационные угрозы для государства.
2. Какие создаются информационные угрозы для компании?
3. Что угрожает личности (физическому лицу)?
4. Назовите причины информационных угроз.
5. Какие действия и события нарушают ИБ?
6. Какие личностно-профессиональные характеристики сотрудников способствуют реализации угроз ИБ?
7. Назовите основные компьютерные вирусы.
8. Какие вы знаете компьютерные преступления?

Тесты к теме 2

1.Несанкционированным доступом является:

А. недостаточное знание работниками предприятия правил защиты информации;
Б. слабый контроль за соблюдением правил защиты информации;
В. хищение носителей информации и документальных отходов.

2. Реализации угроз информационной безопасности способствуют:
А. болтливость;
Б. простудные заболевания;
В. Налоговый кодекс.

3. Типовыми путями несанкционированного доступа к информации, являются:
А. дистанционное фотографирование;
Б. выход из строя ПЭВМ;
В. ураганы.

4. Несанкционированным доступом к информации НЕ является:
А. использование программных ловушек;
Б. любительское фотографирование;
В. включение в библиотеки программ специальных блоков типа «троянский конь».

5. К способам воздействия угроз на информационные объекты НЕ относятся:
А. программно-математические;
Б. организационно-правовые;
В. договорные отношения.

6. Хакерная война – это?
А. атака компьютеров и сетей гражданского информационного пространства;

Б. использование информации для влияния на умы союзников и противников;
Б. блокирование информации, преследующее цель получить экономическое превосходство.

7. Угрозы доступности данных возникают в том случае, когда?
А. объект не получает доступа к законно выделенным ему ресурсам;
Б. легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;
В. случаются стихийные бедствия.

8. Внедрение компьютерных вирусов является следующим способом воздействия угроз на информационные объекты?
А. информационным;
Б. физическим;
В. программно-математическим способом.

9. Логическая бомба – это?
+А. компьютерный вирус;
Б. способ ведения информационной войны;
В. прием, используемый в споре на философскую тему.

10. Объектом информационной атаки не является:
А. АИС в целом;
Б. каналы передачи данных;
В. природоохранные мероприятия.

11. Под «маскарадом» понимается?
А. выполнение каких-либо действий одним пользователем от имени другого пользователя;
Б. обработка денежных счетов при получении дробных сумм;
В. монополизация какого-либо ресурса системы.

12. «Люком» называется?
А. использование после окончания работы части данных, оставшиеся в памяти;
Б. передача сообщений в сети от имени другого пользователя;
В. не описанная в документации на программный продукт возможность работы с ним.

13. «Мобильные» вирусы распространяются:
А. путем взлома программ ВЭВМ;
Б. в виде «червей» и «троянцев» для мобильных телефонов;
В. по линии связи между узлами сети.

14.Для компьютерных преступлений НЕ характерна:
А. сложность сбора доказательств;
Б. наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ;
В. высокая латентность.

Тема 3. Государственное регулирование информационной безопасности

1. Деятельность международных организаций в сфере информационной безопасности
2. Нормативно-правовые акты в области информационной безопасности в РФ

1. Деятельность международных организаций в сфере информационной безопасности

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Менеджмент информационной безопасности предполагает выделение нескольких ИБ:

1. Уровень международных профессиональных объединений, связанных со сферой информационных технологий, телекоммуникаций и информационной безопасности.

2. Уровень крупных компаний, работающих в сфере информационных технологий и в значительной мере определяющих состояние информационной безопасности в сообществе пользователей информационных систем, а также влияющих на безопасность различных элементов информационной инфраструктуры.

3. Государственный уровень - уровень государственных и межправительственных организаций, влияющих на жизнь общества, состояние правовой системы, развитие экономики и технологий.

4. Уровень отдельных компаний - сообщество пользователей информационных систем, заинтересованных в собственной информационной безопасности и обеспечивающих защиту имеющихся у них информационных ресурсов собственными силами.

Некоторые исследователи выделяют дополнительный промежуточный уровень - консалтинговые и внедренческие компании, учебные центры, работающие в сфере информационной безопасности и действующие как связующее звено между различными организационными уровнями.

Для каждого уровня указанной иерархии характерны свои задачи и специфичные методы организационной работы[25].

Выделяют несколько типов международных организаций, действующих в сфере информационной безопасности и оказывающих существенное влияние на функционирование глобальных информационных систем и деятельность всего информационного сообщества:

1. Крупные международные некоммерческие и неправительственные организации, объединяющие специалистов в определенных областях, существующие, как правило, уже в течение многих лет и охватывающие множество основных направлений развития компьютерной инженерии, электроники и телекоммуникаций, включая в том числе и определенные вопросы обеспечения безопасности современных информационных технологий.

2. Отдельные относительно небольшие организации, которые специализируются на более или менее узких вопросах информационной безопасности, имеющих глобальное значение для всего сообщества пользователей информационных систем, и появились на

базе частных компаний или исследовательских структур в течение последнего десятилетия, когда проблемы информационной безопасности стали особенно актуальными.

3. Совместные структуры (комитеты, альянсы и т.п.), создаваемые (иногда временно) крупными компаниями (иногда при участии крупных исследовательских центров, учебных заведений и правительственных структур) для решения определенных задач в сфере информационных технологий и информационной безопасности [42].

Для каждого типа характерны свои специфические организационные особенности, но их объединяет решение общей задачи разработки, согласования и дальнейшего распространения общих для всего сообщества пользователей информационных систем технических и организационных решений, к числу которых относятся протоколы глобальных сетей; архитектуры, алгоритмы, протоколы публичных средств шифрования данных; правила построения глобальных сетей обмена данными и других элементов глобальной инфраструктуры информационной безопасности [53].

В качестве важных элементов организационной работы на уровне международных структур являются:

- организация обмена знаниями и актуальными новостями в среде специалистов по информационной безопасности в таких формах, как публикация специализированных периодических изданий и сборников научных работ, организация специализированных научно-практических конференций, семинаров и т.п.;

- организация и поддержание в актуальном состоянии баз данных и баз знаний, которые содержат сведения, необходимые пользователям информационных систем, администраторам, разработчикам и другим участникам для обеспечения информационной безопасности. В качестве примера можно привести базы данных, содержащие сведения о выявленных уязвимостях различных программных и аппаратных платформ информационных систем [19].

Для организационной работы международных структур не характерна универсальность, поскольку их отличает самостоятельное построение работы на некоторых общих организационных принципах: принципе самофинансирования; принципе добровольности участия в работе таких структур и в отдельных проектах или во всей работе; принципе открытости (доступности) результатов работы (всех или их части) для сообщества специалистов в сфере информационных технологий [32].

К числу основных и наиболее крупных известных международных профессиональных объединений в сфере информационной безопасности относят ITU - International Telecommunication Union; IEEE - Institute of Electrical and Electronics Engineers; ACM - Association for Computing Machinery; W3 Consortium; ISSA - Information Systems Security Association; ISO - International Organization for Standardization; IETF - Internet Engineering Task Force; ICSA - International Computer Security Association;Information Systems Audit and Control Association (ISACA); Internet Security Alliance [43].

Более подробно рассмотрим деятельности отдельных организаций. Начнем со старейшей - InternationalTelecommunicationUnion (ITU) - Международный союз электросвязи. Она была основана в 1885 году как Международный телеграфный союз и получила свое новое название в 1934 году. В настоящее время ITU объединяет 189 государств. Первоначально ее задачей изначально было управление и координация деятельности в сфере передачи информации и, в частности, в радиосвязи и телеграфной

связи. Однако по мере развития глобальных компьютерных сетей и интеграции компьютерных и телекоммуникационных систем, область деятельности ITU была значительно расширена и в настоящее время включает в себя множество вопросов, связанных с построением компьютерных сетей, передачей цифровых данных, обработкой информации и т.п. Членами ITU-T являются государственные органы власти (министерства и ведомства связи отдельных стран); научные организации и компании - производители телекоммуникационного оборудования; региональные и международные телекоммуникационные организации.

Структура ITU-T включает 4 функциональных органа: Всемирную ассамблею по стандартизации телекоммуникаций (WorldTelecommunicationStandardizationAssembly), проводимую каждые четыре года, - основной руководящий орган сектора стандартизации; Бюро по стандартизации телекоммуникаций (TelecommunicationStandardizationBureau) - исполнительное подразделение сектора стандартизации; исследовательские группы (всего их 14); консультативную группу по стандартизации телекоммуникаций (TelecommunicationStandardizationAdvisoryGroup) - вспомогательное подразделение, осуществляющее координационную работу.

Наиболее известной международной организацией в сфере информационной безопасности является InstituteofElectricalandElectronicsEngineers (IEEE) - Институт инженеров по электронике и электротехнике. Она существует с 1884 года и в настоящее время насчитывает около 380000 членов из 150 стран мира. В сферу ее интересов входит множество вопросов, связанных с электротехникой, радиоэлектроникой, вычислительной техникой, информатикой, а также некоторыми разделами физики и математики. Организация работает в следующих основных направлениях: проведение специализированных профессиональных конференций; публикация специализированных изданий; поддержка образовательной деятельности; поддержка инновационных технических и методических разработок в различных сферах; разработка и распространение технических стандартов.

Одной из старейших ассоциаций является AssociationforComputingMachinery (ACM) - Ассоциация вычислительной техники, созданная в 1947 году. Основные задачи ACM - поддержка образовательных проектов в сфере информационных технологий, организация научно-практических конференций, симпозиумов и семинаров, общественно-политическая работа, связанная с информационными технологиями, публикация периодических изданий и сборников научных трудов, посвященных проблемам современных информационных технологий, поддержка электронного архива таких публикаций, а также другая подобная деятельность.

WorldWideWebConsortium (W3C) - Консорциум Всемирной Паутины. Создание W3C было инициировано в 1989 году с целью разработки единых, согласованных стандартов обмена информацией в глобальных сетях передачи данных, а официально создание консорциума было оформлено в 1994г. для обеспечения возможности доступа к сети Интернет для как можно большего числа людей, обеспечение возможности подключения к Интернет различных технических устройств, обеспечение возможности структурирования и формализации интернет-информации, обеспечение надежности и безопасности обмена информацией. К настоящему времени консорциум объединяет более четырехсот ведущих технологических и телекоммуникационных компаний, правительственных организаций, исследовательских центров, институтов и университетов

по всему миру. Кроме того, в штате консорциума состоят около 70 независимых технических экспертов, обеспечивающих его работу.

International Organization for Standardization (ISO) - Международнаяорганизацияпостандартизации. ISOбыла учреждена в 1946г. как неправительственное объединение национальных организаций по стандартизации, нацеленное на унификацию стандартов в различных областях производственной деятельности и оказания услуг. Помимо основных членов (156 стран), непосредственно участвующих в работе, в ISOтакже входят члены-корреспонденты (Correspondentmember) - страны, не имеющие полноценных органов стандартизации, а также члены-подписчики (Subscribermember) - страны с небольшими экономиками, получающие необходимую справочную информацию на льготных условиях. Главным органом управления ИСО является ежегодная Генеральная Ассамблея, принимающая стратегические решения, касающиеся развития всей организации, подготовкой которых занимается Совет ИСО на собраниях, проходящих два раза в год. Непосредственно разработкой стандартов занимаются технические комитеты и подкомитеты с участием представителей заинтересованных стран. Проекты международных стандартов, принятые техническими комитетами, рассылаются в национальные организации для голосования; документ приобретает статус международного стандарта, если за него проголосовало не менее 75% членов, участвовавших в голосовании. Основным подразделением ИСО, занимающимся вопросами информационной безопасности, является Объединенный технический комитет JTC1 «Информационные технологии», в состав которого входит подкомитет SC27 «Средства безопасности в информационных технологиях» (ГГSecuritytechniques) [51].

ДЕЯТЕЛЬНОСТЬ СПЕЦИАЛИЗИРОВАННЫХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ И ОБЪЕДИНЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Функционирование специализированных организаций, имеющих глобальное влияние на управление информационной безопасностью на различных уровнях и общее состояние информационной безопасности, осуществляется, как правило, на базе:

- частных компаний, занимающихся исследованиями, разработками и консультированием в сфере информационной безопасности;
- крупных учебных заведений, специализирующихся на информационных технологиях, а также обладающих существенным авторитетом и финансовыми ресурсами;
- правительственных учреждений, ответственных за обеспечение информационной безопасности в определенных сферах [44].

Основным направлением организационной работы становится формирование и поддержание баз данных, содержащих информацию о ставших известными уязвимостях различных программных и аппаратных средств, а также другие формы и направления информационной, консультативной и методической работы в данной сфере. В качестве важных факторов успешности в данном случае выступает объединение информации из как можно большего числа источников и как можно более эффективное распространение знаний в сообществе пользователей информационных систем. Для данной формы организационной работы характерны отсутствие общих правил работы и изменения в составе организаций [16].

В настоящее время можно выделить следующие наиболее значимые организации, занимающие эту нишу: CERTCoordinationCenter- Координационный центр *CERT,*

Исследовательская группа X-Forceкомпании IBM.

CERTCoordinationCenter (CERT/CC) - Координационный центр CERT,возникшая в 1988 году как Computersecurityincidentresponseteam(Группа реагирования на инциденты, связанные с компьютерной безопасностью), функционирует на базе Института разработки программного обеспечения при Университете Карнеги-Мелон(SoftwareEngineeringInstitute, CarnegieMellonUniversity) и финансируется Министерством обороны и Министерством национальной безопасности США.

X-Forcesecurityintelligenceteam - Исследовательская группа X-Forceотносится к компании InternetSecuritySystems(755) - наиболее авторитетного поставщика комплексных решений в сфере информационной безопасности, клиентами которого являются все без исключения крупнейшие компании США, а также правительственные организации. В конце 2006 года 755 была куплена компанией IBMи интегрирована в нее в качестве самостоятельного подразделения. Одной из задач группы X-Forceявляется поддержание в актуальном состоянии базы данных известных уязвимостей различных программных и аппаратных платформ.

Также одним из направлений справочно-информационной деятельности этой исследовательской группы является оказание услуг по индивидуальному анализу угроз информированию (X-Force*Threat*AnalysisService (XFTAS)). Данный комплекс услуг позволяет заказчикам ежедневно получать адаптированную актуальную информацию об угрозах и уязвимостях с учетом особенностей построения их информационных систем (платформ, приложений, сферы ведения бизнеса, географического положения) и включает в себя информацию об угрозах; экспертный анализ угроз; описание текущего и прогнозного состояния угроз; рекомендуемые способы устранения угроз; количественный анализ атак за последние 30 дней. Еще одной из задач группы является выпуск периодических (ежеквартальных, ежегодных) информационных бюллетеней с обзорами наиболее значимых событий в сфере информационной безопасности.

Альянсы крупных технологических компаний представляют собой временные (заключаемые на краткосрочную или среднесрочную перспективу) или долгосрочные соглашения между несколькими фирмами, направленные на совместное, скоординированное, целенаправленное решение определенных масштабных и ресурсоемких задач развития технологии, формирования рыночного спроса на определенные продукты и организации инфраструктуры информационной безопасности.

SmartCardAlliance (SCA) - Альянс по смарт-картам занимается вопросами развития технологии смарт-карт - одной из ключевых технологий в сфере информационной безопасности, используемой для идентификации пользователей различных сервисов и информационных систем (таких как мобильные телефонные сети, банковские «электронные кошельки» и т.п.). Этот долгосрочный (стратегический) альянс был образован в начале 2001 года путем слияния двух организаций: SmartCardIndustryAssociationи SmartCardForum.В состав альянса входят около сотни различных компаний и правительственных организаций.

InternetSecurityAlliance (ISA) - Альянс по безопасности сети Интернет создан в апреле 2001 года по инициативе двух крупных авторитетных организаций: *CERTJCC*Университета Карнеги-Меллон и Ассоциации электронной промышленности (ElectronicIndustriesAlliance, EIA). Уже к середине 2004 года в альянс входило около тридцати членов, в числе которых такие крупные компании, как Boeing, NEC, Mitsubishi, FederalExpress, AIG, Sony, Symanteси другие. В состав альянса входят около тридцати

ассоциированных членов. На первоначальном этапе создания альянса его основной задачей было повышение эффективности обмена информацией об уязвимостях, распространяемой *CER7JCC.*

TheInternationalBiometricIndustryAssociation (IBIA) - Международная ассоциация компаний-производителей биометрического оборудования создана в 1998 году с целью коллективной поддержки интересов компаний, связанных с производством биометрического оборудования. Основной задачей является взаимодействие с потенциальными заказчиками их продукции с целью продвижения средств биометрической идентификации. Членами ассоциации являются около 30 компаний и организаций, среди которых Hitachi, LGElectronics, Panasonic, NEC и другие [45].

2.Нормативно-правовые акты в области информационной безопасности в РФ

Первоначально, столкнувшись с компьютерной преступностью, органы уголовной юстиции государства 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 (например, воровство из квартиры – это одно, а копирование секретной компьютерной информации – это другое).

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

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

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

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

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

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.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Службы, организующие защиту информации на уровне предприятий (банков и др.):

- отдел экономической безопасности;
- служба безопасности персонала (режимный отдел);
- службы информационной безопасности;
- отдел кадров.

Нормативно-правовые акты в области информационной безопасности в РФ представлены на рис.9.

Рис.9. Нормативно-правовые акты в области информационной безопасности в РФ

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

- ***Акты федерального законодательства*:**
  - Международные договоры РФ;
  - Конституция РФ [1];
  - Законы федерального уровня (включая федеральные конституционные законы, кодексы) [6-10];
  - Указы Президента РФ [2];
  - Постановления Правительства РФ [3];
  - Нормативные правовые акты федеральных министерств и ведомств;
  - Нормативные правовые акты субъектов РФ, органов местного самоуправления и т.д.

К нормативно-методическим документам можно отнести

- Методические документы государственных органов России:

- Доктрина информационной безопасности РФ (Утверждена указом Президента Российской Федерации от 5 декабря 2016 г. №646) [2];
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ.
- Документы и стандарты, регламентирующие защиту объектов информатизации от несанкционированного доступа к информации.
- Документы и стандарты, регламентирующие требования к подсистеме криптографической защиты.

- Документы, регламентирующие защиту объектов информатизации от воздействий вредоносных программ.
- Документы и стандарты, регламентирующие особенности защиты сетей передачи данных.
- Документы и стандарты, регламентирующие защиту объектов информатизации от утечки информации по техническим каналам.
- Документы и стандарты, регламентирующие защиту зданий, помещений и контролируемых зон объекта информатизации.
- Документы и стандарты, регламентирующие защиту объекта информатизации от внешних воздействующих факторов.
- Стандарты, регламентирующие требования к оформлению документации и документов на объект информатизации.
- Документы и стандарты, регламентирующие оценку качества объекта информатизации, виды испытаний этих объектов.
- Стандарты в области терминов и определений.
- Правовой режим информации, средств информатики, индустрии информатизации и систем информационных услуг в условиях риска, средства и формы защиты информации.
- Правовой статус участников правоотношений в процессах информатизации.
- Порядок отношений субъектов с учетом их правового статуса на различных стадиях и уровнях процесса функционирования информационных структур и систем.

Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”

Итак, правовое обеспечение компьютерной безопасности включает нормы, осуществляющие общественные отношения, возникающие в процессе деятельности физических лиц, организаций и государственных органов.

Правовое обеспечение информационной безопасности означает:

- *защиту интересов физических лиц* - путем введения норм, устанавливающих пределы сбора и использования сведений об этих лицах со стороны государства и иных субъектов;
- *защиту интересов государства и общества* - путем установления приоритетов защиты информации, охраняемой как собственность государства [1];
- *защиту интересов юридических и физических лиц* - путем установления норм, регулирующих обращение с охраняемой информацией, обеспечивающей деятельность этих лиц, и установления механизмов защиты этих субъектов.

Правовое обеспечение компьютерной безопасности включает в себя виды деятельности, представленные на рис. 10.

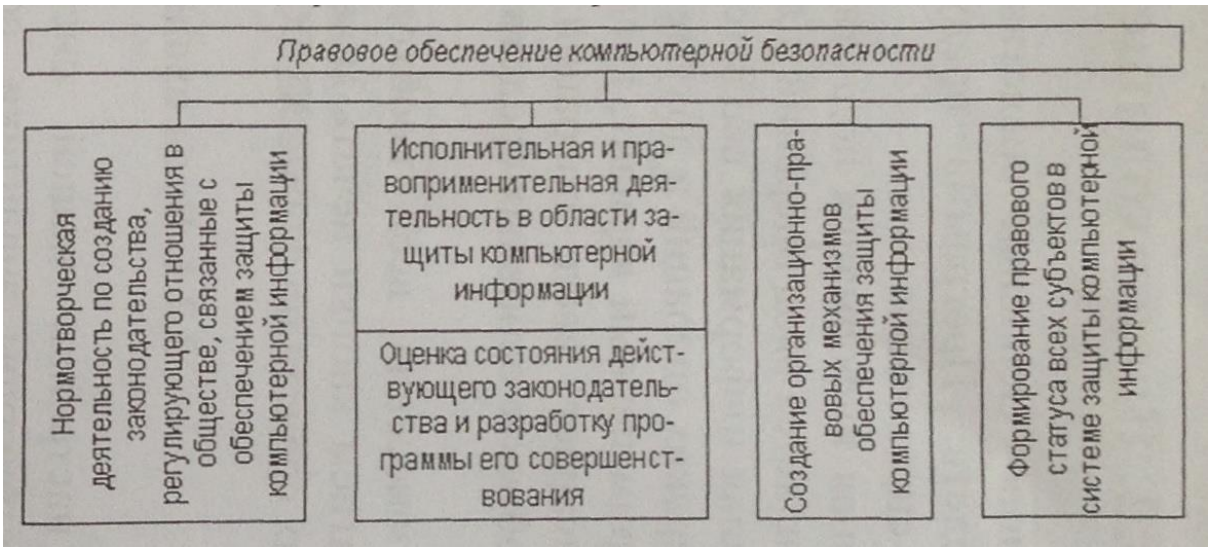


Рис.10. Составляющие правового обеспечения ИБ

В 2016 году утверждена новая **Доктрина информационной безопасности России.** [2].

В ней определены стратегические цели и основные направления обеспечения информационной безопасности.

Проанализированы основные информационные угрозы. Дана оценка состоянию информационной безопасности.

Отмечается, что практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

На состояние информационной безопасности влияет, в частности, тот факт, что некоторые зарубежные страны наращивают возможности информационно-технического воздействия на информационную инфраструктуру в военных целях. Усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских госорганов, научных организаций и предприятий ОПК.

Отмечается тенденция к увеличению в иностранных СМИ объема материалов с предвзятой оценкой отечественной госполитики. Российские СМИ зачастую подвергаются за рубежом откровенной дискриминации.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия. Возрастают масштабы компьютерной преступности.

Приводятся основные направления обеспечения информационной безопасности в области обороны, государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, стратегической стабильности и равноправного стратегического партнерства.

Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности в соответствии со стратегией являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и

предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности,

разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является **Совет безопасности РФ.**

Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является **Федеральная служба по техническому и экспортному контролю – ФСТЭК**. Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также **Служба специальной связи и информации ("Спецсвязь России")**, с 2004 года входящая в состав Федеральной службы охраны. Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

- Министерство связи и массовых коммуникаций РФ;
- Министерство внутренних дел РФ.

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия *по* обеспечению защиты информации:

- ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);
- Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр "Атомзащитаинформ");
- Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации) и некоторые другие.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, **информационной,** экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ, осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия *по* информационной безопасности. Функциями Управления информационной безопасности являются:

- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних *угроз информационной безопасности* и подготовка предложений Совету Безопасности по их предотвращению;
- рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;
- участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;
- подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ. [14]

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как **Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия РФ)**, была создана в январе 1992 года на базе Гостехкомиссии СССР *по* противодействию иностранным технологическим разведкам, которая, в свою *очередь* ведет отсчет своего существования с декабря 1973 года. Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и других.

Основными функциями ФСТЭК являются:

- проведение единой технической политики и координация работ по защите информации;
- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;
- поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций *по* лицензированию в составе ФСТЭК функционируют 7 региональных управлений (*по* федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь России), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

При этом задачами Спецсвязи также являются:

- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи России;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;

- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих *государственную тайну*;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи России;
- выполнение требований обеспечения информационной безопасности объектов государственной охраны.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды *работ* в сфере информационной безопасности:

- подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;
- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;
- выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Уполномоченным органом *по* ведению реестра доверенных удостоверяющих центров является ФГУП НИИ "Восход".

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти *по* защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ. [15]

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является **Комитет по безопасности Государственной думы Федерального собрания Российской Федерации**. В составе этого Комитета функционирует **Подкомитет по информационной безопасности.** В законодательной работе в рамках этого Комитета принимают участие:

- специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и других ведомств;
- руководители Совета безопасности РФ и других правительственных органов;
- представители общественных организаций, фондов и профессиональных объединений;
- представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);

- представители ведущих научно-исследовательских учреждений и учебных заведений.

Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается или наказывается обществом, что так поступать не принято. В рамках обеспечения информационной безопасности следует рассмотреть на законодательном уровне две группы мер:

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

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

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

В Уголовном кодексе РФ имеются нормы, затрагивающие вопросы информационной безопасности граждан, организаций и государства. В числе таких статей ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых и телеграфных или иных сообщений», ст. 140 «Отказ в предоставлении гражданину информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст.159.1-159.6 «Мошенничество», 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. [57].

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.

Принято Постановление Правительства РСФСР О перечне сведений, которые не могут составлять коммерческую тайну (от 5 декабря 1991 г. №35).

В соответствии с этим Постановлением 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 договор учредителей) и Устав;

документы, дающие право заниматься предпринимательской деятельностью (документы, подтверждающие факт внесения записей о юридических лицах в Единый

государственный реестр юридических лиц, свидетельства о государственной регистрации индивидуальных предпринимателей, лицензии, патенты) (абзац в редакции, введенной в действие с 24 октября 2002 года постановлением Правительства Российской Федерации от 3 октября 2002 года N 731;

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 мест;

документы об уплате налогов и обязательных платежах;

сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, не соблюдений 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 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

В Федеральном законе от 21.07.1993 г №5485-1 «О государственной тайне» представлены следующие статьи [6]:

Раздел I. Общие положения

• Статья 1. Сфера действия настоящего Закона

• Статья 2. Основные понятия, используемые в настоящем Законе

• Статья 3. Законодательство Российской Федерации о государственной тайне

• Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты

Раздел II. Перечень сведений, составляющих государственную тайну

• Статья 5. Перечень сведений, составляющих государственную тайну

Раздел III. Отнесение сведений к государственной тайне и их засекречивание

• Статья 6. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений

• Статья 7. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

• Статья 8. Степени секретности сведений и грифы секретности носителей этих сведений

• Статья 9. Порядок отнесения сведений к государственной тайне

• Статья 10. Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием

• Статья 11. Порядок засекречивания сведений и их носителей

• Статья 12. Реквизиты носителей сведений, составляющих государственную тайну

Раздел IV. Рассекречивание сведений и их носителей

• Статья 13. Порядок рассекречивания сведений

• Статья 14. Порядок рассекречивания носителей сведений, составляющих государственную тайну

• Статья 15. Исполнение запросов граждан, предприятий, учреждений, организаций и органов государственной власти Российской Федерации о рассекречивании сведений

Раздел V. Распоряжение сведениями, составляющими государственную тайну

• Статья 16. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями

• Статья 17. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ

• Статья 18. Передача сведений, составляющих государственную тайну, другим государствам или международным организациям

• Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений

Раздел VI. Защита государственной тайны

• Статья 20. Органы защиты государственной тайны

• Статья 21. Допуск должностных лиц и граждан к государственной тайне

• Статья 21.1. Особый порядок допуска к государственной тайне

• Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

• Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне

• Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне

• Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну

• Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

• Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

• Статья 28. Порядок сертификации средств защиты информации

Раздел VII. Финансирование мероприятий по защите государственной тайны

• Статья 29. Финансирование мероприятий по защите государственной тайны

Раздел VIII. Контроль и надзор за обеспечением защиты государственной тайны

• Статья 30. Контроль за обеспечением защиты государственной тайны

• Статья 30.1. Федеральный государственный контроль за обеспечением защиты государственной тайны

• Статья 31. Межведомственный и ведомственный контроль

• Статья 32. Прокурорский надзор.

Основополагающими документами в сфере информационных технологий и информационной безопасности является Федеральный закон «Об информации, информационных технологиях и о защите информации»(от 27 июля 2006 года N 149-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_61798/) [8].

Он включает следующие статьи:

Статья 1. Сфера действия настоящего Федерального закона.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе.

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации.

Статья 5. Информация как объект правовых отношений.

Статья 6. Обладатель информации.

Статья 7. Общедоступная информация.

Статья 8. Право на доступ к информации.

Статья 9. Ограничение доступа к информации.

Статья 10. Распространение информации или предоставление информации.

Статья 11. Документирование информации.

Статья 12. Государственное регулирование в сфере применения информационных технологий.

Статья 13. Информационные системы.

Статья 14. Государственные информационные системы.

Статья 15. Использование информационно-телекоммуникационных сетей.

Статья 16. Защита информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

В 2006 (с изм. на 1 января 2017г.) принят ФЗ «О персональных данных» № 152, направленный на защиту личной информации. Инициатива законодателей была своевременна: участились случаи мошенничества, связанные с использованием персональных данных, в том числе для изъятия крупных сумм денег. Этот закон является предпосылкой для обеспечения должного уровня безопасности хранения информации, защиты от утечек из баз данных крупных организаций: государственных структур, страховых компаний, it-компаний и других.

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

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

Субъектами права здесь выступают:

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

Персональные данные и работа с ними должны соответствовать следующим требованиям:

1. Персональные данные должны быть получены и обработаны законным образом на основании действующего законодательства.

2. Персональные данные включаются в базы персональных данных на основании свободного согласия субъекта, выраженного в письменной форме, за исключением случаев, прямо установленных в законе.

3. Персональные данные должны накапливаться для точно определенных и законных целей, не использоваться в противоречии с этими целями и не быть избыточными по отношению к ним. Не допускается объединение баз персональных данных, собранных держателями в разных целях, для автоматизированной обработки информации.

4. Персональные данные, предоставляемые держателем, должны быть точными и в случае необходимости обновляться.

5. Персональные данные должны храниться не дольше, чем этого требует цель, для которой они накапливаются, и подлежать уничтожению по достижении этой цели или поминовании надобности.

6. Персональные данные охраняются в режиме конфиденциальной информации, исключающем их случайное или несанкционированное разрушение или случайную их утрату, а равно Несанкционированный доступ к данным, их изменение, блокирование или передачу.

7. Для лиц, занимающих высшие государственные должности, и кандидатов на эти должности может быть установлен специальный правовой режим для их персональных данных, обеспечивающий открытость только общественно значимых данных.

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.

При организации ИБ организации руководствуются стандартами, в частности используется ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (Дата актуализации: 21.05.2015) ГОСТ Р ИСО/МЭК 27005-2010.

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

Итак, основные правовые документы в сфере информационной безопасности:

- Конституция РФ (http://constitutionrf.ru/);
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации» (http://base.garant.ru/12148555/);
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями вступивших в силу 01.03.17 г.) (http://kodeks.systecs.ru/zakon/fz-152/);
- Федеральный закон от 06 апреля 2011 №63 «Об электронной подписи» (с изменениями на 23.06.16 г.) (http://docs.cntd.ru/document/902271495);
- Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне") (ред. от 12.03.14 г.) (http://yconsult.ru/zakony/zakon-rf-98-fz/);
- Доктрина информационной безопасности Российской Федерации (утв. утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.) (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html);

- Указ правительства РФ №188 об утверждении перечня сведений конфиденциального характера 1997г. (с изм. и доп. от 23 сентября 2005 г., 13 июля 2015 г.) (http://base.garant.ru/10200083/#ixzz4bCt8H6TU);
- Федеральный Закон от 21 июля 1993г. №5485 «О государственной тайне» (Федеральный закон "О внесении изменений в статью 5 Закона Российской Федерации "О государственной тайне" от 15.11.2010 N 299-ФЗ (последняя редакция) (http://www.consultant.ru/document/cons_doc_LAW_106802/);
- Трудовой кодекс РФ – глава 14 «Защита персональных данных работника» (от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (http://www.consultant.ru/document/cons_doc_LAW_34683/);
- Гражданский кодекс Ч. №4 Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (18 декабря 2006 года N 230-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_64629/).

Студентам следует ознакомиться с этими документами в Интернете (эл.адреса прилагаются). Кроме того, необходимо ознакомиться с основным ГОСТом (http://gostrf.com/normadata/1/4293804/4293804268.pdf).

Контрольные вопросы по теме 3

1. Что составляет базу функционирования специализированных организаций в сфере информационной безопасности?
2. Назовите характерные черты организационной работы специализированных организаций в сфере информационной безопасности.
3. Что представляют собой альянсы крупных технологических компаний?
4. Перечислите типичные приемы организационной работы альянсов крупных технологических компаний.
5. Сделайте доклад о деятельности одной из специализированных организаций в сфере информационной безопасности.
6. Чем занимается Альянс по смарт-картам?
7. Какие задачи решает Альянс по безопасности сети Интернет?
8. Сделайте доклад о деятельности одной из международных организаций в сфере информационной безопасности.
9. О чем Доктрина информационной безопасности РФ (5 декабря 2016 г.)?
10. Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
11. О чем Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (с изм. на 2014 г.)?
12. Охарактеризуйте содержание статей 159(1-6), 272, 273, 274 УК.

Задание для самостоятельной работы: заполните таблицу.

Наименование международной организации	Основные задачи

Тесты к теме 3

1. **Ассоциация вычислительной техники создана в**

А. 1947 году;
Б. 1964 году;
В. 2017 году.

2. Консорциум Всемирной Паутины оформлен

А. в 1989 году;
Б. в 1994 году;
В. в 2017 году.

3. Международная организация по стандартизации это

А. ISO;
Б. ACM;
В. ООН.

4.Проект международных стандартов приобретает статус международного стандарта, если за него проголосовало

А. 100% членов;
Б. 75% членов;
В. 80% членов.

5. Альянс по безопасности сети Интернет создан в

А. 2001 г.
Б. 2016 г.
В. 2017 г.

6.Доктрина Информационной безопасности принята в

А. 2012 году
Б. 2014 году
В. 2016 году

7. В организационную основу системы обеспечения информационной безопасности РФ входит:

А. Совет безопасности РФ;
Б. Министерство образования и науки РФ;
В. ЦРУ США.

8. К актам федерального законодательства по ИБ в РФ входят:

А. Приказы ФСБ;
Б. Международные стандарты;
В. Конституция РФ.

9. Правовое обеспечение ИБ означает:

А. Защиту интересов физических и юридических лиц;
Б. Защиту интересов государства и общества;
В. Все вышеперечисленное.

10.Масштабы компьютерной преступности в РФ

А. Неуклонно снижаются;
Б. Возрастают;
В. Остаются из года в год неизменными.

11. Статья 23 Конституции РФ определяет:

А. Право на получение достоверной информации о состоянии окружающей среды;
Б. Право на неприкосновенность частной жизни, личную и семейную тайну и иные сообщения;
В. Отказ в предоставлении гражданину информации.

12. В Налоговом кодексе РФ имеется:

А. ст.139 «Служебная и коммерческая тайна»;
Б. ст.102 «Налоговые тайны»;
В. ст.946 «Тайна страхования».

13. Федеральный закон «Об информации, информационных технологиях и о защите информации»

А. пока не принят;
Б. принят в 2000 году;
В. принят в 2006 году.

14. Федеральный закон «О персональных данных» принят:

А. в 2006 году с изменениями на 1 января 2017 года;
Б. в 2009 году;
В. в 2016 году.

15. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?

А. в ст.272;
Б. в ст.273;
В. в ст.274.

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

1. Политика безопасности и ее принципы.
2. Методы и средства обеспечения ИБ.

1. Политика безопасности и ее принципы

Инструменты и механизмы информационной безопасности включают в себя процессы и процедуры ограничения и разграничения доступа, информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); использование методов надежного хранения, преобразования и передачи информации; нормативно-административное побуждение и принуждение [52].

На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и др.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией др.)., но одних технических средств недостаточно: необходима организационно-управленческая деятельность - организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации [40].

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 [57]:

- ✓ невозможность миновать защитные средства;
- ✓ усиление самого слабого звена;
- ✓ невозможность перехода в небезопасное состояние;
- ✓ минимизация привилегий;
- ✓ разделение обязанностей;
- ✓ эшелонированность обороны;
- ✓ разнообразие защитных средств;
- ✓ простота и управляемость информационной системы;
- ✓ обеспечение всеобщей поддержки мер безопасности;
- ✓ адекватность (разумная достаточность);
- ✓ системность;
- ✓ прозрачность для легальных пользователей;
- ✓ равностойкость звеньев.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в

крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Принцип адекватности (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Вряд ли деклассированный пролетарий потратит деньги на металлическую дверь, суперзамок и сигнализацию, если в квартире непропитые вещи можно пересчитать по пальцам.

Системность. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забывать о важности системного подхода. Он состоит в том, что системазащиты должна строиться не

абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств.

Прозрачность для легальных пользователей. Можно заставлять пользователей перед каждой операцией для надежной идентификации вводить 10-значный пароль, прикладывать палец к сканеру и произносить кодовую фразу. Но не разбегутся ли после этого сотрудники.

Равностойкость звеньев. Звенья - это элементы защиты, преодоление любого из которых означает преодоление всей защиты (например, окно и дверь в равной степени открывают вору путь в квартиру). Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае прочность защиты (или ее уровня, см. ниже) определяется прочностью самого слабого звена.

Главными этапами построения политики безопасности являются следующие:

- обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
- выбор и установка средств защиты;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается **Концепция информационной безопасности ИС,** на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;
- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
- организация хранения информации в ИС;
- организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);
- регламентация допуска персонала к той или иной информации;
- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается схема безопасности, структура которой должна удовлетворят» следующим условиям:

1. Защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи.
2. Разграничение потоков информации между сегментами сети.
3. Защита критичных ресурсов сети.
4. Защита рабочих мест и ресурсов от несанкционированного доступа *(НСД).*
5. Криптографическая защита информационных ресурсов.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации.

Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от верхнего уровня, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны

для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Прежде чем строить какую-то систему защиты, определим, что и от кого (чего) мы хотим защитить. Нельзя защитить все и от всего. Согласитесь, не вся информация для вас одинаково ценна.

Итак, для начала выделите перечень информации (файлов), которые необходимо защитить, и ее физическое размещение (сразу станет ясно, что защищать лучше информацию, которая хранится на одном **компьютере). Прикиньте, во что может обойтись простой компьютеров, потеря электронной почты за день или утрата важных данных.**

Второе, что необходимо уяснить - от кого мы защищаем информацию. Кто тот злоумышленник (или их несколько), который теми или иными средствами может завладеть вашей информацией? Одновременно надо оценить силы злоумышленника - какие он может иметь организационные и технические возможности для доступа к информации (ведь злоумышленник может быть и сотрудником фирмы), сколько времени и денег ему не жалко на добычу информации. Потенциальный злоумышленник в принципе может и отсутствовать, а безопасности информации могут угрожать случайные факторы (вирусные эпидемии выход из строя компьютеров и т. д.).

Третье, что надо оценить - это угрозы информации. Различают следующие группы угроз:

- несанкционированный доступ к информации (чтение, копирование или изменение информации, ее подлоги навязывание);
- нарушение работоспособности компьютеров и прикладных программ, что может повлечь остановку производственных процессов;
- уничтожение информации.

В каждой из этих трех групп можно выделить десятки конкретных угроз, однако пока остановимся. Заметим только, что угрозы могут быть преднамеренными и

случайными, а случайные, в свою очередь, обусловленные естественными факторами (например, стихийные бедствия) и человеческим фактором (ошибочные действия персонала). Случайные угрозы, в которых отсутствует злой умысел, обычно опасны только возможностью потери информации и нарушения работоспособности системы, от чего достаточно легко застраховаться. Преднамеренные же угрозы более серьезны с точки зрения потери для бизнеса, ибо здесь приходится бороться не со слепым (пусть и беспощадным в своей силе) случаем, но с думающим противником.

Выяснение того, что, от кого и от чего мы будем защищать - большой шаг на пути к ответу на главный вопрос: как защищать? Так что на первый этап не жалко потратить времени, тем более что в небольшой фирме для мозгового штурма начальнику и его приближенным достаточно одного рабочего дня. Можно все это провести в виде импровизированной деловой игры, в том числе и с самим собой.

Итак, следует определить политику применительно к различным элементам защиты:

Политика управления паролями (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований. Политика на этом уровне также может устанавливать запрет хранения записанных паролей, запрет сообщать кому-либо свой пароль (в том числе руководителям и администраторам информационных систем) и другие аналогичные ограничения.

Политика установки и обновления версий программного обеспечения не является внутри-организационной политикой безопасности, но фактически должна либо напрямую использоваться государственными учреждениями и предприятиями, имеющими доступ к информации, составляющей государственную тайну РФ, как политика безопасности, либо ее положения должны быть прямо перенесены во внутренние политики информационной безопасности таких учреждений и предприятий.

Политика приобретения информационных систем и их элементов (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

Политика доступа сторонних пользователей (организаций) в информационные системы предприятия может содержать перечень основных ситуаций возможности доступа, критериев и процедур его осуществление, распределение ответственности сотрудников компании.

Политика в отношении разработки ПО может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств сторонним специализированным организациям, а также в отношении приобретения и использования тиражируемых программных библиотек компаний-производителей.

Политики использования отдельных универсальных информационных технологий в масштабе всего предприятия могут включать в себя политику

использования электронной почты (e-mail); политику использования средств шифрования данных; политику защиты от компьютерных вирусов и других вредоносных программ; политику использования модемов и других аналогичных коммуникационных средств; политику использования Инфраструктуры публичных ключей; политику использования технологии Виртуальных частных сетей (VirtualPrivateNetwork- VPN).

Политика использования электронной почты может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.

Политика использования коммуникационных средств может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами.

Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.) [30].

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

* управление рисками (**оценка рисков**, выбор эффективных средств защиты);

* **координация** деятельности в области информационной безопасности, пополнение и распределение ресурсов;

* **стратегическое планирование;**

* **контроль** деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие

следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

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».

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации вцелом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц но выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение **непрерывной работы организации;**
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отодраться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень

безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного

Программа безопасности

После .того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности и области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок

сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис, рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

— какого рода информация предназначается для обслуживания новым сервисом?

каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?

— каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?

— есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?

— каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

— каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами

коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно’ анализируют регистрационную информацию, То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи.

Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Тема управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, нужно только для тех организаций, информационные системы которых

и/или обрабатываемые данные можно считать нестандартными. Типовую организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами.

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере) оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные подходы, методы и средства обеспечения информационной безопасности.

2. Методы и средства обеспечения информационной безопасности

Под обеспечением безопасности информационных систем понимают меры, предохраняющие информационную систему от случайного или преднамеренного вмешательства в режимы ее функционирования.

Существует два принципиальных подхода к обеспечению компьютерной безопасности [57].

- Фрагментарный. Данный подход ориентируется на противодействие строго определенным угрозам при определенных условиях (например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д.).

Достоинством фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Недостатком - локальность действия, т.е. фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов от конкретной угрозы. Но не более того.

- Комплексный. Данный подход получил широкое распространение вследствие недостатков, присущих фрагментарному. Он объединяет разнородные меры противодействия угрозам (рис.1) 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.

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. 11.

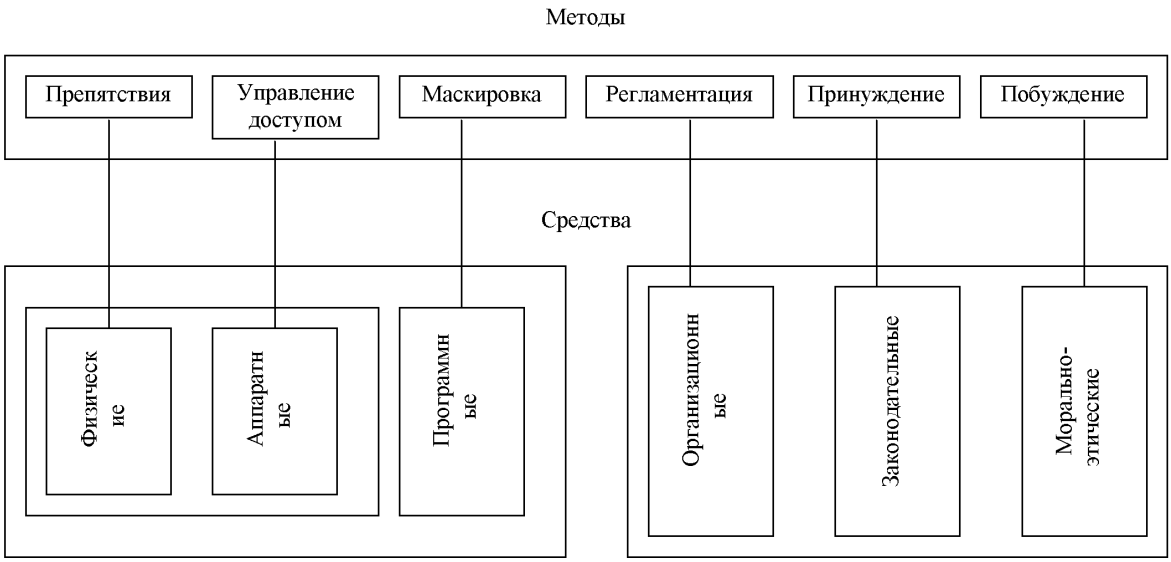


Рис. 11. Методы и средства информационной безопасности экономического объекта

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 документа, обычно называется открытым,

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:

- электронная подпись;
- контроль доступа;
- дублирование каналов интернет связи;

5) По сути электронная подпись (ЭП) — это некая последовательность символов, которая получена в результате определенного преобразования исходного документа (или любой другой информации) при помощи специального программного обеспечения.

ЭП добавляется при пересылке к исходному документу. Любое изменение исходного документа делает ЭП недействительной.

Виды электронной подписи: простая электронная подпись и усиленная электронная подпись, которая, в свою очередь, может быть квалифицированной и неквалифицированной.

- Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
- Неквалифицированной (усиленной) электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

- Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

ЭП предназначена для аутентификации лица подписавшего электронный документ и позволяет осуществить:

- доказательное подтверждение авторства документа (могут быть подписаны поля: «автор», «внесенные изменения», «метка времени»)

- контроль целостности передаваемого документа (при любом случайном или преднамеренном изменении документа изменится подпись следовательно она станет недействительной).

Все эти свойства электронной подписи позволяют использовать её для следующих целей:

- Декларирование товаров и услуг (таможенные декларации);
- Регистрация сделок по объектам недвижимости;
- Использование в банковских системах;
- Электронная торговля и госзаказы;
- В системах обращения к органам власти;
-Для организации юридически значимого электронного документооборота;
- В бухгалтериях предприятий различных форм собственности.

В настоящее время существуют следующие устройства хранения ключа ЭП:

- Дискеты
- Смарт-карты
- USB-брелок(eToken)
- Таблетки Touch-Memory

6) Дублирование канала интернет и сжатие информации позволяет повысить надежность системы в случае отказа или перегрузки канала связи. 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.

Контрольные вопросы к теме 4

1. Назовите основные принципы политики безопасности.
2. Что означает принцип эшелонированности обороны?
3. Какие вопросы отражаются в Концепции информационной безопасности?
4. Что включает политика безопасности верхнего уровня?
5. Как организован удаленный доступ к сервису?
6. Что включает политика управления паролями?
7. Как оценить риски реализации угроз информации?
8. Какие этапы выделяются в жизненном цикле информационного сервиса?
9. На каких принципах базируется системный подход к защите информации?
10. Как обеспечивается управление доступом?
11. Какие программные средства используются для ИБ?
12. В чем отличия метода принуждения от метода побуждения?
13. Чем занимается криптография?
14. Что такое электронная подпись и для чего она используется?

Тесты к теме 4

1. Принципом политики безопасности являются:
А. Опора на собственные силы;
Б. Усиление самого слабого звена;
В. Демократический централизм.

2. Принцип системности означает:
А. Комплексный анализ угроз, средств защиты от этих угроз;
Б. Прозрачность для легальных пользователей;
В. Эшелонированность обороны.

3. Политика безопасности разрабатывается применительно к
А. Одному верхнему уровню управления;
Б. Трем уровням управления (верхнему, среднему и нижнему);
В. Решению акционеров компании.

4. Программа безопасности синхронизируется с жизненным циклом системы?
А. да;
Б. нет;
В. отчасти.

5. В политике безопасности основным принципом является усиление самого слабого звена?
А. нет:
Б. да;
В. отчасти.

6. В политике безопасности не должна быть:
А. невозможность миновать защитные средства;
Б. разделение обязанностей;
В. возможность перехода в небезопасное состояние.

7. Контроль целостности программного обеспечения НЕ проводится с помощью:
А. внешних средств (программ контроля целостности);
Б. внутренних средств (встроенных в саму программу);
В. криптографических средств.

8.Какой подход к обеспечению безопасности информации не существует?
А. комплексный;
Б. фрагментарный;
+В. теоретический.

9. Криптография – это..?
А. наука о шифровании (преобразовании) информации;
Б. наука о вирусах;

В. наука об информационных войнах.

10. Криптографические средства – это..?

А. регламентация правил использования, обработки и передачи информации ограниченного доступа;

Б. средства защиты с помощью преобразования информации (шифрование);

В. средства, в которых программные и аппаратные части полностью взаимосвязаны.

11. Шифрование с симметричным ключом предполагает, что..?

А. используются два разных ключа;

Б. оба ключа одинаковы;

В. невозможно отказаться от авторства.

Тема 5. Организация системы защиты информации

1. Организационное обеспечение информационной безопасности
2. Защита информации в Интернет.
3. Этапы построения системы защиты информации.

1. Организационное обеспечение информационной безопасности

Выделяют 4 основные задачи организационно-управленческой деятельности в сфере информационной безопасности: обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности; обеспечение непрерывности и целостности процессов информационной безопасности; решение методических задач, лежащих в основе эффективного управления информационной безопасностью (вопросов управления рисками, экономического моделирования и т.п..).; управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности. При этом данные задачи должны решаться в комплексе и непрерывно [36].

Управление человеческими ресурсами в рамках управления информационной безопасностью включает в себя комплекс задач, охватывающий все основные аспекты деятельности людей: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п. Под организационным обеспечением и менеджментом в сфере информационной безопасности обычно принято понимать решение управленческих вопросов на уровне отдельных субъектов (предприятий, организаций) или групп таких субъектов (партнеров по бизнесу, организаций, которые совместно решают определенные задачи, требующие защиты информации) [12].

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.

Организационное обеспечение компьютерной безопасности включает в себя ряд мероприятий:

- организационно-административные;
- организационно-технические;
- организационно-экономические.

Организационно-административные мероприятия предполагают:

- 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.

Таблица 4

Обеспечение информационной безопасности организации

Составные части делопроизводства	**Функции обеспечения ИБ при**	**Способы выполнения**
Документирование	Предупреждение: - необоснованного изготовления документов; - включение в документы избыточной конфиденциальной информации; - необоснованного завышения степени конфиденциальности документов; - необоснованной рассылки	Определение перечня документов Осуществление контроля за содержанием документов и степени конфиденциальности содержания Определение реальной степени конфиденциальности сведений, включенных в документ Осуществление контроля за размножением и рассылкой документов
Учет документов	Предупреждение утраты (хищения) документов	Контроль за местонахождением документа
Организация документооборота	Предупреждение: - необоснованного ознакомления с документами; - неконтролируемой передачи документов	Установление разрешительной системы доступа исполнителей к документам Установление порядка приема-передачи документов между
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. 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, Internettex 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. 12 приведена классификация методов обеспечения информационной безопасности, основанных на использовании инженерно-технических средств.

Рис. 12. 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:

• Выявление возможных каналов утечки.

• Обнаружение реальных каналов.

• Оценка опасности реальных каналов.

• Локализация опасных каналов утечки информации.

• Систематический контроль за наличием каналов и качеством их защиты.

Защита информации от утечки по техническим каналам - это комплекс

мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

Постулаты такой защиты:

- Безопасных технических средств нет.

- Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

- Любой канал утечки информации может быть обнаружен и локализован. «На каждый яд есть противоядие».

- Канал утечки информации легче локализовать, чем обнаружить.

Для непосредственной организации обеспечения информационной безопасности структурой и штатным расписанием предусматриваются специальные подразделения и сотрудники. Основные функции таких служб заключаются в следующем:

- На этапе проектирования (совершенствования) системы информационной безопасности:
- формирование требований к системе информационной безопасности;
- участие в разработке компонентов и системы информационной безопасности в целом.
- На этапе эксплуатации:
- планирование, организация и обеспечение функционирования системы информационной безопасности;
- обучение пользователей и технического персонала организации формам и методам эксплуатации технических средств;
- контроль за 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. 13 [57].

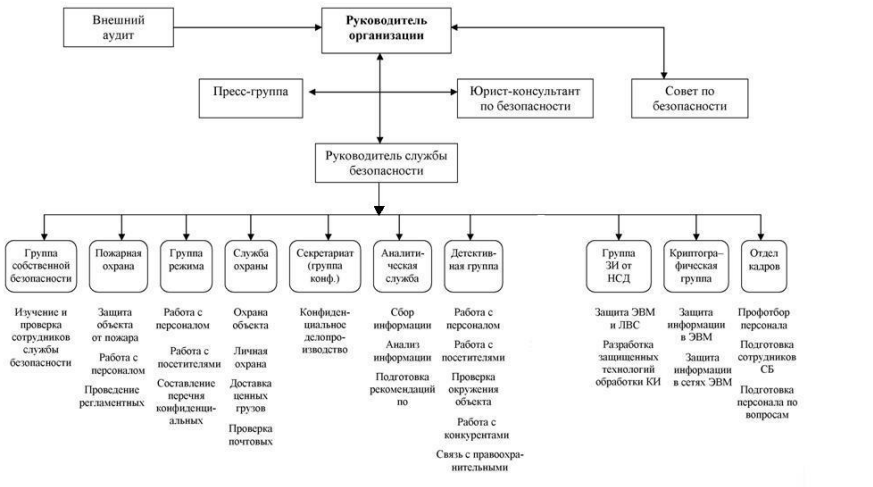


Рис. 13. Структура и задачи службы безопасности

2. Защита информации в Интернет

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 Internetимеет более 3 млр. пользователей в более чем 150 странах мира. 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 локальным 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 Internetможно 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 Internetмеханизмов расчета.

Разработка средств электронных расчетов для Сети финансируется банками, некоторые из которых создают службы расчетов, целиком ориентированные на Internet.

Основные сервисы системы Интернет

- WorldWideWeb (WWW) – главный информационный сервис. Гипермедийная информационная система поиска ресурсов Интернет и доступа к ним.
- Программы-браузеры. Информацию, полученную от любого сервера, браузер WWW выводит на экран в стандартной, удобной для восприятия форме.
- Программа удаленного доступа Telnet. Позволяет входить в другую вычислительную систему, работающую в Интернет.
- Программа пересылки файлов_Ftp. Перемещает копии файлов с одного узла Интернет на другой.

- Электронная почта (Electronicmail, англ. Mail – почта, сокр.E-mail).Служит для передачи текстовых сообщений в пределах Интернет, а также между другими сетями электронной почты.
- Система телеконференций Usenet (от UsersNetwork). Организует коллективные обсуждения по различным направлениям, называемые телеконференциями.
- Системы информационного поиска сети Интернет.

Функции электронной почты

- Обмен сообщениями между пользователями;
- Обмен документами между пользователями;
- Обмен данными между приложениями;
- Оповещение пользователей о наступлении определенных событий.

Адрес электронной почты имеет вид:

Логин @ символический адрес сервера.имя зоны

Первая часть почтового адреса – это имя пользователя, вторая часть – доменная.ivanov@unn.ru

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 вархивам 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, apriori.

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 Internetв 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.

Подключение корпоративных, локальных сетей или отдельных персональных компьютеров к сети Интернет таит в себе определенные угрозы информационной безопасности.

I. Угроза внешних кибератак и, прежде всего, угроза удаленного администрирования.

Согласно отчету компании «Майкрософт» о тенденциях кибербезопасности в 2016 году [1] наибольшую опасность представляет угроза удаленного администрирования, реализуемая, чаще всего, через запуск троянских программ или с использованием программ-эксплойтов.

Под удаленным администрированием понимается несанкционированное управление удаленным компьютером. В этом случае злоумышленник может:

1) манипулировать, то есть удалять, блокировать, модифицировать и копировать ценную компьютерную информацию;

2) устанавливать на этом компьютере произвольные программы, в том числе вредоносные;

3) использовать компьютер для совершения преступных действий в сети «от его имени».

II. Угроза активного содержимого.

Под активным содержимым понимаются активные объекты, встроенные в Web-страницы (включают в себя не только данные, но и программный код). Агрессивный программный код, попавший на компьютер «жертвы», способен вести себя как вирус или как агентская программа, которая может взаимодействовать с удаленными программами и готовить почву для удаленного администрирования.

III. Угроза перехвата или подмены данных при их пересылке по открытым каналам связи.

С развитием Интернет-коммерции и Интернет-банкинга эта угроза становится все более актуальной. Например, расчет электронными платежными средствами предполагает отправку покупателем конфиденциальных данных о своей карте продавцу. Нет гарантий, что эти данные не будут перехвачены злоумышленником, поскольку используются открытые каналы связи.

IV. Угроза мониторинга и сбора частной информации в интересах третьих лиц.

В основе этой угрозы лежат коммерческие интересы рекламных организаций. В желании увеличить свои доходы множество компаний организуют Web-узлы, прежде всего, для сбора персональных сведений и предпочтений пользователей Интернета. Эти сведения поставляются рекламным и маркетинговым службам. Процесс сбора персональной информации автоматизирован и позволяет без санкции клиентов изучить их

вкусы и привязанности. Например, браузер «изучает» то, что Вы ищите в Сети и во время следующего сеанса выдает Вам массу рекламы по теме Вашего поиска.

V. Угроза поставки неприемлемого содержимого.

Не вся информация в Интернете может считаться общественно полезной. По разным причинам морально-этического, религиозного или политического характера, людям может быть неприятна поставляемая информация, и они хотят от нее защититься.

Кроме этого, сюда можно отнести и спам. Спам – это нежелательные рассылки, которые могут приходить на адрес вашей электронной почты. Они содержат рекламные предложения, «письма счастья», компьютерные вирусы или могут оказаться попыткой компьютерного мошенничества. Для создания базы адресов спамеры используют программное обеспечение, которое подбирает адреса с помощью специального словаря или собирает адреса, опубликованные на общедоступных сайтах.

VI. Угроза Интернет-мошенничества.

Целью Интернет-мошенничества (фишинга) является получение секретных данных пользователя (паролей от учетных записей, номера или PIN-кода кредитной карты и т.д.). Злоумышленники рассылают письма от имени компаний, сервисов, социальных сетей, которые очень похожи на настоящие. В них просят:

- предоставить ваш логин и пароль к сервису или сайту, например, в связи с проблемами с доставкой или сбоем в системе (чаще всего в поле «От кого» у таких писем указывается «Служба поддержки», «support» или «admin»);
- отправить СМС на короткий номер, чтобы подтвердить личность или активировать почтовый ящик (в результате с вашего телефона списывается некоторая сумма, а в ряде случаев может включиться ежедневное списание денежных средств);
- заполнить анкету, чтобы поучаствовать в розыгрыше призов или получить подарок (в такой анкете, помимо фамилии, имени, отчества и контактных телефонов, обычно просят указать паспортные данные и номер кредитной карты);
- перейти по ссылке на сайт, например, чтобы ввести логин и пароль (такие сайты выглядят как сайты реально существующих компаний или сервисов, но на самом деле они поддельные, и мошенники могут получить конфиденциальную информацию, если пользователь введет свои данные).

VII. Угроза потери ценной компьютерной информации по различным причинам.

Причинами потери ценной информации могут быть компьютерные вирусы, программные или аппаратные сбои, стихийные бедствия (пожар, потоп) и т.д.

Для противодействия вышеуказанным угрозам и обеспечения надлежащего уровня безопасности при работе в Сети необходимо применять соответствующие защитные меры:

1. Защита от удаленного администрирования.

Удаленное администрирование чаще всего достигается:

- запуском троянских программ (троянцы, трояны, троянские кони);
- использованием программ - эксплойтов, которые атакуют в основном серверы, программное обеспечение которых имеет уязвимости.

Для поражения компьютера троянской программой ее должен запустить кто-то на нем. Мероприятия для защиты от троянов:

1) ограничение доступа посторонних лиц к компьютерам (физическое ограничение доступа, парольная защита и т.д);

2) проверка на безопасность всех данных, вводимых в компьютер (сканирование антивирусным ПО);

3) если получены незатребованные данные из незнакомого источника, их следует уничтожать, не открывая!

4) не запускать ничего, что поступает вместе с электронной почтой, так как злоумышленники могут замаскировать «трояна» как приложение к «письму друга» (есть технические средства, подделывающие адрес отправителя, чтобы письмо злоумышленника выглядело как письма от знакомого).

Мероприятия по защите от программ-эксплойтов:

1) регулярные обновления программного обеспечения на сервере, так как они устраняют уязвимости старого программного обеспечения, которые и используются злоумышленниками, посылающими программы-эксплоиты;

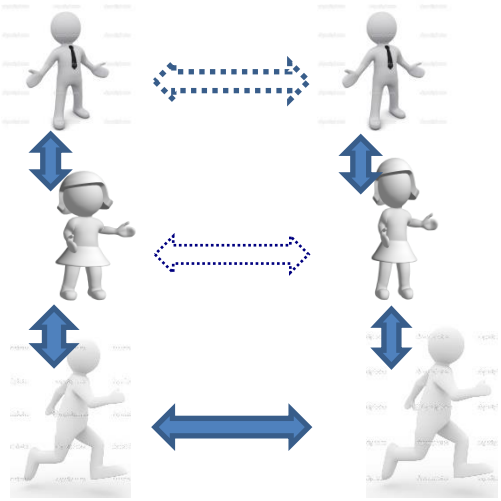
2) использование брандмауэров или файерволов (firewall), выполняющих функцию межсетевых экранов (они занимают положение между локальной сетью и глобальной, не позволяя просматривать извне состав программного обеспечения на сервере, и не пропуская несанкционированные команды и данные).

3) применение прокси-серверов, позволяющих скрыть внутреннюю структуру локальной сети от анализа извне (это важный момент, поскольку атакам на информационные системы, как правило, предшествует предварительное исследование их программного и аппаратного обеспечения, их уязвимостей и т.д.).

Рассмотрим функционирование брандмауэров и прокси-серверов подробнее.

Для понимания сути работы брандмауэра проанализируем простой пример [26].

Два руководителя обмениваются письмами. Написав письмо, они передают его секретарю для печати, а те, в свою очередь, курьерам для доставки, то есть мы имеем 3-х уровневую модель связи (реально 7 уровней модели OSI):



руководитель (user, пользователь)

секретарь

курьер

Предположим, секретари вступили в сговор и начали тайный обмен информацией между собой. Секретарь **А** что-то дописывает карандашом в письме, а секретарь **Б** читает и затем стирает то, что было приписано.

Руководители (пользователи) могут не знать о том, что их канал связи используется несанкционированно, так как они «выше» по уровню реального «трафика».

Что делать? Привлечь к проверке курьера (!). Если курьеру разрешить читать то, что они доставляют, то он может сигнализировать руководителю об обнаружении несанкционированного соединения.

Именно эту функцию и выполняют брандмауэры.

Брандмауэр контролирует соединения на уровнях ниже прикладного, то есть на уровне соединения, сетевом и транспортном, и способен уловить признаки работы несанкционированных средств, например, средств удаленного администрирования. Он также может контролировать трафик и фильтровать его.

Брандмауэр позволяет организовать систему сетевой безопасности, за которую обычно отвечает системный администратор. Он настраивает брандмауэр таким образом, что внешние клиенты имеют весьма ограниченный доступ к службам защищаемой области, а внутренние пользователи – к службам внешней сети (только по служебной необходимости).

Классическим примером является программный комплекс Solstice (со́лстис) FireWall-1 компании Sun Microsystems [34]. Данный пакет неоднократно отмечался наградами на выставках и конкурсах.

Рассмотрим основные компоненты Solstice FireWall-1 и функции, которые они реализуют.

Центральным для системы FireWall- 1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети.

Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

- Определить объекты, участвующие в процессе обработки информации (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 (обычно достаточным оказывается набор описаний, поставляемых с системой FireWall-1);
- 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. 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.

Система Solstice FireWall-1 имеет собственный встроенный объектно - ориентированный язык программирования, применяемый для описания поведения модулей - фильтров системы. На практике данная возможность почти не используется, поскольку графический интерфейс системы 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 следующие данные об эффективности работы Solstice FireWall-1. Модули фильтрации на Internet-шлюзе, сконфигурированные типичным для многих организаций образом, работая на скоростях в 10 Мб/сек, забирают на себя не более 10% вычислительной мощности компьютера.

Теперь рассмотрим прокси-серверы [26]. Это аппаратные и/или программные средства, выполняющие буферные функции между локальной и глобальной сетью. Их основное назначение:

1) оптимизация работы компьютера или локальной сети в WWW (исторически первоначальная функция);

2) защитная функция, но в отличие от брандмауэра это скорее диспетчер, а не инспектор.

Функционирование прокси-сервера (принцип работы):

1) пользователь компьютера адресует запрос в Интернет на поставку определенного Web-ресурса, но этот запрос отправляется не в Сеть, а прокси-серверу;

2) прокси-сервер от своего имени адресует запрос в Интернет и получает отклик от удаленного сервера;

3) полученный ресурс прокси-сервер передает на компьютер пользователя.

Преимущества от использования прокси-сервера:

1) анонимность (удаленный сервер не знает точно, от кого поступил запрос, с его точки зрения он поступил от прокси – сервера);

2) ускорение загрузки (Web-страницы, проходящие через прокси-сервер, запоминаются на нем, и если другой пользователь обращается к тому же ресурсу, то он получит его не от удаленного сервера, а от прокси-сервера, что гораздо быстрее);

3) фильтрация (элементы Web-страниц, проходящих через прокси-сервер, анализируются и фильтруются, поэтому ненужная информация, например реклама, может отсеиваться);

4) ускорение подключения (на прокси-сервере накапливаются данные о соответствии доменных имен хостов Интернета и их IP-адресов; при повторном обращении к тем же хостам уже не надо искать их IP-адреса в сравнительно медленной структуре DNS и можно обращаться прямо по IP- адресу);

Дополнительные защитные функции:

5) прокси-сервер может быть настроен таким образом, чтобы ограничить доступ сотрудников организации узким кругом Web-ресурсов, необходимых им лишь для выполнения служебных обязанностей;

6) прокси-сервер, как буфер, способен контролировать содержание проходящих через него данных; он может блокировать файлы, содержащие вирусы, а также сведения, недопустимые по этическим, политическим или религиозным соображениям;

7) прокси-сервер позволяет скрыть внутреннюю структуру локальной сети от анализа извне (это важный момент, поскольку атакам на информационные системы, как правило, предшествует предварительное исследование их программного и аппаратного обеспечения, их уязвимостей и т.д.).

2. Защита от активного содержимого.

Защита от активного содержимого реализуется соответствующей настройкой браузера, чтобы опасность была минимальной.

Настройка защиты браузера обычно проводится по траектории

«Свойства обозревателя → Безопасность»

или

«Настройки → Безопасность»

или

«Безопасность».

3. Защита данных на путях транспортировки.

Защита данных на путях транспортировки реализуется применением криптографических методов защиты информации и ЭЦП (См. раздел «Электронная цифровая подпись»).

Уже много раз отмечались важность и необходимость защиты данных на путях их транспортировки по открытым каналам связи. Это важно и для электронной коммерции, и особенно важно для Интернет-банкинга. Клиент должен быть уверен, что имеет дело с банком, а банк – в том, что получает указания для управления счетом от его владельца.

В Интернете обычно используются две технологии защищенной связи, закрепленные стандартами:

- протокол HTTPS (Secure http, безопасный http);
- протокол SSL (Secured Socket Layer, уровень безопасных соединений).

Протокол HTTPS (или SHTTP) – это расширение прикладного протокола http и, следовательно, им пользуются только для защищенной связи в WWW при взаимодействии web – сервера и браузера.

Протокол SSL – это сеансовый протокол, который занимает промежуточное место между прикладными протоколами (http, ftp и др.) и транспортным протоколом TCP. С его помощью создается защищенный канал связи (туннель), внутри которого можно работать с любым сервисом Интернета (www, e-mail и др.).

В чем состоит отличие между протоколами HTTPS и SSL?

С помощью HTTPS можно отправить одно защищенное сообщение серверу или клиенту, а с помощью SSL можно создать защищенный сеанс, в рамках которого можно обмениваться многократными сообщениями, то есть, если нужно отправить защищенное сообщение от клиента к серверу, например, при вводе пароля, то можно ограничиться протоколом HTTPS, а если необходим двусторонний обмен данными, например, при взаимодействии с банком, то используют SSL.

В электронной коммерции наиболее широко применяется протокол SSL. Его работу рассмотрим на модели взаимодействия Банк- Клиент в Интернете [26].

Программные средства, реализующие протокол SSL, базируются на гибридной криптографической системе, в которой сочетаются несимметричные (НШ) и симметричные (СШ) алгоритмы шифрования.

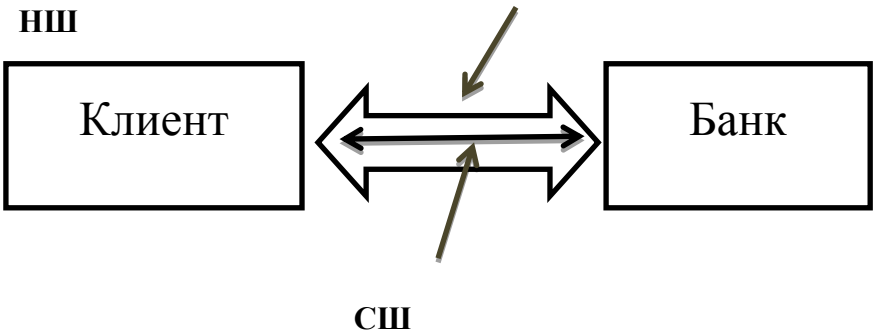
Почему система гибридная?

Симметричные шифры значительно быстрее несимметричных, поэтому при обмене многократными сообщениями, для чего и создан протокол SSL, позволяют поддерживать высокую скорость обмена данными. Проблема симметричных шифров – как передать

ключ партнеру? Здесь и используется несимметричный шифр. Такое маленькое сообщение как ключ он зашифрует и дешифрует быстро, поэтому и применяют гибридную систему.

Протокол SSL состоит из двух компонентов:

- протокол установления защищенной связи (протокол взаимодействия);
- протокол защищенного обмены данными (протокол обмена).



Установление защищенной связи (по шагам):

1. Клиентская программа посылает серверу Банка:

- своё название;
- номер версии;
- сведения о настройках своих средств шифрования, необходимые для взаимодействия с сервером.

2. Сервер посылает Клиенту:

- своё название;
- номер версии;
- сведения о настройках системы шифрования;
- сертификат своего открытого ключа и ключ.

3. Сервер запрашивает сертификат открытого ключа Клиента (если необходимо).

4. Клиент, получив данные от сервера, проводит его идентификацию. Если идентификация прошла успешно, то работа продолжается. Если нет, то сеанс завершается.

5. Клиент создает заготовку ключа настройки (premaster secret), затем шифрует ее открытым ключом сервера и отправляет серверу.

6. Если серверу необходима идентификация Клиента, то Клиент подписывает своим закрытым ключом определенное сообщение, полученное в ходе первичного контакта и известное серверу. Этот образец подписи отправляется вместе с заготовкой ключа настройки.

7. Сервер проверяет образец подписи Клиента с помощью его открытого ключа. Если Клиент не идентифицируется, то сеанс завершается. Если идентифицируется – то работа продолжается.

8. Сервер расшифровывает заготовку ключа настройки с помощью своего закрытого ключа.

9. Сервер и Клиент параллельно выполняют последовательность действий по получению ключа настройки (master secret) из заготовки ключа настройки. Далее они используют эти ключи для генерации одинаковых сеансовых ключей (одноразовых). Сеансовые ключи – симметричные. Используются для шифрования сообщений во время сеанса связи.

10. Клиент и сервер обмениваются сообщениями о том, что далее в обмене данными будут использовать созданный сеансовый ключ. Одновременно они обмениваются сообщениями, зашифрованными этими ключами о том, что процедура создания защищенного канала связи завершена.

После завершения протокола взаимодействия стороны переходят ко второй части – протоколу обмена данными, который основан на использовании симметричных шифров.

Сеансовый ключ – одноразовый, чтобы промежуточные серверы, участвующие в сеансе, не имели достаточно времени для его компрометации. В следующем сеансе ключ будет новым.

Протокол SSL получил развитие в новом протоколе TLS (Transport Layer Security, безопасность транспортного уровня).

Кроме этого, в данном разделе можно обсудить защиту сообщений электронной почты.

S/MIME (Secure/Multipurpose Internet Mail Extensions, Надежные приложения многофункциональной Интернет-почты) — стандарт для шифрования и подписи в электронной почте с помощью открытого ключа. S/MIME предназначен для обеспечения криптографической защиты электронной почты. Обеспечивает аутентификацию сообщения, идентификацию авторства и безопасность данных при их пересылке. Большая часть современных почтовых программ поддерживает S/MIME.

Использование стандарта S/MIME накладывает некоторые ограничения на применение традиционных приложений электронной почты и рабочей среды, в которой они используются.

Отправителю и получателю необходимо согласовывать применение клиентских приложений электронной почты, которые поддерживают данный стандарт.

Эффективное применение S/MIME требует комплексного подхода к обеспечению безопасности. Это означает, что необходимо обеспечивать защиту сообщений не только на пути следования от отправителя к получателю, но и в рабочей среде отправителя и получателя. Несоблюдение этого требования может привести к утечке конфиденциальной информации, несанкционированной модификации сообщений, компрометации секретных ключей непосредственно на компьютерах пользователей.

S/MIME принципиально несовместим с веб-почтой. Это обусловлено тем, что криптография открытых ключей, лежащая в основе стандарта S/MIME, обеспечивает защиту конфиденциальности и целостности сообщений на пути от отправителя до получателя. В то же время конфиденциальность и целостность сообщений недостижимы при традиционном использовании веб-почты, так как провайдер сервиса веб-почты имеет возможность читать сообщения и модифицировать их. Кроме того, основное преимущество веб-почты - её доступность с любого компьютера, где есть веб-обозреватель - противоречит требованию контроля защищенности рабочей среды при использовании S/MIME.

Для защиты веб-почты используется уже изученный протокол HTTPS. Он обеспечивает безопасность и конфиденциальность личных данных, передавая их на сервер в зашифрованном виде. Протокол HTTPS поддерживается во всех современных браузерах.

Кроме этого, веб-почта использует технологию DKIM.

DKIM (Domain Keys Identified Mail, Сообщение, идентифицированное ключами домена) — технология удостоверения подлинности отправителя при помощи цифровой подписи, связанной с именем домена. Наличие данной подписи подтверждает, что письмо не было перехвачено и изменено после отправки с почтового сервера отправителя.

Еще одно популярное приложение, разработанное для защиты посланий и файлов - PGP (Pretty Good Privacy, Очень хорошая секретность). Вероятно, это самое распространенное приложение защиты электронной почты в Интернете, использующее различные стандарты шифрования. Приложения PGP выпускаются для всех основных операционных систем, и послания можно шифровать до использования программы отправки электронной почты. PGP построена на принципе паутины доверия (web of trust) и позволяет пользователям распространять свои ключи без посредничества сертификационных центров.

В заключение коснемся корпоративных сетей.

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. Для этих целей предложена спецификация S/WAN (Secure Wide Area Networks, Защищенная глобальная сеть). Цель S/WAN - обеспечить реализацию комбинированной защиты и создание VPN на основе сетей Интернет. Она поможет 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.

4. Защита от мониторинга и сбора частной информации.

Наиболее простым источником для сбора персональных сведений являются маркеры cookie (куки) - это небольшой пакет данных, который передается сервером браузеру клиента и в котором, согласно протоколу http, закодирована информация, необходимая серверу для идентификации браузера и настройки на работу с ним.

Маркеры могут быть временными и постоянными.

Временные маркеры хранятся в оперативной памяти компьютера. По окончанию работы все временные маркеры стираются.

В принципе, было бы достаточно для технических целей использовать временные метки, но серверы, по понятным причинам, предпочитают отправлять браузеру не временные, а постоянные маркеры.

Постоянные маркеры не стираются после окончания сеанса, а переносятся на жесткий диск в виде файлов cookie. Происходит маркировка жесткого диска и всего компьютера клиента. При последующих выходах в Сеть происходит считывание маркеров в оперативную память компьютера, откуда браузер предъявляет их серверам, которые их поставили.

Физической угрозы компьютеру маркеры cookie **не представляют** (это не программный код), но они представляют угрозу в смысле вмешательства в частную жизнь.

Сервер может прочитать не только свои маркеры, но и все другие.

Защита от маркеров cookie реализуется браузером. В разделе «Безопасность» или аналогичном, устанавливают режим «Предлагать маркировку», тогда наглядно видно какие Web-узлы предлагают маркировать компьютер.

Кроме маркеров cookie, источником сведений о клиенте является сам браузер. Во время связи по протоколу http он сообщает:

- свое название;
- номер версии;
- тип операционной системы компьютера;
- URL - адрес страницы, которую клиент посещал в последний раз.

Еще одним источником персональной информации могут быть активные сценарии Java Script (Джава - скрипты). Защита аналогична защите от активного содержимого (при помощи настройки браузера).

5. Защита от поставки неприемлемого содержимого.

Обычно функции фильтрации поступающего содержания возлагают на браузер или на специальные программы, обслуживающие электронную почту (Windows Mail; Яндекс.Почта использует сервис «Спамооборона»).

При наличии брандмауэра или прокси-сервера в системе данные защитные функции могут возлагаться именно на это оборудование (описание их работы см. выше).

6. Защита от Интернет-мошенничества.

Для защиты от Интернет-мошенничества:

- внимательно просматривайте все приходящие письма и проверяйте адреса ссылок – фишинговые ссылки зачастую содержат бессмысленный набор символов или опечатки, кроме того, внимательно изучите адрес сайта, на который вам предлагают перейти для ввода персональных данных (не стоит вводить номер платежной карты, если адрес сайта выглядит подозрительно или начинается с http; адреса сервисов, которые защищают ваши данные, начинаются с https);

- отключайте дополнения, установленные в браузере, которые могут быть уязвимы для мошенников; чтобы выключить их, можно перейти в режим инкогнито, правда, если вспомнить об этом перед самой оплатой, собирать корзину или искать нужный рейс придется заново;

- никогда не оплачивайте покупок или счетов, в которых вы не уверены;

- не отправляйте СМС на подозрительные номера;

- никому не передавайте ваши логины и пароли;

- при работе на чужом компьютере не допускайте сохранения своих учетных данных;

- не вводите пароли от важных учетных записей при использовании общественной Wi-Fi сети; пользуйтесь мобильным Интернетом 3G или браузерами с режимом «Защита Wi-Fi».

7. Защита от потери ценной компьютерной информации.

При построении системы защиты компьютерной информации необходимо учитывать тезис, что «рано или поздно любой компьютер подвергнется разрушительным последствиям угроз, будь то вирусная атака, кража или выход жесткого диска из строя».

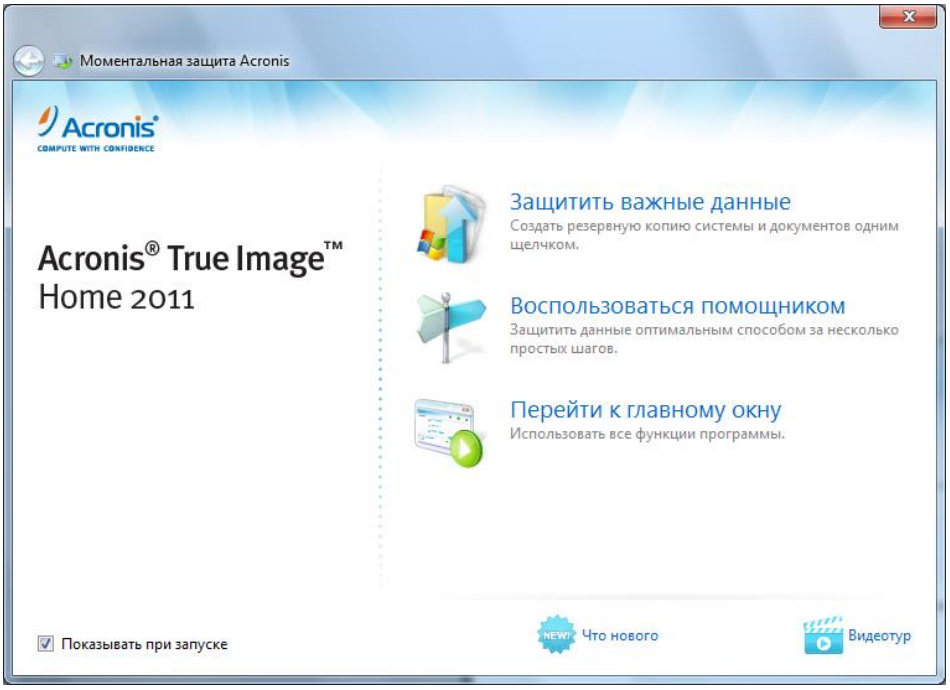
Надежная работа с компьютерной информацией достигается только тогда, когда любое неожиданное событие не приведет к катастрофическим последствиям.

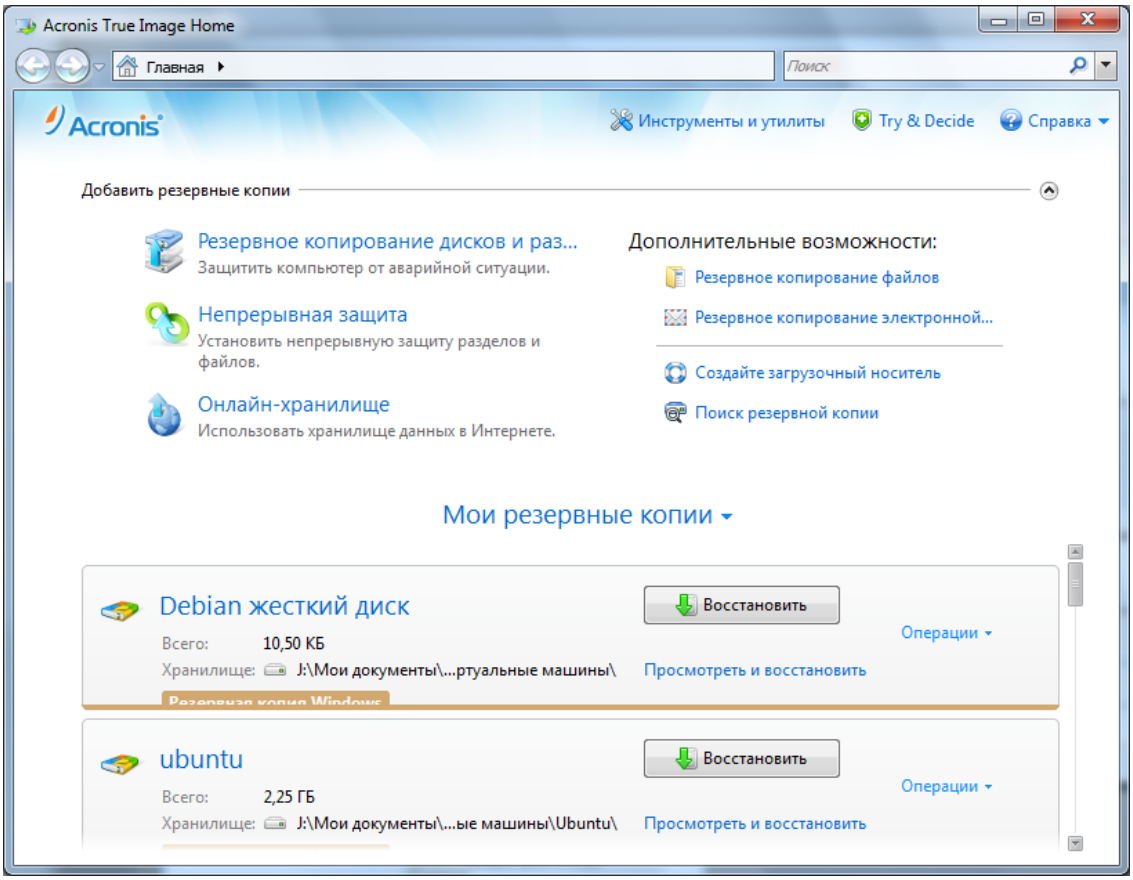
Для этого применяют:

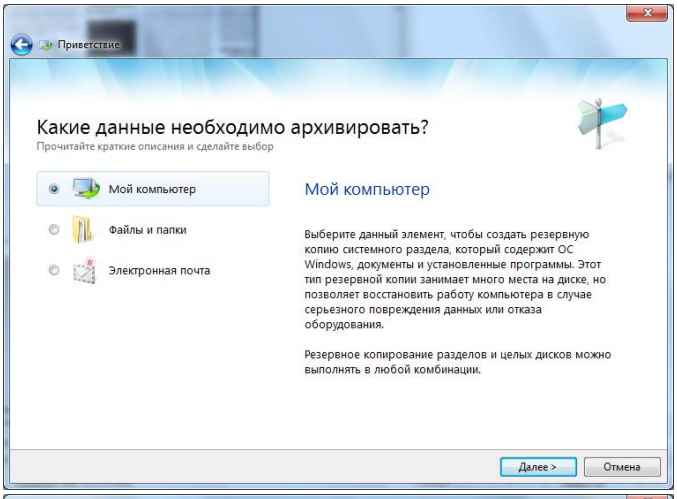
1. Резервное копирование наиболее ценных данных.

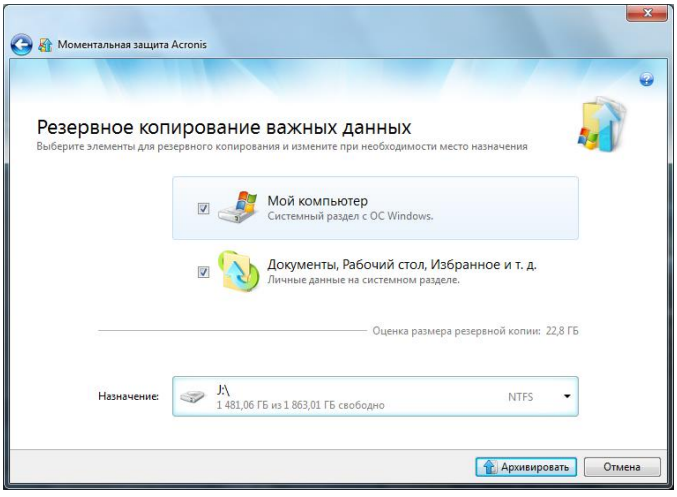
В случае реализации любой угрозы жесткий диск компьютера переформатируют, устанавливают операционную систему и другое программное обеспечение с дистрибутивных носителей, восстанавливают данные, которые берут с резервных носителей.

Резервное копирование проводят регулярно по плану. Копии хранят отдельно от компьютера (минимум две копии, которые хранят в разных местах).




Acronis True Image Home
Главная
Поиск
Acronis
Инструменты и утилиты
Try & Decide
Справка
Добавить резервные копии
Резервное копирование дисков и раз...
Защитить компьютер от аварийной ситуации.
Непрерывная защита
Установить непрерывную защиту разделов и файлов.
Онлайн-хранилище
Использовать хранилище данных в Интернете.
Дополнительные возможности:
Резервное копирование файлов
Резервное копирование электронной...
Создайте загрузочный носитель
Поиск резервной копии
Мои резервные копии
Debian жесткий диск
Восстановить
Операции
Всего: 10,50 КБ
Хранилище: J:\Мои документы\...ртуальные машины\
Просмотреть и восстановить
ubuntu
Восстановить
Операции
Всего: 2,25 ГБ
Хранилище: J:\Мои документы\...ые машины\Ubuntu\
Просмотреть и восстановить


Приветствие
Какие данные необходимо архивировать?
Прочитайте краткие описания и сделайте выбор
Мой компьютер
Файлы и папки
Электронная почта
Мой компьютер
Выберите данный элемент, чтобы создать резервную копию системного раздела, который содержит ОС Windows, документы и установленные программы. Этот тип резервной копии занимает много места на диске, но позволяет восстановить работу компьютера в случае серьезного повреждения данных или отказа оборудования.
Резервное копирование разделов и целых дисков можно выполнять в любой комбинации.
Далее >
Отмена


Моментальная защита Acronis
Резервное копирование важных данных
Выберите элементы для резервного копирования и измените при необходимости место назначения
Мой компьютер
Системный раздел с ОС Windows.
Документы, Рабочий стол, Избранное и т. д.
Личные данные на системном разделе.
Оценка размера резервной копии: 22,8 ГБ
Назначение:
J:\
1 481,06 ГБ из 1 863,01 ГБ свободно
NTFS
Архивировать
Отмена

2. Антивирусные программы, которые необходимо регулярно применять и регулярно обновлять.

3. Средства аппаратной защиты, например, отключение перемычки на материнской плате защитит от стирания ПЗУ (флеш-BIOS), независимо от того, кто будет пытаться это сделать: вирус, злоумышленник или неаккуратный пользователь.

4. Ограничение доступа посторонних лиц к компьютерам (физическое ограничение доступа, парольная защита и т.д).

Общие рекомендации по парольной защите:

- Не используйте одинаковый пароль для доступа к разным ресурсам;
- Не записывайте пароль в общедоступном месте;
- Используйте надежные пароли

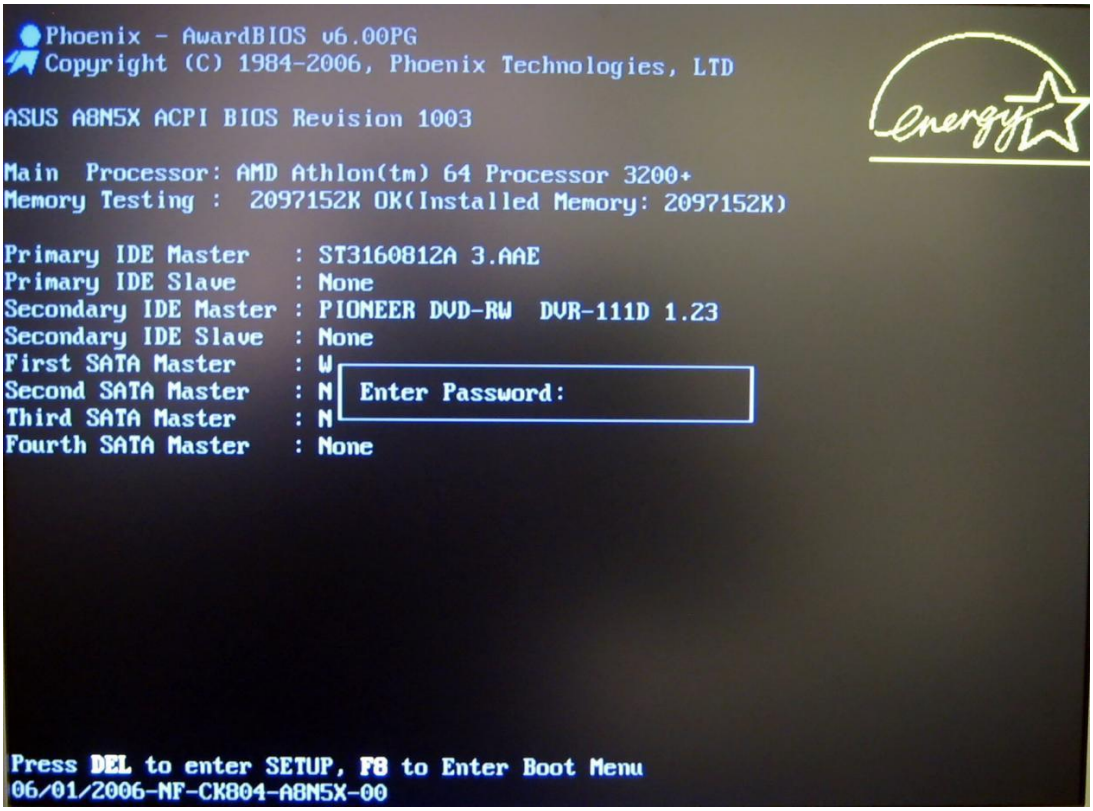
«Неправильные» пароли:

Цифровые (даты, телефоны, номера паспортов);
Слова, имена, клички и т.д.;
Малая длина (менее 8 символов).

«Правильные» пароли:

Длина 10 символов и более;
Комбинации маленьких и больших букв, специальных символов.

Пароль на уровне BIOS



Защита учетной записи пользователя

5. Оборудование компьютерных помещений средствами противодействия стихийным бедствиям (пожарам, потопам и т.д.).

6. Страхование различных видов.

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.

Сейчас защита компьютера от сетевых угроз ограничивается установкой антивируса, независимо от того, где находится ПК – дома или в офисе. Такой минимализм крайне опасен, поскольку установка одного антивируса не спасет от всех опасностей Интернета.

Обычно среднестатистический пользователь, приобретая «машину», через знакомых находит якобы специалиста по компьютерам.

В итоге ваш компьютер остался ненастроенным и. что еще страшнее, беззащитным. А теперь, представьте, что такой «специалист» настраивал не домашний, а ваш рабочий компьютер, на котором хранится большое количество жизненно важных данных, в том числе финансовой информации. Так что не пользуйтесь услугами мастеров, которые с радостью начинят ваш компьютер пиратским софтом.

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.

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.

Можно выделить основные источники проникновения вирусов в компьютерную сеть корпорации:

- 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 некой 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.

Впервые в России зараза атаковала мобильники в 2004 году. Тогда был всего только один вид вредителей - интернет-вирус Cabir. Распространялся он через Bluetooth, и ему поддавались только самые навороченные модели. Однако время не стоит на месте, и с каждым днем появляются все новые экземпляры «микробов». Аналитик «Лаборатории Касперского» Александр Гостев объясняет, насколько они опасны для трубок.

Болезни у мобильников точно такие же, что и у компьютеров. Самые известные - черви и троянцы. Троянцы «помогают» мобильным хакерам незаконно добывать информацию, закачанную в телефон, или воспользоваться трубкой без разрешения владельца. Обычно они не влияют на работу телефона. Но некоторые очень зловредны: им не могут противостоять даже антивирусы, и тогда вернуть трубку к жизни поможет только перепрошивка.

Черви обычно распространяются через MMS (это свойственно только червям). Вирус посылает по всем телефонам, найденным в адресной книге, свои копии в виде вложенного к MMS-сообщению файла. Некоторые модели способны запускать такие файлы автоматически. Это увеличивает угрозу заражения.

Пока в отличие от компьютерных собратьев большинство вирусов, атаковавших мобильники, не способны повредить трубку «насмерть». Максимум, что может произойти с вашим телефоном, - он будет «тормозить», зависать и самостоятельно, без вашей на то команды, рассылать SMS и MMS. А платить за проказы помощника, естественно, придется вам.

Плюс ко всему трубка будет быстро разряжаться. Больной телефон ищет потенциальную жертву и быстренько передает заразу с помощью беспроводной системы BiueTooth (если она есть в вашем аппарате), которая из-за этого постоянно находится в активном состоянии.

Как еще вредит «больной» телефон:

- ✓ Заражает файлы (часть информации может потеряться);
- ✓ Предоставляет удаленный доступ по сети (то есть в ваш телефон могут залезть посторонние, даже его не касаясь);
- ✓ Подменяет файлы иконок (ярлык запускает совсем не ту программу, которую он изображает и которая вам нужна);
- ✓ Загружает из Интернета или использует приложения с ошибками; сбивает с толку программ антивирусов.

Какие модели подвержены болезням

Бояться вирусов стоит владельцам любых смартфонов, работающих под управлением операционных систем Simbian и WindowsMobile – это дорогие, напичканные сложными функциями модели. Тем, кто пользуется простенькими телефонами, волноваться не стоит: они не заражаются, даже если в них загружены Java-приложения.

Защищаем аппарат:

1. В местах массового скопления людей пользуйтесь Bluetooth только в режиме «закрыт для всех».
2. Не принимайте файлы (мелодии, картинки) от незнакомых отправителей. И не рискуйте их запускать.
3. Не злоупотребляйте скачиванием игр, мелодий и изображений в Интернете. Это дополнительный риск.

Наиболее популярные антивирусные программы

Антивирусная программа (антивирус) - программа которая пытается обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы с зараженного компьютера, а также служит для профилактики - предотвращения заражения файлов вирусами.

Первые антивирусные программы появились практически сразу после появления первых вирусов. Сейчас разработкой антивирусных программ занимаются крупные компании. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

Практически все современные антивирусы не ограничиваются защитой только от вирусов, а детектируют так же троянские программы и некоторые другие.

В основу практически всех антивирусов входит:

* ядро;
* сканер;
* монитор активности;
* модуль обновления.

Принцип работы практически всех антивирусов следующий:

* Найти и удалить инфицированный файл;
* Заблокировать доступ к инфицированному файлу;
* Отправить файл в карантин (т.е. не допустить дальнейшего распространения вируса);
* Попытаться "вылечить" файл, удалив вирус из тела файла;
* В случае невозможности лечения-удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Для того, чтобы антивирусная программа постоянно успешно работала, *ф* необходимо базу сигнатур вирусов периодически загружать (обычно, через Интернет).

Для успешной защиты компьютера от вирусов желательно поставить Один "антивирус" и Один "firewall" (сейчас уже есть антивирусные программы которые предоставляют комплексную защиту - совмещая в себе и то и другое), если поставить больше то они не смогут работать вместе и это будет вызывать "зависание" компьютера и постоянное торможение, что только ухудшит защиту.

На сегодняшний день список антивирусных программ весьма огромен. Они различаются как по своим функциональным возможностям, так и по цене. Существуют конечно и бесплатные версии антивирусных программ.

Далее представлен список наиболее популярных антивирусных программ на сегодняшний день:

Антивирус Касперского- продукт для защиты вашего ПК, чья эффективность проверена миллионами пользователей во всем мире. Программа включает в себя основные инструменты для защиты ПК .

Страница разработчика: www.kaspersky.ru

ESETNOD32 обеспечивает обнаружение и блокировку вирусов, троянских программ, червей, шпионских программ, рекламного ПО, фишинг-атак, руткитов и других интернет-угроз, представляющих опасность для компаний. Несмотря на минимальную потребность в ресурсах, данное решение обеспечивает непревзойденный уровень проактивной защиты, практически не снижая производительность компьютера.

Страница разработчика: wvw.eset.com

SymantecNortonAnti-Virus

Разработанная компанией Symantec программа NortonAntiVirus является наиболее популярным антивирусным средством в мире. Эта программа автоматически удаляет вирусы, интернет-червей и троянские компоненты, не создавая помех работе пользователя. NortonAntiVirus позволяет противостоять угрозам самых современных spyware- и adware-программ и блокирует работу таких программ еще до того момента, как пользователь перенаправляется на другой сайт.

Страница разработчика: www.symantec.com

Dr. Web

Антивирус Dr.Web проверит всю Windows память даже зараженного компьютера. Доктор Веб проводит полную антивирусную проверку Windows-памяти компьютера и способен остановить вирусный процесс. Важным показателем качества работы антивирусной программы является не только ее способность находить вирусы, но и лечить их, не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное "здоровое" состояние.

Страница разработчика: www.drweb.ru

TrendMicroInternetSecurity позволяет очень просто защитить ваш компьютер, ваши приватные персональные данные и вашу онлайн- активность. Продукт обеспечивает защиту как от существующих вирусов, программ-шпионов и кражи данных, так и от будущих веб-угроз. Пользуйтесь электронной почтой, интернет-магазинами, онлайн-банкингом, обменивайтесь цифровыми фотографиями и не беспокойтесь о безопасности вашей приватной информации.

Страница разработчика: www.ru.trendinicro.com

Avast! ProfessionalEdition вобрал в себя все высокопроизводительные технологии для обеспечения одной цели: предоставить вам наивысший уровень защиты от компьютерных вирусов. Данный продукт представляет собой идеальное решение для рабочих станций на базе Windows. Новая версия ядра антивируса avast! обеспечивает высокий уровень обнаружения вкупе с высокой эффективностью, что гарантирует 100%-ое обнаружение вирусов "In-the-Wild" и высокий уровень обнаружения троянов с минимальным числом ложных срабатываний. Механизм антивирусного ядра сертифицирован ICSA, постоянно принимает участие в тестах VirusBulletin и получает награды VB100%. Внешний вид пользовательского интерфейса отображается с помощью так называемых скинов, поэтому у вас есть возможность настроить внешний вид панели продуктов avast! по своему желанию.

Страница разработчика: www.avast.ru

BitDefenderAntivirus - мощная антивирусная программа с разнообразными^ возможностями, позволяющими оптимально защитить персональный компьютер.BitDefenderAntivirus защищает от компьютерных вирусов с применением технологий ICSALabs, VirusBulletin, Checkmark, CheckVir и TUV. Модуль B-HAVE подражает действительному (виртуальному) "компьютеру в компьютере". Эта BitDefender-технология представляет новый уровень безопасности, обнаруживая и обезвреживая даже редкие вирусы, или вирусный код, для которого еще не вышли новые базы записей вирусов.

Страница разработчика: www.bitdefender.com

PandaAntivirus является самым простым и интуитивно понятным в использовании решением безопасности для домашнего ПК. После установки программы пользователь может забыть о вирусах, программах-шпионах, руткитах, хакерах, онлайн-мошенниках и больше не беспокоиться о сохранности конфиденциальной информации.

PandaAntivirus имеет простые настройки, легкий и понятный интерфейс, автоматическое обновление (после установки сразу будет искать обновления), осуществляет контроль на уровне TCP/IP.PandaAntivirus является достаточно надежным антивирусом подойдет в первую очередь для домашнего пользования Страница разработчика: http://www.viruslab.ru/

McAfeeVirusScan

Продукт McAfeeVirusScan осуществляет сканирование файловых серверов^ и рабочих станций по расписанию и по запросу пользователя, способен обнаруживать и обезвреживать вирусы-трояны и программы-черви. Кроме того, системные администраторы получают возможность присваивать программам и процессам ту или иную степень приоритетности, в соответствии с которой они и будут сканироваться антивирусом, что позволяет экономить ресурсы корпоративных сетей.

Страница разработчика: www.mcafee.com

AviraAntiVir

Популярный антивирус германской сборки. Эту программу всегда отличали качество работы и быстрая реакция на появление новых вирусов. Она включает в себя резидентный монитор, сканер и программу обновления. AntiVir может постоянно следить за файлами и архивами, которые могут быть потенциальными переносчиками вирусов. Отыскиваются также и макросы, которые внедряются в офисные документы. Программа нетребовательна к ресурсам и показывает хорошие результаты в работе по скорости и качеству поиска.

Страница разработчика: www.free-av.com

Проактивная защитаоснована на контроле и анализе поведения всех программ, установленных на компьютере, может обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. *Таким образом, компьютер защищен не только от уже и местных вирусов, но и от новых, еще не исследованных.*

Анти-Шпионотслеживает нежелательные действия на компьютере и блокирует их выполнение. Например, компонент блокирует показ баннеров и всплывающих окон, мешающих пользователю при работе с веб-ресурсами, блокирует работу программ, пытающихся осуществить несанкционированный пользователем дозвон (если соединение с Интернет осуществлено через телефонную линию), анализирует веб-страницы на предмет фишинг-мошенничества.

Анти-Хакеркомпонент предназначенный для защиты компьютера при работе в интернете и других сетях. Он контролирует все сетевые соединения, обнаруживает сетевые атаки и обеспечивает невидимость компьютера в сети.

Для поиска вирусов в состав антивируса включены три задачи:

1) Критические области проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты исполняемые при старте системы, загрузочные сек тора дисков, системные каталоги Windows. Цель задачи - быстрое обнаружен не в системе активных вирусов, без запуска полной проверки компьютера.

2) Мой компьютер поиск вирусов с тщательной проверкой всех подключенных дисков, памяти файлов.

3) Объекты автозапуска проверка объектов, загрузка которых осуществляется при старте операционной системы, а так же оперативной памяти и загрузочных секторов дисков.

Так же предусмотрена возможность создавать другие задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых баз раз в неделю или задачу поиска в каталоге МОИ ДОКУМЕНТЫ

Разработчики антивирусных программ – www.comss.ru

- Comodo Group – США,
- Dr. Web – Россия (www.drweb.com),
- EsetNOD32 – Словакия (www.esethod32.ru),
- McAfee – США,
- Outpost – Россия,
- Panda Software – Испания,
- Symantec – США,
- Trend Micro – Япония,
- Антивирус Касперского – Россия (www.kaspersky.ru).

Есть и бесплатные антивирусы. Они создаются известными компаниями, однако не содержат многих "удобств", присущих платным версиям, или показывают пользователю рекламные картинки - так называемые баннеры. Тем не менее бесплатные антивирусы также неплохо справляются со своей задачей. Например, чешская компания AVG предлагает всем желающим загрузить свой бесплатный продукт со страницы http://free.avg.com.

Если вы подозреваете, что ПК заражен (например, он заметно "тормозит" и отправляет в Интернет какие-то данные, хотя вы ничего не делаете), однако не можете позволить себе покупку антивируса, можно воспользоваться такими программами. У "Лаборатории Касперского" такая утилита называется KasperskyVirusRemovalTool (www.kaspersky.ru/removaltools). Компания "Доктор Веб" выпускает утилиту Dr.WebCureIt! (www.freedrweb.com/cureit/).

Лучшие протестированные бесплатные антивирусы это (www.computerologia.ru):

- ✓ 360 Total Security;
- ✓ Panda Free Antivirus;
- ✓ Avast Free Antivirus.

Что нужно сделать, для того чтобы не стать жертвой вируса. Во-первых, необходимо установить на компьютер антивирус (хотя бы бесплатный). Во-вторых, следить за обновлениями для операционной системы. В-третьих, быть внимательным и посещать только проверенные интернет-сайты, каждый раз приглядываясь к адресу, который написан в строке браузера (создатели сайтов-подделок могут просто переставить местами буквы: odnoklassinki.ru).

Какие бы не использовались антивирусные программы, 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 KasperskyInspector), однако они, как правило, лишь констатируют факт несанкционированного изменения файлов, а лечение возможно лишь после появления новых версий антивирусов.

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.

- 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 MicrosoftOffice 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. [41]

3. Этапы построения системы защиты информации в информационную безопасность

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 [57]:

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:

• Для определения, общих правил обработки информации в АИС, целей построения и функционирования системы защиты и подготовки сотрудников.

• Для фиксирования на некоторый момент времени состава АИС, технологии обработки информации, средств защиты информации.

• Для определения должностных обязанностей сотрудников организации по защите информации и ответственности за их соблюдение.

План представляет собой организационный фундамент, на котором строится все здание системы защиты. Он нуждается в регулярном пересмотре и, если необходимо, изменении.

План защиты обычно содержит следующие группы сведений:

- Политика безопасности.
- Текущее состояние системы.
- Рекомендации по реализации системы защиты.
- Ответственность персонала.
- Порядок ввода в действие средств защиты.
- Порядок пересмотра плана и состава средств защиты.

Рассмотрим подробнее эти группы сведений.

Политика безопасности. В этом разделе должен быть определен набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в АИС. Раздел должен содержать:

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

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

• Обязательства и санкции, связанные с защитой (например, штрафы, персональная ответственность и др.).

Рекомендации по реализации системы защиты. Всесторонний анализ риска должен определять размеры наибольших возможных потерь, независимо от вероятности появления соответствующих событий; размеры наибольших ожидаемых потерь; меры, предпринимаемые в случае критических ситуаций, а также стоимость таких мер. Эти результаты используются при определении зон особого контроля и распределении средств для обеспечения защиты. В этом случае план защиты должен содержать рекомендации, какие средства контроля лучше всего использовать в чрезвычайных ситуациях (то есть имеющие наибольшую эффективность) и какие лучше всего соответствовали бы средствам контроля повседневной работы.

Некоторые ситуации могут приводить к слишком большому ущербу (например, крушение системы), а стоимость средств защиты от них может быть слишком высока или

эти средства окажутся неэффективны. В этом случае лучше не учитывать такие ситуации при планировании защиты, хотя их и возникающие при этом возможные последствия следует отразить в плане.

Ответственность персонала. Каждый сотрудник обслуживающего персонала вычислительной системы должен хорошо знать свои обязанности и нести ответственность за свои действия. Ниже приводятся некоторые примеры обязанностей сотрудников и групп сотрудников:

- Пользователь персонального компьютера или терминала несет ответственность за физическую целостность компьютера (терминала) во время сеанса работы с АИС, а также за неразглашение собственного пароля.
- Администратор баз данных несет ответственность за конфиденциальность информации в базах данных, ее логическую непротиворечивость и целостность.
- Сотрудник руководства отвечает за разделение обязанностей служащих в сфере безопасности обработки информации, предупреждение возможных угроз и профилактику средств защиты.

Порядок ввода в действие средств защиты. Ввод в работу крупномасштабных и дорогих средств защиты целесообразно проводить постепенно, давая возможность обслуживающему персоналу и пользователям спокойно ознакомиться со своими новыми обязанностями. Для этого необходимо проводить разного рода тренировки, занятия по разъяснению целей защиты и способов ее реализации.

Этот раздел плана содержит расписание такого рода занятий, а также порядок ввода в действие системы защиты.

Порядок модернизации средств защиты. Важной частью плана защиты является порядок пересмотра состава средств защиты. Состав пользователей, данные, обстановка — все изменяется с течением времени, появляются новые программные и аппаратные средства. Многие средства защиты постепенно теряют свою эффективность и становятся ненужными, или подлежат замене по какой-либо иной причине (например, уменьшается ценность информации, для обработки которой достаточно более простых средств защиты). Поэтому список объектов, содержащих ценную информацию, их содержимое и список пользователей должны периодически просматриваться и изменяться в соответствии с текущей ситуацией. Также

периодически должен проводиться анализ риска, учитывающий изменения обстановки. Последний пункт плана защиты должен устанавливать сроки и условия такого пересмотра, а также условия, при которых может производиться внеочередной пересмотр (например, качественный скачок в разработке методов преодоления защиты, что может нанести серьезный ущерб пользователям и владельцам АИС).

Каким бы всеобъемлющим не был план, все возможные угрозы и защиту от них он предусмотреть не в состоянии. К тому же многие ситуации он должен только описывать — их контроль может оказаться неэффективным (в силу дороговизны средств защиты или малой вероятности появления угроз). В любом случае владельцы и персонал системы должны быть готовы к различным непредвиденным ситуациям.

Для определения действий персонала системы в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АИС необходимо разрабатывать план обеспечения непрерывной работы и восстановления (план ОНРВ). В некоторых случаях план обеспечения непрерывной работы и план восстановления —

разные документы. Первый скорее план, позволяющий избежать опасных ситуаций, второй — план реакции на них.

План ОНРВ можно сравнить с планом противопожарной защиты (обеспечение непрерывной работы) и ликвидации последствий (минимизация ущерба и восстановление функционирования АИС). Про этот план обычно все знают, но никто его не читает, хотя на пепелище об этом обычно сожалеют.

Существует несколько способов смягчения воздействия непредвиденных ситуаций:

• Избегать их. Это наиболее эффективный, но не всегда осуществимый способ. Избегать непредвиденных ситуаций можно с помощью ограничительных мер, предусмотренных планом защиты, а можно и с помощью устранения самой причины потенциального нарушения. Например, с пожаром можно бороться огнетушителем, а можно соблюдением мер противопожарной защиты. С рассерженными пользователями можно бороться административными мерами (разозлив этим их еще больше), а можно и поддержанием здоровой атмосферы в коллективе.

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

• Если предполагать, что какие-то нарушения все-таки могут произойти, следует предусмотреть меры сохранения контроля над ситуацией. Например, в любой момент может выйти из строя отдельный блок системы — часть компьютера, компьютер целиком, подсеть и т.д., может наступить нарушение энергоснабжения и др. В принципе это может привести к выходу АИС из строя, однако при правильной организации АИС этого можно избежать.

• Если нарушение произошло, необходимо предусмотреть меры по ликвидации последствий и восстановлению информации. Например, в случае сбоя в компьютере — замену сбойного компонента, в случае уничтожения каких-либо данных — восстановление с резервных копий и т.д.

Все приведенные выше четыре способа должны в той или иной мере присутствовать в плане ОНРВ. Для каждой конкретной АИС эти меры следует планировать в процессе анализа риска с учетом особенностей (специфических видов угроз, вероятностей появления, величин ущерба и т.д.) и на основе критерия «эффективность/стоимость». Хороший план ОНРВ должен отвечать следующим требованиям:

* Реальность плана ОНРВ.

План должен оказывать реальную помощь в критических ситуациях, а не оставаться пустой формальностью. Необходимо учитывать психологический момент ситуации, при которой персонал находится в состоянии стресса, поэтому сам план и предлагаемые действия должны быть простыми и ясными. План должен учитывать реальное состояние компонентов системы, способов их взаимодействия и т.д. Повышению действенности плана ОНРВ способствуют тренировки в условиях, приближенных к реальным (естественно без реальных потерь).

* Быстрое восстановление работоспособности системы.

Предлагаемые планом ОНРВ действия должны восстанавливать повседневную деятельность настолько быстро, насколько это возможно. В принципе это главное назначение плана ОНРВ. Расследовать причины и наказать виновных можно потом, главное — продолжить процесс обработки информации.

• Совместимость с повседневной деятельностью.

Предлагаемые планом ОНРВ действия не должны нарушать привычный режим работы. Если его действия противоречат повседневной деятельности (возможно, возобновленной после аварии), то это приведет к еще большим проблемам.

• Практическая проверка.

Все положения плана ОНРВ должны быть тщательно проверены, как теоретически, так и практически. Только в этом случае план ОНРВ будет удовлетворять перечисленным выше требованиям.

• Обеспечение.

Реальная выполнимость плана ОНРВ будет достигнута только в том случае, если предварительно подготовлено, проверено и готово к работе все вспомогательное обеспечение — резервные копии, рабочие места, источники бесперебойного питания и т.д. Персонал должен совершенно точно знать, как и когда пользоваться этим обеспечением.

Наличие любого плана ОНРВ — полного или краткого, но главное — реального, благотворно влияет на моральную обстановку в коллективе. Пользователи должны быть уверены в том, что даже в самых неблагоприятных условиях какая-то часть их труда будет сохранена; руководство должно быть уверено, что не придется начинать все с начала.

План ОНРВ лучше всего строить как описание опасных ситуаций и способов реакции на них в следующем порядке:

- описание нарушения;
- немедленная реакция на нарушение - действия пользователей и администрации в момент обнаружения нарушения (сведение ущерба до минимума, уведомление руководства, остановка работы, восстановительные процедуры и т.д.);
- оценка ущерба от нарушения — в чем заключаются потери и какова их стоимость (включая восстановление);
- возобновление обработки информации. После устранения нарушения и первичного восстановления необходимо как можно быстрее возобновить работу, так как машинное время — это деньги;
- полное восстановление функционирования системы - удаление и замена поврежденных компонентов системы, возобновление обработки информации в полном объеме.

В части, посвященной реакции на нарушения, план ОНРВ должен содержать перечень действий, которые выполняются персоналом при наступлении различных ситуаций. Причем действия должны быть реальными, иначе в них нет никакого смысла.

Эта часть плана должна определять:

- что должно быть сделано;
- когда это должно быть сделано;
- кем и как это должно быть сделано;
- что необходимо для того, чтобы это было сделано.

При планировании подобных действий необходимо помнить об их экономической эффективности. Например, всю информацию системы в резервных копиях держать в принципе невозможно — ее слишком много и она слишком часто обновляется. В копиях должна содержаться только самая ценная информация, значимость которой уменьшается не слишком быстро. Вообще определение степени дублирования ресурсов (критичной нагрузки; criticalworkload) — самостоятельная и достаточно сложная задача. Она должна решаться индивидуально для конкретных условий с учетом стоимости дублирования и загрузки системы, размеров возможного ущерба, имеющихся ресурсов и других факторов.

Для определения конкретных действий по восстановлению и возобновлению процесса обработки, включаемых в план ОНРВ, может быть полезен приводимый ниже список способов организации восстановления программ и данных, а также процесса обработки информации (первый способ для восстановления программ и данных, остальные — для возобновления самого процесса обработки информации).

Способы организации восстановления работы:

Резервное копирование и внешнее хранение программ и данных. Это основной и наиболее действенный способ сохранения программного обеспечения и данных. Резервные копии делаются с наборов данных, потеря или модификация которых могут нанести значительный ущерб. Обычно в таких копиях хранятся системное программное обеспечение и наборы данных, наиболее важное прикладное программное обеспечение, а также наборы данных, являющиеся основными в данной системе (например, база данных счетов в банке).

Резервное копирование может быть полным (копии делаются со всех наборов данных), возобновляемым (копии некоторых наборов данных периодически обновляются) и выборочным (копии делаются только с некоторых наборов данных, но потом не обновляются). Способы резервного копирования определяются для каждой конкретной АИС индивидуально с точки зрения критерия экономической эффективности.

Резервное копирование не имеет никакого, смысла, если копии могут быть уничтожены вместе с оригиналами. Поэтому копии должны храниться в надежном месте, исключающем возможность уничтожения. В тоже время, должны существовать возможность их оперативного использования. Иногда хранят две и более копий каждого набора данных. Например, одна копия может храниться в сейфе, находящемся в границах доступа персонала системы, а другая — в другом здании. В случае сбоя оборудования в системе используется первая копия (оперативно!), а в случае ее уничтожения (например, при пожаре) — вторая.

Взаимодействие служб. Услуги по возобновлению процесса обработки предоставляются по взаимной договоренности другими службами или организациями, обычно безвозмездно. Взаимопомощь бывает двух видов:

• Внешняя — другая организация предоставляет свою АИС, возможно программное обеспечение для временной обработки информации пострадавшей стороной. Такой способ возобновления процесса обработки информации может использоваться для обработки небольших объемов некритичной информации. При этом желательно, чтобы две организации были примерно одного типа и работали в одной области.

• Внутренняя — возможность обработки информации предоставляется другими подразделениями одной и той же организации (департаментами, отделами, группами).

Такой способ обычно не требует больших затрат и легко доступен, если дублирующая АИС позволяет проводить такого рода обработку.

Любой план хорош в том случае, если он выполним. Для обеспечения выполнимости планов необходимо чтобы работу по их составлению выполняла группа квалифицированных специалистов, размеры которой зависят от характера организации и масштабов предполагаемых мер защиты. Оптимальная численность группы 5-7 человек. Можно привлечь дополнительных сотрудников для обработки и анализа выводов и рекомендаций основной группы, или, в случае больших объемов работы, каждая группа должна составлять один план или один из пунктов плана.

Специализация сотрудников, входящих в группу разработки планов, зависит от конкретных условий. Использование защищенных протоколов, механизмов защиты операционных систем и сетей требует привлечения системных программистов. Применение средств защиты, встраиваемых в прикладное программное обеспечение, делает необходимым участие в группе проблемных программистов. Необходимость организации защиты физических устройств, организации резервных рабочих мест также требует присутствия в рабочей группе соответствующих специалистов. И, наконец, поскольку система функционирует для пользователя, то целесообразно присутствие пользователей различных категорий - для учета взгляда со стороны на удобство и эффективность предлагаемых методов и средств защиты. В большинстве случаев целесообразно, чтобы в эту группу входили следующие специалисты, каждый из которых должен отвечать за свой участок работы:

- специалисты по техническим средствам;
- системные программисты;
- проблемные программисты;
- сотрудники, отвечающие за подготовку, ввод и обработку данных;
- специалисты по защите физических устройств;
- представители пользователей.

После подготовки плана необходимо его принять и реализовать, что напрямую зависит от его четкости, корректности и ясности для сотрудников организации.

Понимание необходимости мер защиты и контроля - 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.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов.

Разработка политики и программы безопасности начинается с анализа рисков, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными угрозами.

Главные угрозы - внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе нарушений растет доля внешних атак, но основной ущерб по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить базовый уровень безопасности при минимальных интеллектуальных и разумных материальных затратах.

Существенную помощь в разработке политики безопасности может оказать британский стандарт BS7799:1995, предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия уровня детализации. Они должны подразделяться на несколько уровней, трактующих вопросы разной степени специфичности. Важным элементом программы является разработка и поддержание в актуальном состоянии карты ИС.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение жизненного цикла ИС и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Меры процедурного уровня ориентированы на людей (а не на технические средства) и подразделяются на следующие виды; управление персоналом;

- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

Здесь также применимы объектный подход и понятие жизненного цикла. Первый позволяет разделить контролируемые сущности (территорию, аппаратуру и т.д.) на относительно независимые подобъекты, рассматривая их с разной степенью детализации и контролируя связи между ними.

Понятие жизненного цикла полезно применять не только к информационным системам, но и к сотрудникам. На этапе инициации должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности; на этапе выведения из эксплуатации следует действовать аккуратно, не допуская нанесения ущерба обиженными сотрудниками.

Информационная безопасность во многом зависит от аккуратного ведения текущей работы, которая включает:

- поддержку пользователей; поддержку программного обеспечения; конфигурационное управление;
- резервное копирование; управление носителями;
- документирование;

- регламентные работы.

Элементом повседневной деятельности является отслеживание информации в области ИБ; как минимум, администратор безопасности должен подписаться на список рассылки по новым пробелам в защите (и своевременно знакомиться с поступающими сообщениями).

Нужно, однако, заранее готовиться к событиям неординарным, то есть к нарушениям ИБ. Заранее продуманная реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

Выявление нарушителя - процесс сложный, но первый и третий пункты можно и нужно тщательно продумать и отработать.

В случае серьезных аварий необходимо проведение восстановительных работ. Процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;

идентификация ресурсов, необходимых для выполнения критически важных функций;

- определение перечня возможных аварий;
- . разработка стратегии восстановительных работ; подготовка к реализации выбранной стратегии;
- проверка стратегии.

Оценка эффективности инвестиций в информационную безопасность [57]

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 GartnerGroup 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 GartnerGroup, 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 (**DiscountedCashFlows – 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 (**WeightedAverageCostofCapital – 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 (**NetPresentValue – 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 5.

Таблица 5

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 (**InternalRateofReturn – 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.

Контрольные вопросы к теме 5

1. Какие организационно-административные меры Вы знаете?
2. Назовите составляющие организационного обеспечения компьютерной безопасности.
3. Что входит в состав организационно-технических мер?
4. Перечислите организационно-экономические меры защиты информации.
5. Какие качества проверяются у лиц при приеме на работу?
6. Что включает конфиденциальное делопроизводство?
7. Для чего применяют межсетевые экраны?
8. Как классифицируются технические средства противодействия?
9. Какие подразделения в службе безопасности?
10. Каковы масштабы применения Интернета в мире?
11. Какие информационные угрозы являются платой за использования Интернета?
12. Назовите меры по защите информации в интернете.
13. Для чего используются межсетевые экраны-брандмауэры?
14. Что используется для защиты электронной почты?
15. Что можно использовать для защиты от вирусов?
16. Какие Вы знаете антивирусные программы?
17. Назовите основные источники проникновения вирусов.
18. Как пакостит «больной» телефон?
19. В чем разница симметричного и ассиметричного шифрования?
20. Какие особенности компании необходимо учитывать при разработке системы защиты?
21. Что необходимо защищать в корпоративной сети?
22. Назовите основные этапы построения системы защиты.
23. Как классифицируют меры обеспечения безопасности по способам осуществления?
24. В чем отличия «встроенной» защиты от «добавленной»?
25. Что делается на этапе сопровождения системы?
26. Назовите критерии оптимального соотношения в анализе различных вариантов построения системы защиты.
27. Что включает план защиты?
28. Дайте характеристику плана обеспечения непрерывной работы и восстановления (ОНРВ).
29. Как оценить эффективность инвестиций в информационную безопасность?

Тесты к теме 5

1. Минимизация утечки информации через персонал это

А. организационно-технические средства защиты информации;
Б. организационно-экономические меры;
В. организационно-административные меры.

2. К организации конфиденциального делопроизводства относится:

А. организация документооборота;
Б. использование сертифицированных технических и программных средств;
В. проверка надежности сотрудников.

3. Организационное обеспечение информационной безопасности – это..?

А. реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;
Б. совокупность средств, обеспечивающих удобства работы пользователей;
В. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

4. С увольняющимися сотрудниками
А. подписывается договор о не распространении конфиденциальности;
Б. обмениваются рукопожатием;
В. предлагают вернуться.

5. Организация документооборота предполагает:
А. исключение доступа к бумажной «стружке»;
Б. предупреждение не обоснованного ознакомления с документами;
В. исключение не обоснованной рассылки.

6. Проведение организационно-экономических мероприятий предполагает:
А. страхование информационных рисков;
Б. организацию пассивного противодействия техническими средствами;
В. обеспечения электронного документооборота.

7. Адрес электронной почты включает:
А. Логин.
Б. Символический адрес сервера и имя зоны.
В. Все вышеперечисленное.

8. Электронная почта НЕ служит для:
А. Передачи текстовых сообщений в пределах Интернет.
Б. Системы телеконференций.
В. Оповещения пользователей о наступлении определенных событий.

9. Информационными угрозами в Интернете НЕ является:
А. Несанкционированный доступ к сети организации.
Б. Сбор и мониторинг сетевой информации в интересах третьих лиц.
В. Использование брандмауэра.

10. Для защиты электронной почты в Интернете используются:
А. Антивирусные программы.
Б. Специальные протоколы (REM, CryptoAPi и др.)
В. Наиболее простое обозначение электронной почты (фамилия, паспортные данные и т.п.).

11. Основные сервисы системы Интернет:
А. WorldWideWeb (WWW).
Б. Программы-браузеры и системы телеконференций.
В. Все вышеперечисленное.

12. К серверам системы Интернет НЕ относятся:

А. Программа печати учетных документов.

Б. Программа пересылки файлов.

В. Система информационного поиска сети Интернет.

13. Адрес электронной почты имеет вид:

А. логин@символический адрес сервера.имя зоны;

Б. логин.имя зоны;

В. логин.

14. Межсетевой экран – это

А. Брандмауэр (Firewalls);

Б. Фильтр;

В. Антивирусная программа.

15. Чтобы избавиться от мобильного вируса:

А. Нужно пользоваться клавишным мобильником.

Б. Приобрести самый дорогостоящий мобильник.

В. Познакомиться с хакером.

16.Каждую систему защиты следует разрабатывать индивидуально, учитывая:

А. Организационную структуру организации;

Б. Объем и характер информационных потоков;

В. Все вышеперечисленное.

17. Первый этап построения системы защиты:

А. Планирование;

Б. Анализ;

В. Реализация системы защиты.

18. По способу осуществления всех мер обеспечения безопасности подразделяются на:

А. Правовые и морально-этические;

Б. Административные, физические, аппаратные и программные;

В. Все вышеперечисленное.

19. Чаще всего применяется способ реализации защиты:

А. «Встроенная»;

Б. Комбинированная;

В. «Добавленная».

20. Этапы сопровождения это:

А. Контроль работы системы, регистрация происходящих в ней событий и их анализ;

Б. Планирование системы защиты;

В. Реализация системы защиты.

21. Политика безопасности входит в

А. Анализ рисков;

Б. План защиты;

В. Управление доступом.

22. План обеспечения непрерывной работы и восстановления включает:
А. Что и когда должно быть сделано;
Б. Кем и как это должно быть сделано;
В. Все вышеперечисленное.

23. Относится к вложениям в информационную безопасность следует как:
А. К затратам;
Б. к инвестициям;
В. К неизбежным потерям.

Тема 6. Менеджмент и аудит систем ИБ

1. Управление информационной безопасностью государственных структур.
2. Менеджмент и аудит информационной безопасности на уровне предприятия.
3. Аудит информационной безопасности электронной коммерции.
4. Менеджмент информационной безопасности электронной коммерции.

1. Управление информационной безопасностью государственных структур

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и т.п.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике *деятельность* органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная *стабильность* и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают *затраты* и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и т.п.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- сохранение суверенитета государства;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- укрепление законности и правопорядка;
- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- участие в жизни международного сообщества. [8]

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, *деятельность* государства в этой сфере, подразделяются на:

- политические;
- социально-экономические;
- организационно-технические.

Организационная *деятельность* государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

- внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и т.п.;
- внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и т.п.

Таким образом, *деятельность* государства в этой сфере направлена на нейтрализацию существующих *угроз информационной безопасности* с учетом всех факторов, воздействующих как на сами *управляющие* государственные структуры, так и на *информационные системы*.

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют *доступ* к информации, составляющей *государственную тайну*, и другие.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

- создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и *банковской тайны*, право на беспрепятственный доступ к информации и т.п. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками;
- осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для *реализации требований* законодательства;
- выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности. [6]

Функции создания и постоянного совершенствования законодательно-правовой базы, обеспечивающей защиту законных частных, коммерческих, общественных и государственных интересов, реализуются законодательными органами (парламентами) государств. Как правило, все законодательные функции в данной сфере в большинстве стран осуществляются центральными (федеральными) органами законодательной власти, а местные (региональные) органы таких полномочий не имеют. Для создания и поддержания в актуальном состоянии законодательства в сфере информационной безопасности в законодательных органах могут создаваться профильные комитеты и комиссии, которые состоят из членов данного законодательного органа, имеющих некоторые базовые знания и навыки в сфере информационных технологий и правового регулирования вопросов информационного обмена. Кроме того, вопросы

совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- оборона;
- национальная безопасность;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика;
- наука и образование
- и других.

Для разработки соответствующих нормативно-правовых актов *подразделения* (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

- органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. "силовых" министерствах и ведомствах, юридических ведомствах и т.п.);
- частных компаниях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и т.п.;
- научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.

Процедуры согласования, принятия и утверждения законодательных актов, а также процедуры контроля за действиями органов исполнительной власти в каждой стране определяются в соответствии с действующим законодательством (конституцией).

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную *деятельность*.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется *по* нескольким относительно самостоятельным направлениям.

- Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.
- Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.
- Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).
- Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и т.п.).

• Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и т.п.).

• Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).

• Поддержка научных исследований в сфере информационной безопасности.

• Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами других стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инцидентов (раскрытия преступлений и т.п.). [3]

Судебные функции, как правило, реализуются судами общей юрисдикции, так же как и для всех остальных гражданских и уголовных дел. Специальных судебных инстанций, которые были бы предназначены для рассмотрения дел, связанных с информационной безопасностью (таких как, например, суды *по* правам человека или военные суды), не существует. При этом могут создаваться судебные лаборатории, специализирующиеся на проведении экспертиз, анализов и исследований различных элементов информационных систем в связи с расследованиями и судебными разбирательствами *по* делам о нарушениях в сфере информационной безопасности.

Основой организации государственной деятельности в сфере информационной безопасности является национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности. Этот документ, издаваемый, как правило, главой исполнительной ветви власти (президентом страны) отражает:

• признание государственной властью существенной значимости проблем защиты информации для общества, личности, экономики и самого государства;

• современное понимание общего ландшафта информационной безопасности на национальном уровне: потенциально уязвимые информационные объекты, *источники угроз* и др.;

• основные направления, в которых государство намерено осуществлять активные действия с целью повышения уровня информационной безопасности на национальном уровне (создание систем безопасности, упорядочивание взаимоотношений различных субъектов, пресечение правонарушений, развитие инфраструктуры и технологий безопасности и т.п.).

В рамках утвержденной государственной доктрины информационной безопасности:

• создаются специализированные правительственные организации, отвечающие за реализацию политики информационной безопасности и решение отдельных задач в этой сфере;

• отдельные правительственные учреждения наделяются специфическими функциями и полномочиями, связанными с *управлением информационной безопасностью* (как в общегосударственном масштабе, так и в рамках определенных сфер ответственности), а также создаются специальные структурные подразделения, отвечающие за решение вопросов защиты информации и информационной инфраструктуры;

• создается система локальных правовых актов, регулирующих отношения в сфере защиты информации, а также система государственных стандартов, относящихся к технологиям и организации защиты информации.

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и т.п.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий. Государственная стандартизация позволяет достичь универсальности при оценке используемых технологий и методов и, таким образом, до определенной степени упорядочить многие взаимоотношения, связанные с использованием таких технологий и методов. Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов. Основными объектами государственной и международной стандартизации могут выступать:

- методы шифрования и криптографической защиты данных;
- технологии идентификации пользователей информационных систем;
- методы аутентификации;
- методы тестирования (проверки) и оценки информационных систем на предмет их защищенности;

а также некоторые другие элементы систем обеспечения информационной безопасности.

Основой современной политики Российской Федерации в сфере информационной безопасности можно считать "Доктрину информационной безопасности РФ", утвержденную Президентом РФ Владимиром Путиным 9 сентября 2000г. Этот документ:

- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, *источники угроз* и т.п.);
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и т.п.;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни;

- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности. [5]

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- экономика;
- внутренняя политика;
- внешняя политика;
- наука и техника;
- духовная жизнь;
- информационные системы государственного управления;
- оборона.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- совершенствование законодательной базы в сфере информационных отношений;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- подготовку кадров для работы в сфере информационной безопасности;
- совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения и т.п.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия "*информационная безопасность*" и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории "*информационная безопасность*" в ее первоначальном понимании.

Помимо Доктрины также важным основополагающим документом, в значительной мере определяющим политику государства в сфере информатизации и обеспечения защиты информации, можно считать Федеральную целевую программу "Электронная Россия", реализация которой планируется в три этапа в период с 2002 *по* 2010 год. В частности, одной из заявленных целей реализации данной Программы является обеспечение реализации прав на "обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах". В целом предполагается, что весь комплекс мероприятий, предусмотренных Программой, должен обеспечить принципиально более высокий уровень надежности ключевых информационных потоков на государственном уровне.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- Федеральный Закон "О *государственной тайне*";
- Федеральный Закон "Об информации, информационных технологиях и о защите информации";
- Федеральный Закон "Об участии в международном информационном обмене".

Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является **Совет безопасности РФ**.

Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является **Федеральная служба по техническому и экспортному контролю – ФСТЭК**. Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также **Служба специальной связи и информации ("Спецсвязь России")**, с 2004 года входящая в состав Федеральной службы охраны. Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

- Министерство связи и массовых коммуникаций РФ;
- Министерство внутренних дел РФ.

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия *по* обеспечению защиты информации:

- ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);
- Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр "Атомзащитаинформ");
- Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации)
- и некоторые другие.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, **информационной,** экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ, осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия *по* информационной безопасности. Функциями Управления информационной безопасности являются:

- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних *угроз информационной безопасности* и подготовка предложений Совету Безопасности по их предотвращению;
- рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;
- участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;
- подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ. [14]

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как **Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия РФ)**, была создана в январе 1992 года на базе Гостехкомиссии СССР *по* противодействию иностранным технологическим разведкам, которая, в свою *очередь* ведет отсчет своего существования с декабря 1973 года. Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и других.

Основными функциями ФСТЭК являются:

- проведение единой технической политики и координация работ по защите информации;
- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими

средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;

- поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций *по* лицензированию в составе ФСТЭК функционируют 7 региональных управлений (*по* федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь России), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

При этом задачами Спецсвязи также являются:

- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи России;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;
- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих *государственную тайну*;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи России;
- выполнение требований обеспечения информационной безопасности объектов государственной охраны.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды *работ* в сфере информационной безопасности:

- подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;
- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;
- выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Уполномоченным органом *по* ведению реестра доверенных удостоверяющих центров является ФГУП НИИ "Восход".

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти *по* защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ. [15]

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является **Комитет по безопасности Государственной думы Федерального собрания Российской Федерации**. В составе этого Комитета функционирует **Подкомитет по информационной безопасности**. В законодательной работе в рамках этого Комитета принимают участие:

- специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и других ведомств;
- руководители Совета безопасности РФ и других правительственных органов;
- представители общественных организаций, фондов и профессиональных объединений;
- представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);
- представители ведущих научно-исследовательских учреждений и учебных заведений.

2.Менеджмент и аудит информационной безопасности на уровне предприятия

Предпосылки развития менеджмента в сфере информационной безопасности на уровне предприятий.

Обеспечение собственной информационной безопасности на предприятиях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению информационной безопасности становится тем более высокой, чем выше степень автоматизации бизнес-процессов предприятия и чем больше "интеллектуальная составляющая" в его конечном продукте, т.е. чем в большей степени успешность деятельности зависит от наличия и сохранения определенной информации, обеспечения ее конфиденциальности и доступности для владельцев и пользователей.

Так же, как и на государственном уровне, управление информационной безопасностью на уровне предприятий направлено на нейтрализацию различных видов угроз:

- внешних, таких как неправомерные действия государственных органов, противоправная деятельность преступников и преступных группировок, незаконные действия компаний- конкурентов и других хозяйствующих субъектов, недобросовестные действия компаний-партнеров, несоответствие действующей нормативно-правовой базы фактическому развитию технологий и общественных отношений, сбои и нарушения в работе глобальных информационных и телекоммуникационных систем и информационных систем компаний-партнеров и др.;

- внутренних, таких как ошибки и халатность персонала предприятия, а также намеренно допускаемые нарушения, сбои и нарушения в работе собственных информационных систем и др.

Таким образом, управление информационной безопасностью на каждом отдельном предприятии должно осуществляться в контексте его общей хозяйственной деятельности: с учетом характера деятельности компании, а также фактически складывающейся ситуации в рыночной конкурентной борьбе, государственной политике, развития правовой и правоохранительной системы, уровня развития отдельных используемых информационных и телекоммуникационных технологий и других факторов, формирующих общие условия текущей деятельности.

Кроме того, необходимость разработки и внедрения политики информационной безопасности может быть обусловлена такими обстоятельствами, как:

- необходимость уменьшения стоимости страхования информационных рисков или определенных бизнес-рисков;

необходимость внедрения международных стандартов, таких как *ISO 17799* или BS 7799.

-

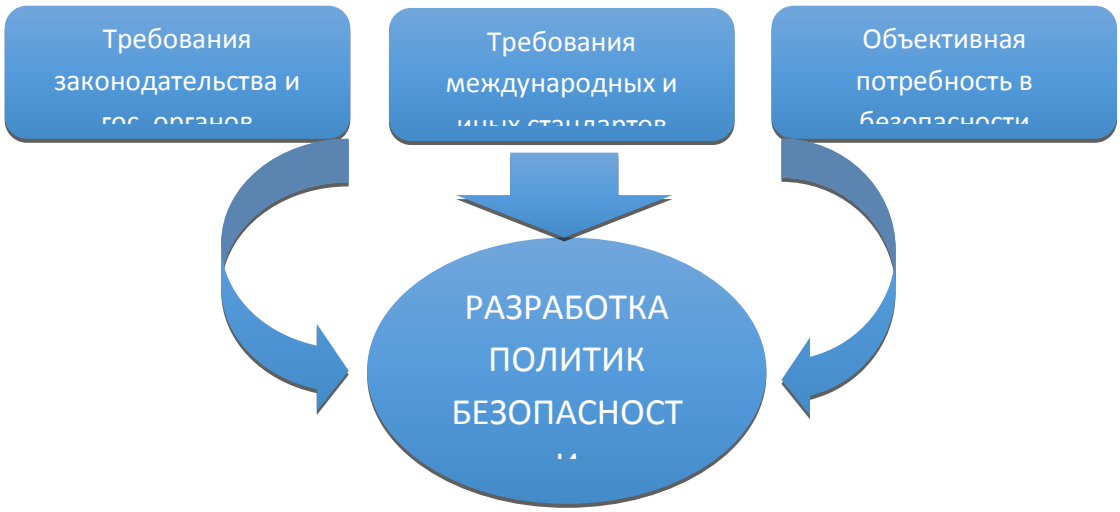


Рис. 14. Предпосылки разработки политики безопасности предприятия.

Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия.

Для нейтрализации существующих угроз и обеспечения информационной безопасности предприятия организуют систему менеджмента в сфере информационной безопасности, в рамках которой (системы) проводят работу по нескольким направлениям:

- формирование и практическая реализация комплексной многоуровневой политики информационной безопасности предприятия и системы внутренних требований, норм и правил;
- организация департамента (службы, отдела) информационной безопасности;
- разработка системы мер и действий на случай возникновения непредвиденных ситуаций ("Управление инцидентами");
- проведение аудитов (комплексных проверок) состояния информационной безопасности на предприятии.[24]

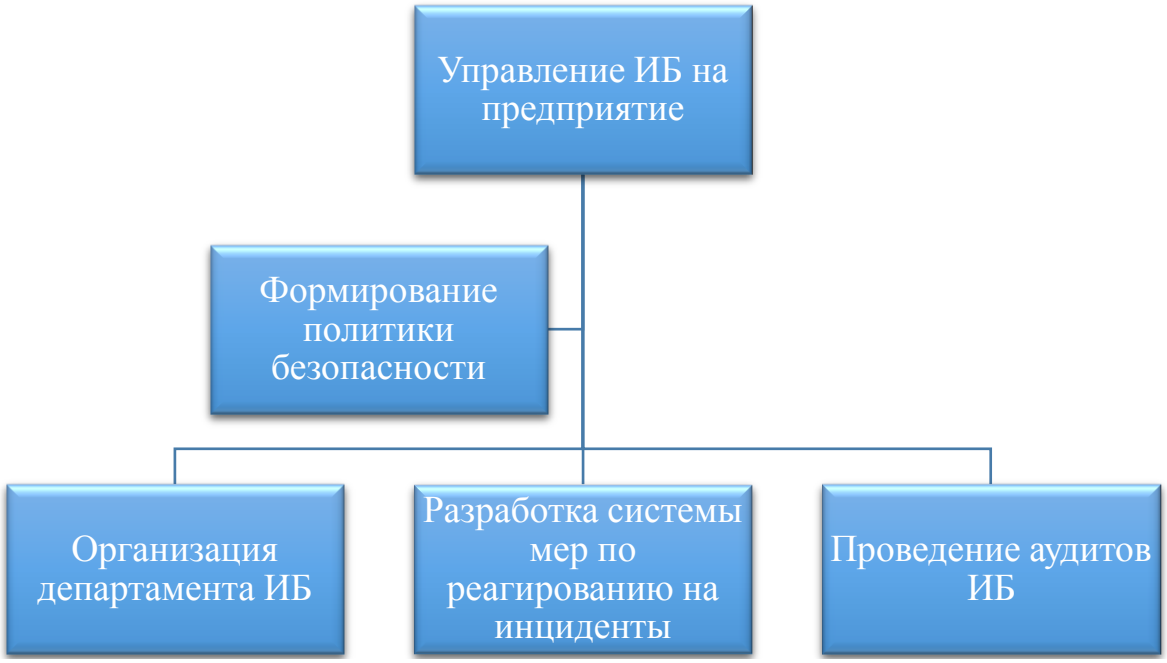


Рис. 15. Структура организационной деятельности в сфере информационной безопасности.

Каждое из этих направлений организационной работы имеет свои особенности и должно реализовываться с использованием специфических методов менеджмента и в соответствии со своими правилами. Политики и правила информационной безопасности являются организационными документами, регулирующим деятельность всей организации или отдельных подразделений (категорий сотрудников) в части обращения с информационными системами и информационными потоками. Департамент информационной безопасности является узко специализированным подразделением, решающим специфические вопросы защиты информации. Система мер по реагированию на инциденты обеспечивает готовность всей организации (включая Департамент информационной безопасности) к осмысленным целенаправленным действиям в случае каких-либо происшествий, связанных с информационной безопасностью. Проведение внутренних аудитов информационной безопасности (периодических или связанных с определенными событиями) должно обеспечить контроль за текущим состоянием системы мер по защите информации и, в частности, независимую проверку соответствия реального положения дел установленным правилам и требованиям.

При этом каждое из направлений деятельности должно постоянно совершенствоваться по мере развития организации, а конкретные задачи должны постоянно уточняться в соответствии с изменением в организационной структуре, производственных процессах или внешней среде.

Формирование политики информационной безопасности на предприятии.

Структура политики информационной безопасности и процесс ее разработки.

Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно условно выделить три ее основных уровня: верхний, средний и нижний.

Верхний уровень политики информационной безопасности предприятия служит:

- для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области; основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы;
- средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.[14]

Политики информационной безопасности среднего уровня определяют отношение предприятия (руководства предприятия) к определенным аспектам его деятельности и функционирования информационных систем:

- отношение и требования (более детально по сравнению с политикой верхнего уровня) предприятия к отдельным информационным потокам и информационным системам, обслуживающим различные сферы деятельности, степень их важности и конфиденциальности, а также требования к надежности (например, в отношении финансовой информации, а также информационных систем и персонала, которые относятся к ней);
- отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем;
- отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации, от которых напрямую зависит эффективность многих процессов и защищенность информационных ресурсов, а также основные направления и методы воздействия на персонал с целью повышения информационной безопасности.[23]

Политики безопасности на самом низком уровне относятся к отдельным элементам информационных систем и участкам обработки и хранения информации и описывают конкретные процедуры и документы, связанные с обеспечением информационной безопасности.

Разработка политики безопасности предполагает осуществление ряда предварительных шагов:

- оценку личного (субъективного) отношения к рискам предприятия его собственников и менеджеров, ответственных за функционирование и результативность работы предприятия в целом или отдельные направления его деятельности;
- анализ потенциально уязвимых информационных объектов;
- выявление угроз для значимых информационных объектов (сведений, информационных систем, процессов обработки информации) и оценку соответствующих рисков.

При разработке политик безопасности всех уровней необходимо придерживаться следующих основных правил.

Политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов.

Текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.

Текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован.

В целом политика информационной безопасности должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении информационного обмена и выполнении операций по обработке информации. Важной функцией политики безопасности является четкое разграничение ответственностей в процедурах информационного обмена: все заинтересованные лица должны ясно осознавать границы как своей ответственности, так и ответственности других участников соответствующих процедур и процессов. Также одной из задач политики безопасности является защита не только информации и информационных систем, но и защита самих пользователей (сотрудников предприятия и его клиентов и контрагентов).

Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов.

1. Проведение предварительного исследования состояния информационной безопасности.
2. Собственно разработку политики безопасности.
3. Внедрение разработанных политик безопасности.
4. Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (возврат к первому этапу, на новый цикл совершенствования).

Этот цикл может повторяться несколько раз с целью совершенствования организационных мер в сфере защиты информации и устранения выявляемых недоработок.

Организация внутриобъектового режима и охраны помещений и территорий является частью общей работы предприятия по обеспечению сохранности имущества и непрерывности текущей деятельности. Основной задачей обеспечения внутриобъектового режима является недопущение посторонних лиц к информационным активам и предотвращение угроз информационной безопасности.

Основой внутриобъектового режима является пропускной режим, в рамках которого, как правило, устанавливаются:

- документы, дающие право прохода на территорию предприятия — как пропуска и карты доступа, выданные самим предприятием, так и документы, выданные сторонними организациями;
- категории пропусков, используемых на предприятии, в соответствии с которыми (категориями) ограничивается срок действия пропусков, время возможного прохода на территорию предприятия (дни недели, часы суток) и некоторые другие параметры;
- порядок выдачи, обмена, продления и изъятия пропусков, а также порядок действий сотрудников и должностных лиц при утрате пропуска;
- порядок организации пропуска лиц, автотранспорта и проноса (провоза) имущества: размещение и порядок работы контрольно-пропускных пунктов, возможность пропуска тех или иных лиц, средств автотранспорта и грузов через те или иные КПП и др.;
- основные положения документооборота, используемого при проходе посетителей на территорию предприятия — требования к ведению Журнала регистрации

прохода посетителей, требования к документам, на основе которых выдаются разовые пропуска, порядок выдачи разовых пропусков и т.п.;

- порядок досмотра транспортных средств, допускаемых на территорию предприятия.

Кроме того, в рамках организации внутриобъектового режима может быть предусмотрено разделение помещений и территорий на отдельные зоны с ограничением доступа (в том числе на основе разделения помещений и территорий на различные категории), а также разграничение доступа отдельных сотрудников (категорий персонала) и посетителей в различные зоны; также могут быть определены основные требования к техническим средствам разграничения доступа и организации их использования.

В основе **средств контроля доступа** лежат механизмы опознавания личности и сравнения с установленными параметрами. Политика предприятия может устанавливать как упрощенные подходы к опознаванию, так и использование автоматизированных средств.

Физическая защита объектов, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений.

С физической защитой непосредственно связано использование средств **сигнализации и видеонаблюдения.** В зависимости от характера охраняемого объекта в средствах сигнализации могут применяться датчики, работающие на различных физических принципах, имеющие различные настройки и использующие различные каналы связи. В отличие от средств сигнализации средства видеонаблюдения позволяют не только установить факт нарушения, но и в деталях отслеживать его, контролировать ситуацию, а также вести видеозапись, которую можно будет использовать для принятия дальнейших мер (поиск нарушителей, уголовное преследование и т.п.) [18].

Отдельной задачей является обеспечение **информационной безопасности при процессе транспортировки** носителей информации и других объектов, требующее использования как специальных организационных приемов, так и специальных технических средств. К организационным методам относится привлечение специально подготовленных курьеров, а также разделение носителей информации (объектов) на части и их раздельная транспортировка с целью минимизации возможностей утечки информации. К техническим средствам, применяемым при транспортировке объектов, относятся защищенные контейнеры, специальные упаковочные материалы, а также тонкопленочные материалы и голографические метки, позволяющие идентифицировать подлинность объектов и контролировать несанкционированный доступ к ним.

Организация режима секретности в учреждениях и на предприятиях в РФ основывается на требованиях федерального законодательства, касающегося вопросов государственной тайны, и соответствующих подзаконных актов. Отнесение конкретной информации к государственной тайне производится решением специально назначаемых должностных лиц, а общий Перечень сведений, отнесенных к государственной тайне, утверждается Президентом РФ и подлежит обязательному опубликованию. Для сведений, составляющих государственную тайну, устанавливаются три степени секретности: «особой важности», «совершенно секретно» и «секретно», а носители таких сведений (документы) должны иметь соответствующие реквизиты.

Основным элементом организации режима секретности является допуск должностных лиц и граждан к сведениям, составляющим государственную тайну. Он предполагает выполнение руководством предприятия и подразделений по защите

государственной тайны (во взаимодействии с уполномоченными правоохранительными органами) следующих основных мероприятий.

- Ознакомление должностных лиц и граждан с нормами законодательства, предусматривающими ответственность за нарушение требований.
- Получение согласия на временные ограничения их прав в соответствии с законодательством.
- Получение согласия на проведение в отношении их проверочных мероприятий.
- Принятие решения о допуске к сведениям, составляющим государственную тайну.
- Заключение с лицами, получившими допуск, трудового договора (контракта), отражающего взаимные обязательства таких лиц и администрации предприятия (в т.ч. обязательства таких лиц перед государством по нераспространению доверенных им сведений, составляющих государственную тайну).[27]

Также важным элементом обеспечения режима секретности является организация **передачи сведений, составляющих государственную тайну, другим государствам**. В каждом отдельном случае решение о передаче сведений выносится Правительством РФ на основании экспертного заключения Межведомственной комиссии по защите государственной тайны, которая, в свою очередь, руководствуется мотивированным ходатайством предприятия, заинтересованного в передаче секретных сведений, и решением органа государственной власти, курирующего круг вопросов, к которому относятся передаваемые сведения.[33].

Политика опубликования материалов в открытых источниках должна обеспечивать предотвращение случайных и организованных утечек конфиденциальной информации при взаимодействии предприятия со средствами массовой информации, общественными и государственными органами, научным, академическим и бизнес-сообществом. Для того чтобы избежать ущерба интересам предприятия, такая политика должна содержать основные правила и процедуры подготовки информационных материалов к открытому опубликованию.

Политика управления паролями (или, в более общем виде, политика идентификации и аутентификации) может определять периодичность замены паролей, действия, которые необходимо осуществить при компрометации паролей, основные требования к их качеству, процедурам их генерации, распределению основных обязанностей, связанных с генерацией паролей, их сменой и доведением до пользователей, а также основные меры ответственности за нарушение установленных правил и требований.

Политика установки и обновления версий программного обеспечения может включать в себя некоторые ограничения на самостоятельное приобретение и установку программного обеспечения отдельными подразделениями и пользователями, а также определенные требования к квалификации специалистов, осуществляющих их установку, настройку и поддержку.

Политика приобретения информационных систем и их элементов (программных и аппаратных средств) может включать в себя требования к лицензированию и сертификации используемых программного обеспечения и оборудования, а также определенные требования к фирмам, осуществляющим их поставку и внедрение.

Политика доступа сторонних пользователей (организаций) в информационные системы предприятия может содержать перечень основных ситуаций, когда такой доступ возможен, а также основные критерии и процедуры, в соответствии с которыми осуществляется доступ.

Политика в отношении разработки ПО может содержать требования как к вопросам безопасности и надежности программных средств, самостоятельно разрабатываемых предприятием, так и в отношении передачи разработки программных средств (модулей информационных систем, отдельных программных библиотек и т.п.) сторонним специализированным организациям (т.н. «аутсорсинг»), а также в отношении приобретения и использования тиражируемых программных библиотек (модулей), распространяемых компаниями-производителями.

Политики использования отдельных универсальных информационных технологий в масштабе всего предприятия могут включать в себя:

- Политика использования электронной почты может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.

- Политика использования коммуникационных средств может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами.

- Политика использования мобильных аппаратных средств может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.). Она может отражать общее отношение предприятия к использованию сотрудниками таких устройств, определять требования и устанавливать конкретные области, в которых их использование допустимо. Также могут устанавливаться дополнительные общие требования к стационарному оборудованию в целях ограничения подключения к ним мобильных компьютеров и средств переноса данных.

- Политика информационной безопасности предприятия: нижний уровень. Данный уровень включает в себя документы, являющиеся инструкциями и методиками прямого действия, используемыми в повседневной деятельности сотрудников предприятия. Процедурные документы, относящиеся к предоставлению доступа к ресурсам (таким как сеть Интернет, корпоративные информационные системы и базы данных, аппаратные средства, средства передачи информации и т.п.) могут включать как типовые бланки заявок на предоставление доступа, так и описание основных процедур (регламента) принятия решений о предоставлении такого доступа и предоставлении конкретных прав при работе с информационными ресурсами, а также перечни критериев, необходимых для предоставления тех или иных прав в информационных системах.

Процедуры работы с отдельными информационными системами и/или модулями информационных систем могут перечислять все основные требования, правила и ограничения. Требования и правила, связанные с обеспечением информационной безопасности, могут быть как включены в общие инструкции по использованию информационных систем или регламенты осуществления бизнес процессов, так и оформлены в виде специальных инструкций и памяток, содержащих исключительно требования и правила информационной безопасности.

Должностные обязанности персонала предприятия, связанные с обеспечением информационной безопасности, должны входить как составная часть в должностные инструкции для каждого сотрудника. Кроме того, политика безопасности может предусматривать подписание (как при поступлении на работу или переводе на определенную должность, так и при увольнении с нее) отдельными категориями персонала дополнительных соглашений, обязательств и подписок о неразглашении определенной информации. Также политика безопасности может вводить дополнительные требования к персоналу, работающему с определенными сведениями или информационными системами.

Политики безопасности, относящиеся к работе с внешними контрагентами, могут предусматривать типовые формы и отдельные инструкции по составлению коммерческих контрактов (для каждого типа контрактов, а также для отдельных групп контрагентов) и обмену информацией с поставщиками, покупателями, консультантами, посредниками, субподрядчиками, поставщиками финансовых и информационных услуг и другими участниками хозяйственной деятельности. В частности, в политике для каждой из этих категорий может предусматриваться специфический порядок информационного обмена, взаимные требования по обеспечению конфиденциальности и возможные меры ответственности в случае нарушения согласованных требований какой-либо из сторон.

3. Аудит информационной безопасности автоматизированных банковских систем

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 [57].

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.

Дистанционное банковское обслуживание

Виды дистанционного банковского обслуживания с точки зрения оказания различных услуг:

- интернет-банкинг - оказание услуг ДБО на основе банковской системы платежей через Интернет; при котором пользователю предоставляется доступ к счетам и операциям через Интернет

- мобильный банкинг - оказание услуг ДБО на основе мобильных технологий; (смс оповещение)

- внешние сервисы - киоски, банкоматы.

- телефонный банкинг - оказание услуг ДБО на основе банковской системы голосовых сообщений;

- классический «Банк-Клиент».

Интернет-банкинг чаще всего используется через систему банк-клиент. (Например:Сбербанк-онлайн, Альфа-клик).

Услуги Интернет-банкинга:

- Посмотреть остатки по счетам, кредитам, депозитам и пластиковым картам
- Заявки на открытие депозитов, получение кредитов, банковских карт и т. д.
- Внутренние переводы на счета банка
- Переводы на счета в других банках
- Конвертация средств (перевод из одной валюты в другую)
- Оплатить услуги оператора сотовой связи, интернет-провайдера или коммерческого ТВ, коммунальные услуги, междугороднюю связь.
- Угрозы автоматизированным банковским системам или
- Через проникновения на компьютер троянских программ, которые похищают файлы с ключами, а так же могут отслеживать нажатие клавиш на клавиатуре компьютера для получения логина и пароля (кейлоггер).
- Фишинг, когда мошенники узнают конфиденциальную информацию о пользователе, например, с помощью подложных писем из банка с запросом данных или

ссылками на сайты имитирующие сайты банков

- Кроме того, мошенники могут перевыпустить сим-карту по подложным доверенностям, для того чтобы получить доступ к одноразовым кодам.

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.

DataproInformationServicesGroup 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 в основном 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.

Классические угрозы безопасности информации в АБС – это вывод системы из строя, отказ в обслуживании и компрометация или подмена данных. И эти угрозы слишком реальны.

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.

Нормативные аспекты обеспечения информационной безопасности автоматизированных банковских систем включает ряд документов (см. Тема 5).

Защита информации определена ФЗ №149 от 07.2006 г. «Об информации, информационных технологиях и защите информации». Так же вопрос информационной безопасности затрагивается в Положение банка России №242-п 16.12.2003 г. Международный стандарт информационной безопасности ISOи 17799. Стандарт содержит практические правила по управлению информационной безопасностью банка и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Аудит информационной безопасности банка ISO 17799 включает в себя десять основных разделов:

1. Политика безопасности.

2. Организационные меры по обеспечению безопасности.

о Распределение ответственности за обеспечение безопасности.

3. Классификация и управление ресурсами.

4. Безопасность персонала.

о Тренинги персонала по вопросам безопасности.

о Реагирование на секьюрити инциденты и неисправности.

5. Физическая безопасность.

о Рабочие процедуры и ответственность.

о Защита от злонамеренного программного обеспечения.

o Управление внутренними ресурсами.

o Управление сетями.

6.Безопасность носителей данных.

7. Контроль доступа.

o Бизнес требования для контроля доступа.

o Управление доступом пользователя.

o Ответственность пользователей.

o Контроль и управление удаленного (сетевого) доступа.

o Контроль и управление доступом к приложениям.

o Мобильные пользователи.

8. Криптография.

o Безопасность системных файлов.

9. Управление непрерывностью бизнеса.

o Непрерывность бизнеса и анализ воздействий.

o Создание и внедрение плана непрерывного ведения бизнеса.

10. Соответствие системы основным требованиям.

o Соответствие требованиям законодательства.

o Анализ соответствия политики безопасности.

o Анализ соответствия техническим требованиям.

К недостаткам стандарта можно отнести поверхностное освещение материала, который позволяет только обозначить области информационной безопасности, не конкретизируя их.

Важным Федеральным законом, определяющим защиту электронных платежей является,ФЗ «Об электронной подписи» (с изменениями на 23 июня 2016 года) Принят Государственной Думой 25 марта 2011 года, Одобрен Советом Федерации 30 марта 2011 года. (Тема5).

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.

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 в АБС.

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) сотрудников, время и дата входа (выхода) субъекта доступа в систему (из системы) или загрузки (остановки) 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;
- учет конфиденциальных документов проводится 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 компьютере 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).

- Применение специальных программ-анализаторов, осуществляющих постоянный контроль возникновения отклонений в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (например, обнаружение нарушений целостности программного обеспечения), а также входной контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований).

Защита от несанкционированного копирования и распространения программ 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.

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, BarclaysBank тратит на защиту своей автоматизированной системы около $ 20 млн. ежегодно.

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.

Обеспечение безопасности в системе интернет-банкинга:

- Авторизация пароль-логин. Постоянный логин выдается банком. Пароль может меняться для осуществления мер безопасности.
- Система одноразовых паролей или (переменных кодов) может использоваться как для подтверждения входа в систему, так и для подтверждения каждой операции. (оплаты или перевода)(пароль приходит на мобильный телефон, либо через банкомат когда он выдаст около 20 разных паролей).
- **Виртуальная** клавиатура аналог обычной клавиатуры только ввод осуществляется без нажатия клавиш на клавиатуре используетсядля ввода (одноразовых) паролей.
- Электронная цифровая подпись и шифрование. По аналогии с подписанием бумажных документов существует механизм заверения электронных документов, позволяющий идентифицировать владельца, а также установить отсутствие искажения информации в документе. Формируется ЭЦП с помощью закрытого ключа, который

может хранится в файле у пользователя на компьютере, на внешнем носителе (USB-flash) или генерироваться специальными устройствами (электронными ключами/токенами). С помощью закрытого ключа также производится шифрование пересылаемой информации. Использование цифровой подписи в некоторых банках позволяет увеличить лимиты на проведение денежных операций, т.к. электронная цифровая подпись имеет юридическую силу.

- **Виртуальная карта для совершения оплаты в интернет**
- **Разграничение доступа к счетам.** Некоторые банки позволяют видеть в интернет-банкинге не все счета, а только заранее оговоренные с пользователем.
- **Лимиты на операции.** При отсутствии электронной цифровой подписи банки устанавливают лимиты на некоторые операции, например переводы и платежи третьи лицам.
- Подключение к системе ни в коем случае не должно проходить по незащищенному протоколу.
- **Пароль** к системе **должен удовлетворять** следующим **требованиям**: не содержать повторяющиеся или идущие подряд цифры или буквы (например,111111 или qwerty); не содержать дат рождения, имен и фамилий родственников; быть известным только клиенту интернет-банкинга; периодически изменяться
- Переменные коды, закрытые ключи, логин и **пароли должны храниться в недоступном для посторонних месте.**
- Компьютер для входа в систему интернет-банкинга: должен быть защищен антивирусными программами с регулярно обновляемыми антивирусными базами; к нему должен быть ограничен доступ посторонних лиц, в том числе не рекомендуется выходить в интернет-банкинг с рабочего компьютера и из интернет-кафе.
- При соединении с системой интернет-банкинга нужно проверять **сертификат соответствия.** Это необходимо для обеспечения защиты от фишинга (проверка сертификата позволит определить оригинальный сайт или поддельный). Для того чтобы проверить сертификат соответствия при входе на стартовую страницу системы интернет-банкинга кликните на замок в нижней полоске экрана и посмотрите кому выдан сертификат и совпадает ли он с владельцем ресурса (банком).
- Если страница авторизации при входе в систему онлайн-банкинга изменилась или запрашиваются дополнительные конфиденциальные сведени, — это является вероятным признаком, что вы на фишинговой странице. С нее нужно уйти и проинформировать об этом случае банк.

- Нельзя переходить по ссылкам, указанным в подозрительных письмах и открывать прикрепленные к ним файлы.
- Нельзя отвечать на подозрительные электронные письма, которые запрашивают конфиденциальную информацию, т.к. банки никогда не рассылают письма с подобными просьбами.
- Если система онлайн-банкинга «привязана» к мобильному телефону, нужно обратиться к вашему оператору с требованием – не проводить без вашего личного присутствия никаких операций по замене сим-карты. В этом случае, перевыпуск сим-карты по доверенности будет невозможен.

4. Менеджмент информационной безопасности электронной коммерции

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 (businesstobusiness, B2B);

* торговля между предприятиями и физическими лицами, т.е. потребителями (businesstoconsumer, 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.

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, MASTERCARD 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 составляет более 2 трлн. долл. Но именно низкая защищенность системы электронной коммерции является сдерживающим фактором дальнейшего развития электронного бизнеса.

Решение проблемы обеспечения информационной безопасности электронной коммерции в первую очередь связано с решением вопросов защиты информационных технологий, применяемых в ней.

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 [57]:

- 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 – InternetSecurityTaskForce (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 и др.

Контрольные вопросы к теме 6

1. Охарактеризуйте основные потери банков от реализации информационных угроз.
2. Назовите основные виды дистанционного банковского обслуживания.
3. Что такое интернет-банкинг?
4. Дайте характеристику мобильного банка.
5. Какие услуги оказывает коммерческий банк через телефонный банкинг?
6. Назовите основные нормативные документы, определяющие информационную безопасность банка.
7. Что такое фишинг?
8. Для чего используется электронная цифровая подпись в системе электронных платежей?
9. Назовите особенности электронной коммерции.
10. В чем отличия электронного магазина от электронного каталога?
11. Какие выгоды приносит Интернет в сфере электронной коммерции?
12. Какие способы доставки и оплаты товара в ЭК?
13. В чем состоит проблема информационной безопасности ЭК?
14. Назовите основные угрозы ЭК.
15. Что включает комплексная система ИБ ЭК?

Тесты к теме 6

1. Безопасность информации банков влияет на уровень их рентабельности:

А. Да;

Б. Нет;

В. Иногда.

2. Интернет-банкинг это

А. оказание услуг на основе банковской системы платежей через Интернет;

Б. внешние сервисы через банкоматы;

В. банковская система голосовых сообщений через телефон.

3. Фишинг – это

А. разглашение открытой в СМИ информации;

Б. воровство конфиденциальной информации о пользователе, в частности, с помощью подложных писем из банка.

В. система «Банк-Клиент».

4. Какие нарушения преобладают в банках

А. внутренние;

Б. внешние;

В. нет ни тех, ни других.

5. К нормативно-правовым документам по ИБ банка НЕ относится:

А.СтандартISO 17799;

Б. ФЗ «об электронной подписи»;

В. Налоговый кодекс.

6. Чем выше уровень защиты банка, тем

А она дороже;

Б. она дешевле;

В. без разницы.

7. На подозрительные электронные письма, которые запрашивают конфиденциальную информацию:

А. надо ответить незамедлительно;

Б. проигнорировать;

В. переслать другому.

8.Электронная коммерция – это предпринимательская деятельность по продаже товаров через Интернет?

А. Да

Б. Нет

В. отчасти.

9.Электронный магазин – это

А. виртуальное сообщество;

Б. электронная витрина и торговые системы;

В. электронный аукцион.

10.Доминирующее положение в ЭК стал сектор

А. Business to business, B2B

Б. Business to consumer, B2C

В. Business to organization, B2O

11.Информационные угрозы ЭК это

А. Проникновение в систему извне;

Б. Взлом программно-аппаратной защиты;

В. Все вышеперечисленное.

12.Создание ложных заказов в ЭК

А. Опасно;

Б. Не опасно;

В. Не влияет на работу электронного магазина.

7. Учебно-методическое обеспечение самостоятельной работы обучающихся

Рекомендации студентам

Для лучшего усвоения положений дисциплины студенты должны:

- постоянно и систематически, с использованием рекомендованной литературы и электронных источников информации, закреплять знания, полученные на лекциях;
- находить решения проблемных вопросов, поставленных преподавателем в ходе лекций и практических заданий;
- регулярно и своевременно изучать материал, выданный преподавателем на самостоятельную проработку;
- с использованием средств информационных систем, комплексов и технологий, электронных учебников и практикумов, справочных правовых и тренинго-тестирующих систем, информационных ресурсов сети Интернет выполнить на компьютере тематические практические задания, предназначенные для самостоятельной работы;
- находить, используя разные источники информации, ответы на теоретические и практические контрольные вопросы по темам дисциплины;
- использовать информацию, найденную на сайтах фирм–разработчиков информационных систем и технологий, применяемых в экономике;
- при подготовке к экзамену учитывать общие требования и рекомендации.

При освоении данного курса бакалаврам может быть предложено выполнение инициативной научно-исследовательской работы.

Методические указания по выполнению научно-исследовательской работы

Целью выполнения работы является:

– закрепление знаний, полученных студентами в процессе теоретического обучения;

– проведение исследования проблемы;

– активное использование пакетов прикладных программ; анализ библиографических материалов.

– отработка приемов и способов аналитических расчетов на практическом материале.

Выбор темы производится студентом и утверждается преподавателем. Рекомендуемый объем работы 10-15 страниц машинописного текста.

В каждой работе, кроме основных разделов, независимо от темы, предусматривается «Введение», «Заключение», «Список используемой литературы», «Приложения».

Список литературы должен быть составлен в соответствии с библиографическими требованиями.

Выполнять научно-исследовательскую работу необходимо с использованием текстового редактора MS Word, электронных таблиц Excel, а также можно использовать пакеты прикладных программ (ППП).

К оформлению научно-исследовательской работы предъявляются общие типовые требования.

Рекомендуемые направления научно-исследовательских работ

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

6 Информационная безопасность **(**по материалам зарубежных источников и литературы).

7 Правовые основы защиты конфиденциальной информации.

8 Экономические основы защиты конфиденциальной информации.

9 Организационные основы защиты конфиденциальной информации.

10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

11 Составление инструкции по обработке и хранению конфиденциальных документов.

12 Направления и методы защиты документов на бумажных носителях.

13 Направления и методы защиты машиночитаемых документов.

14 Архивное хранение конфиденциальных документов.

15 Направления и методы защиты аудио- и визуальных документов.

16 Порядок подбора персонала для работы с конфиденциальной информацией.

17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

18 Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

19 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

20 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

21 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

22 Порядок защиты информации в рекламной и выставочной деятельности.

23 Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

24 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

25 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

26 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

27 Назначение, виды, структура и технология функционирования системы защиты информации.

28 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

29 Аналитическая работа по выявлению каналов утечки информации фирмы.

30 Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

31 Направления и методы защиты профессиональной тайны.

32 Направления и методы защиты служебной тайны.

33 Направления и методы защиты персональных данных о гражданах.

34 Методы защиты личной и семейной тайны.

35 Построение и функционирование защищенного документооборота.

36 Защита секретов в дореволюционной России.

37 Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Перечень вопросов к экзамену

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.

22. Деятельность международных организаций в сфере информационной безопасности.

23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.

24. Доктрина информационной безопасности России.

25. Уголовно-правовой контроль над компьютерной преступностью в России.

26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.

28. Фрагментарный и системный подход к защите информации.

29. Методы и средства защиты информации.

30. Организационное обеспечение ИБ.

31. Организация конфиденциального делопроизводства.

32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.

33. Инженерно-техническое обеспечение компьютерной безопасности.

34. Организационно-правовой статус службы безопасности.

35. Защита информации в Интернете.

36. Электронная почта и ее защита.

37. Защита от компьютерных вирусов.

38. «Больные» мобильники и их «лечение».

39. Популярные антивирусные программы и их классификация.

40. Организация системы защиты информации экономических объектов.

41. Криптографические методы защиты информации.

42. Этапы построения системы защиты информации.

43. Оценка эффективности инвестиций в информационную безопасность.

44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.

45. Управление информационной безопасности на государственном уровне.

46. Аудит ИБ автоматизированных банковских систем.

47. Электронная коммерция и ее защита.

48. Менеджмент и аудит информационной безопасности на уровне предприятия.

49. Информационная безопасность предпринимательской деятельности.

50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

Список используемых источников

Основная литература

1. Конституция РФ (http://constitutionrf.ru/);
2. Доктрина информационной безопасности Российской Федерации (утв. утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.) (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html);
3. Указ правительства РФ №188 об утверждении перечня сведений конфиденциального характера 1997г. (с изм. и доп. от 23 сентября 2005 г., 13 июля 2015 г.) (http://base.garant.ru/10200083/#ixzz4bCt8H6TU);
4. Трудовой кодекс РФ – глава 14 «Защита персональных данных работника» (от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (http://www.consultant.ru/document/cons_doc_LAW_34683/);
5. Гражданский кодекс Ч. №4 Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (18 декабря 2006 года N 230-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_64629/).
6. Федеральный Закон от 21 июля 1993г. №5485 «О государственной тайне» (Федеральный закон "О внесении изменений в статью 5 Закона Российской Федерации "О государственной тайне" от 15.11.2010 N 299-ФЗ (последняя редакция) (http://www.consultant.ru/document/cons_doc_LAW_106802/);
7. Федеральный закон от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне") (ред. от 12.03.14 г.) (http://yconsult.ru/zakony/zakon-rf-98-fz/);
8. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации» (http://base.garant.ru/12148555/);
9. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями вступивших в силу 01.03.17 г.) (http://kodeks.systecs.ru/zakon/fz-152/);
10. Федеральный закон от 06 апреля 2011 №63 «Об электронной подписи» (с изменениями на 23.06.16 г.) (http://docs.cntd.ru/document/902271495);
11. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. Журнал «Вопросы кибербезопасности», №5(8) – 2014.
12. Баскаков А. В., Остапенко А. Г., Щербаков В. Б. Политика информационной безопасности как основной документ организации // Информация и безопасность. – 2016. - №2. – С. 43-47.
13. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. – Режим доступа: http://znanium.com
14. Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.
15. Бондаренко Т.Г., Клочкова А.А. Развитие информационных технологий: необходимость усиления информационной безопасности банковского сектора. Журнал «Известия Тульского государственного университета. Экономические и юридические науки», №1-1, 2014.
16. Борисова К. В., Кудашкин Я. В. Международная информационная безопасность как основополагающий фактор национальной безопасности// Сборник научных трудов. Национальная безопасность: противодействие экстремизму и терроризму и перспективы преодоления глобальных проблем. – 2016. – С. 68-73.
17. Галушкин А. А. К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. – 2015. - №2. – С. 8.

18. Государственная тайна и её защита. Серия «Закон и право» М.: Ось-89, 2004 г.
19. Дойникова Е. В. Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности // Материалы конференции «Информационные технологии в управлении». – 2014. – С. 601-604.
20. Дорожкин А.В., Ясенев В.Н. Информационная безопасность как инструмент обеспечения экономической безопасности хозяйствующего субъекта. Журнал «Экономика и предпринимательство», № 5 (1), 2015.
21. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. Журнал «Вопросы кибербезопасности» №1 (2) – 2014.
22. Жукова М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб.пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2012. – Режим доступа: http://znanium.com
23. Защита конфиденциальной информации: учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – М.: ФОРУМ, 2009. - 256 с.: ил. - (Высшее образование).
24. Зегжда Д.П., Ивашко А.М.. Основы безопасности информационных систем. М., Горячая линия-Телеком, 2005.
25. Зефиров С. Л., Голованов В. Б. Система менеджмента информационной безопасности организации // Труды международного симпозиума «Надежность и качество». – 2016. – С. 364-366.
26. Информатика для юристов и экономистов/ Под. Ред. С.В. Симоновича.- СПб.: Питер, 2008.- 688 с.
27. Информационная безопасность гос.организаций. [Электронный ресурс]: http://library.tuit.uz/skanir_knigi/book/infor_bezop/infor_2.htm
28. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: http://znanium.com
29. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб. заведений. – М.: Издательский центр «Академия», 2005.
30. Камалова Г. Г. Вопросы ограничения доступа к информации в системе государственного управления// Вестник Удмуртского университета. – 2015. - №6. – С. 91-104.
31. Кирильчук С.П., Наливайченко Е.В. Обеспечение информационной безопасности предприятий. Международный научный журнал «Символ науки», № 3, 2015.
32. Крупко А. Э. Плитика информационной безопасности: состав, структура, аудит // ФЭС: Финансы. Экономика. Стратегия. – 2015. - №8. – С. 27-32.
33. Лопатин В.Н.. Правовые основы информационной безопасности. Курс лекций. М., МИФИ, 2000.
34. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для вузов.- М.: Академия, 2008.- 336 с.
35. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов ; Интернет-университет информационных технологий .— Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2010 .— 175 с. : ил .— (Основы информационных технологий) .— Библиогр.: с. 172-175 .
36. Нестеров А. В. Существует ли информационная безопасность? // Правовые вопросы связи. – 2017. - №1. – С. 32-35.

37. Одинцов А. А. Экономическая и информационная безопасность. – М.: Дело, 2014. – С. 91.
38. Организационное обеспечение информационной безопасности : учебник для вузов / О.А. Романов, С.А. Бабин, С.Г. Жданов .— М. : Академия, 2008 .— 190 с. : ил .— (Высшее профессиональное образование, Информационная безопасность) .— Библиогр.: с. 185 .— ISBN 978-5-7695-4272-5 : 236-50.
39. Основы безопасности бизнеса и предпринимательства / В. И. Ярочкин, Я. В. Бузанова. - М. : Академический проект : Фонд "Мир", 2005. - 205 с. - (Технологии безопасности). - ISBN 5-8291-0490-3. - ISBN 5-902357-21-7.
40. Пархоменко Н. Г. , Боташев Н. М. , Колбанов П. М., Григоренко Е. С. Выявление угроз информационной безопасности в реальном времени // Известия ЮФУ. Технические науки. – 2016. - №4. – С. 325-326.
41. Потресов, С. Средство от случайных связей. Бухгалтер и компьютер №9(24) 2001г.
42. Родина Ю. В. Информационная безопасность и риски информационной безопасности. Интерпретация понятий // Экономика и менеджмент: от теории к практике. – 2014. – С. 122-144.
43. Соляной В. М., Сухотерин А. И. Становление международных организаций в сфере информационной безопасности // Информационное противодействие угрозам терроризма. – 2015. - №25. – С. 255-260.
44. Талимончик В. П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Известия высших учебных заведений. Правоведение. – 2014. - №2. – С. 103-111.
45. Тарасов А. М. Информационная безопасность в ракурсе деятельности международных организаций // Вестник академии и права. – 2016. - №4. – С. 37-48.
46. Тенденции кибербезопасности в 2016 году [Электронный ресурс]: краткое руководство по наиболее важным выводам в области безопасности.- Электрон.дан.- М.: Корпорация Майкрософт, 2016.- Режим доступа: https:// www. microsoft. com/ ru-ru/ security/ default.aspx.
47. Тропин С. А. Экономическая безопасность России // Законодательство и экономика. 2004. № 5.
48. Управление кадровой безопасностью организации : учебник / А. Р. Алавердов. – М. : Маркет ДС, 2008. – 176 с. – (Университетская серия).
49. Формы утечки информации, составляющей коммерческую тайну, и управление персоналом предприятия в целях обеспечения информационной безопасности. [Электронный ресурс]: http://www.juristlib.ru/book_5770.html
50. Хаханов В.И.. Чумаченко С.В., Литвинова Е.И., Мищенко А.С. Развитие киберпространства и информационная безопасность. Журнал «Радіоелектроніка, інформатика, управління», № 1(28), 2013.
51. Цюк О. А. Международная организация по стандартизации // Мир науки, культуры и образования. – 2014. - №4. – С. 67-78.
52. Шерстюк В. П. Информационная безопасность в системе обеспечения безопасности России // Информационное общество. – 2015. - №6. – С. 3-5.
53. Юсупов Р. М., Шишкин В. М. Информационная безопасность, кибербезопасность и смежные понятия // Информационное противодействие угрозам терроризма – 2016. - №1. – С. 27-35.

Дополнительная литература

54. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. – Режим доступа: http://znanium.com
55. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. – Режим доступа: http://znanium.com
56. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с. – Режим доступа: http://znanium.com
57. Ясенев В.Н. Информационная безопасность экономических систем. Учебно-методическое пособие. - Н.Новгород: Нижегородский госуниверситет им. Н.И.Лобачевского, 2006.-373с.+вкл.

Рекомендуемые Интернет-ресурсы

1. www.cyberpol.ru Компьютерная преступность и способы борьбы.
2. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
3. www.itsec.ru Интернет-журнал «Информационная безопасность».
4. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд».
5. www.kaspersky.ru Лаборатория Касперского.
6. www.comss.ru.
7. www.drweb.com.
8. www.esethod32.ru.
9. www.kaspersky.ru.
10. http://free.avg.com
11. www.kaspersky.ru/removaltools
12. www.freedrweb.com/cureit/
13. www.computerologia.ru
14. www.free-av.com
15. www.mcafee.com
16. http://www.viruslab.ru/
17. www.bitdefender.com.