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 38.03.02
«Менеджмент»

Нижний Новгород
2018

УДК 311 (075.8)
ББК У051

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Матвеев В.А., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2018. – 182 с.

Рецензенты:
Зав. Кафедрой «Экономики и экономической безопасности»
Нижегородской правовой академии
Академик финансовой академии «Элита» проф., д.э.н. Чеботарев В.С.
Зав.кафедрой «Менеджмента и государственного управления» проф., д.э.н. Яшин С.Н.

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 направлению 38.03.02 «Менеджмент» в Институте экономики и предпринимательства ННГУ им. Н.И. Лобачевского.

Ответственный за выпуск:
председатель методической комиссии ИЭП ННГУ,
доц. Едемская С.В.

УДК 311 (075.8)
ББК У051

© Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2018

СОДЕРЖАНИЕ

Предисловие

Дисциплина «Информационная безопасность» относится к базовой части учебного плана 38.03.02 «Менеджмент», 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 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», «Экономика», «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 государственного и корпоративного управления.

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 в менеджменте

1.1.Основные понятия информационной безопасности управленческих систем.
1.2.Экономическая информация как товар и объект безопасности
Контрольные вопросы и тесты

1.1. Основные понятия информационной безопасности управленческих систем

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;
- информационное вбрасывание – современное дезинформационное воздействие для нанесения ущерба государственным структурам, неблаговидные дезинформационные воздействия на управленческие структуры компаний со стороны конкурентов, сбор и публикации негативной информации о деятельности руководящего персонала.

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.

1.2. 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.
7. Тайна усыновления.
8. 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

2.1. Понятие информационных угроз, их виды и способы воздействия на экономический объект
2.2 Понятие и виды компьютерных преступлений
2.3. Вредоносные программы для ПК и мобильных устройств
Контрольные вопросы и тесты

2.1. Понятие информационных угроз, их виды и способы воздействия на экономический объект

Современный этап развития человечества характеризуется существенным возрастанием рисков реализации угроз информационной безопасности, причинения прямого или косвенного ущерба интересам общества, личности или государства. Для организаций и конкретных граждан – это реальные или потенциально возможные риски нанесения ущерба деловой репутации, нарушения защищаемых информационных ресурсов (коммерческая тайна, ноу-хау и т.д.) и возникновения дополнительных затрат на их восстановление, причинения морального вреда, противозаконного использования персональных данных, невозможности выполнения взятых на себя обязательств перед третьей стороной и т.п., а для государства – это риски снижения эффективности проводимой политики, вовлечения в информационные войны, разглашения государственной тайны и т.д.

В 2014 Россия вступила в фазу крупномасштабной информационной войны со странами ЕС и США. Ряд информационных всплесков, как известно, был вызван событиями на Украине, сменой власти в Крыму, обвинениями в коррупции и т.п. Помимо чисто политических, имеется и ряд формальных причин, например, в сфере спорта. В результате взаимное противостояние переместилось в информационную плоскость.

Сфера использования информационного оружия – массовые сообщения в СМИ, по каналам спецслужб, в Internet и т.д. Соответствующая информация предоставляется в подавляющем большинстве случаев как бездоказательные факты, а тактикой информационных атак является многократное повторение желаемой установки, что требует применения адекватных мер со стороны российских властей.

Помимо удара по репутации государства, было нарушено международное взаимодействие, что привело к ухудшению инвестиционного климата, росту оттока капиталов, выход с российского рынка ряда иностранных компаний, в конечном счете снижению уровня жизни граждан. Информационные атаки нанесли существенный ущерб в особенности на финансовых рынках. Так, 25 апреля 2014 рейтинговое агентство Standard & Poor's понизило суверенный рейтинг России с «BBB-» до «BBB» с рейтингом «негативный», что вызвало девальвацию рубля, подавляющего большинства котировок российского рынка акций.

Таким образом, информационные атаки, которые проводятся в переломный момент времени, могут вызвать не только нарушение функционирования отдельных элементов, но и значительные системные разрушения.

Сформировалась тенденция к использованию современных информационных технологий организованными преступными группами и распространение их деятельности на межгосударственный уровень. Серьезное увеличение числа киберпреступлений в последнее время обусловливает необходимость систематического формирования единого концептуального подхода и соответствующией системы мер по обеспечению информационной безопасности, нормативно-правового регулирования, существенного увеличения расходов на создание и совершенствование систем защиты информации, контроля качества полученных результатов, формирования информационной культуры во всех секторах экономики, политической системы, а также социальной сферы.

Под угрозой информационной безопасности понимается случайное или преднамеренное явление, событие, действие или процесс, которые могут привести к искажению, несанкционированному использованию или к уничтожению информационных ресурсов информационной системы, используемых программных и технических средств (например, неправильные действия обслуживающего персонала, хакерские атаки, действие компьютерного вируса, несанкционированный доступ к служебной документации, подслушивание коммерческих переговоров и т.д.) (Рисунок 2).

Реализация угроз информационной безопасности заключается в частичном или полном нарушении работоспособности информационной системы, утрате ценности или частичном обесценивании информации в случае нарушения:

а) конфиденциальности (при хранении и распространении информации);

б) целостности (при изменении или уничтожении информации);

в) доступности информации (в случае неполучения или несвоевременного получения информации легальным пользователем).

Рис.2. Информационные угрозы и их виды

В наиболее общем виде можно выделить следующие основные виды негативного воздействия информационных угроз на объекты информационной безопасности:

- раскрытие и несанкционированное использование конфиденциальной информации;
- ошибочное использование информационных ресурсов – санкционированное использование, которое привело к разрушению, раскрытию или компрометации информационных ресурсов;
- компрометация информации – внесение несанкционированных изменений в базы данных, в результате чего возникает необходимость опровержения информации, отказа от нее, а также выявления изменений и восстановления истинных сведений;
- отказ от предоставляемой информации – нанесение ущерба вследствие непризнания получателем или отправителем информации фактов ее получения или отправки;
- отказ в предоставлении информации – задержка с предоставлением или непредставление информации или неполучение доступа к информационным системам.

Причинами реализации информационных угроз являются:

- недостаточное знание проблемы информационной безопасности конкретного объекта, несоблюдение правил защиты конфиденциальной информации;

- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими и иными мерами;
- неадекватность разработанной политики информационной безопасности состоянию информационной системы или некорректность ее реализации на практике, пренебрежение профилактикой информационных угроз;
- наличие уязвимых мест в системе защиты (ошибки в программном обеспечении, применение устаревшего программного обеспечения, отсутствие, непродуманный выбор или некорректная установка и настройка средств защиты, антивирусных программ, программ-сторожей компьютерных портов и т.д.);
- использование неаттестованных средств обработки конфиденциальной информации;
- недостаточное внедрение средств автоматизации при работе с информационными системами для устранения непреднамеренных информационных угроз.

Информационные угрозы по отношению к объекту информационной безопасности можно подразделить на две основные группы:

- внутренние, возникающие внутри этого объекта, вследствие воздействия человеческого фактора (например, по причине социальной напряженности внутри коллектива, неправомерных действий квалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, представителей службы защиты информации, вспомогательного персонала), ошибки и перебои в работе программно-аппаратных и вспомогательных технических средств (охраны, сигнализации, телефонии);
- внешние, связанные с информационным противоборством государств, личными противоправными мотивами отдельных лиц (конкурентов, недобросовестных партнеров, уволенных работников, мошенников, криминальных структур, потенциальных преступников, хакеров и т.д.), взаимодействием информационной системы предприятия через Internet со смежными информационными системами банков, страховых компаний, налоговых органов и т.д.

Непосредственным объектом воздействия информационной угрозы может выступать информационная система объекта в целом (неправомерное получение логина и пароля для авторизации в системе, внедрение вируса, нарушающего работоспособность системы и т.д.), ее составные элементы (воздействие на программные и технические средства, копирование баз данных, раскрытие содержимого носителей информации и т.д.), узлы и каналы передачи информации (анализ трафика, подмена или модификация передаваемых сообщений и т.д.).

Информационные угрозы можно подразделить по причине возникновения на две основные группы: естественные (например, стихийные бедствия, аварии электропитания и т.д.) и человеческие, которые подразделяются по характеру возникновения на две основные группы:

1. Случайные информационные угрозы, которые носят непреднамеренный характер, в том числе:

- неумышленные ошибки операторов, системных администраторов и других, обслуживающих информационные системы лиц при сборе, создании, обработке, переработке и передаче информации (например, при подготовке документации, вводе и выводе данных, округлении, неверные алгоритмы расчета экономических показателей, ошибки аппаратных средств и т.д.);
- стихийная утечка знаний и информации (например, в связи с миграцией населения);
- неумышленные ошибки на стадии проектирования, разработки и внедрения информационных систем и их составляющих (компьютеры, средства связи, операционные системы, прикладные программы и др.) по причине недостаточного уровня квалификации программистов и пользователей и т.д.

2. Преднамеренные информационные угрозы – это целенаправленное воздействие на аппаратные, программные и информационные ресурсы, несанкционированное использование информационных ресурсов по личным противоправным мотивам (например, с целью нанесения ущерба пользователям информационной системы).

Так, начиная с сентября 2017 г. более чем в 25 городах России были получены анонимные сообщения о минировании, из-за чего была проведена массовая эвакуация из объектов пребывания людей (административные здания, торговые центры, кинотеатры, автовокзалы и аэропорты), которые были зарегистрированы в российских населенных пунктах. Источником сообщений называют виртуальные иностранные телефонные номера, средства IP-телефонии.

По характеру воздействия их можно подразделить на пассивные, не оказывающие влияния на состояние информационной системы (например, копирование трафика, документации, подслушивание переговоров и т.п.), и активные, нарушающие нормальный процесс функционирования информационной системы.

К ним относятся:

- получение, передача, искажение и уничтожение научных открытий, изобретений, секретов производства, новых технологий, подслушивание и передача служебных, научно-технических и коммерческих разговоров, документации, электронных носителей информации и т.д., несанкционированным доступ к ресурсам информационной системы;
- целенаправленная утечка знаний и информации (например, промышленный шпионаж и т.д.);
- внесение недокументированных технических изменений аппаратно-программные средства.

Информационные угрозы по виду воздействия на объект информационной безопасности можно разделить на три группы:

1. Разглашение – умышленные или неосторожные действия, приведшие к неправомерному ознакомлению с конфиденциальной информацией в виде утери, сообщения, передачи, предоставления, пересылки, опубликования и т.д. по различным каналам распространения (например, в качестве мести, за вознаграждение, под угрозой шантажа и т.д.).

2. Утечка – бесконтрольный выход конфиденциальной информации за пределы информационной системы или круга лиц, которым она была доверена по службе или стала известна в процессе работы вследствие разглашения, ухода по различным каналам (материально-вещественным, визуально-оптическим, акустическим, электромагнитным) через соответствующие носители информации, которыми могут выступать световые лучи, звуковые волны, бумага, фото, магнитные носители и т.д. (например, магнитное и электрическое поле телефонных проводов, кабелей связи за счет наводок на другие провода, элементы аппаратуры и т.п.), несанкционированного доступа.

3. Несанкционированный доступ – это противоправное преднамеренное ознакомление с конфиденциальной информацией недопущенных лиц, нарушение целостности (подделка, модификация, уничтожение) и доступа к защищаемой информации, в том числе:

- фиктивное сотрудничество и склонение к сотрудничеству;
- подслушивание и выведывание с использованием особенностей характера, обмана и т.д.;
- наблюдение, сбор и аналитическая обработка информации;
- хищение носителей информации, документальных отходов;
- копирование носителей информации, фотографирование, скрытая видеосъемка и т.д.;
- перехват электронных и акустических излучений, электромагнитное облучение и получение паразитной модуляции линий связи, несанкционированное подключение к линиям связи и аппаратным средствам информационной системы с нейтрализацией средств ее защиты;
- восстановление уничтоженной и чтение остаточной информации;
- распространение вредоносных программ, осуществляющих различные воздействия: получение информации скрытым образом от определенных процессов информационной системы или через заданные каналы сети путем перехвата прерываний, адресов и т.д. (программные ловушки, троянские программы и т.д.), использование уязвимостей программного кода, недокументированных функций программ (люки), маскировка под авторизованного пользователя (маскарад), неправомерные «замаскированные» запросы конфиденциальных данных (фишинг), несанкционированное использование привилегий администратора и т.п.

Так, системный администратор в американском штате Массачуссетс преднамеренно обрушил финансовую базу данных бывшего работодателя с помощью вредоносного ПО, внедренного в корпоративную сеть уже после своего увольнения из компании Allegro MicroSystems, производящей компоненты для высокопроизводительных компьютерных систем. Он был осужден за месть работодателю через заражение финансовой базы на Oracle. Компания утверждает, что этот инцидент обошелся фирме в $100 тыс., которые она теперь пытается взыскать с обвиняемого.

От действий бывших или штатных сотрудников с каждым годом страдают все больше компаний по всему миру, в частности, утечки Огромный ущерб по некоторым оценкам в несколько десятков миллиардов долларов несут компании только вследствие утечки

информации в том числе по причине нарушения норм внутренней безопасности при работе информцией. При этом тенденция к постепенному увеличению убытков вследствие утечек все более растет. Так, на протяжении нескольких лет компании ACS (Affiliated Computer Services) и NCsoft неоднократно были скомпрометировалы и понесли убытки на несколько миллиардов долларов в результате утечки программного кода новых компьютерных игр из-за проблемы с внутренним менеджментом. Чтобы изменить ситуацию, владельцы сначала уволили руководителя, а затем компанию покинуло большое число разработчиков. Семеро программистов перед увольнением скопировали код новой игры и продали исходники конкурирующей фирме.

Способы воздействия информационных угроз на объект информационной безопасности подразделяются на следующие группы:

1. Информационные, в том числе:

- 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.

2. Программно-математические, в том числе:

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

3. Организационно-правовые – это невыполнение требований законодательства, несвоевременное применение необходимых нормативно-правовых положений или неправомерное ограничение доступа к нормативно-правовым документам в информационной сфере.

4. Физические, в том числе:

- уничтожение или порча средств обработки информации и связи, радиоэлектронное подавление линий связи и систем управления;
- уничтожение, порча или хищение машинных или других носителей информации; хищение программных или аппаратных ключей и средств криптографической защиты информации; воздействие на персонал;
- перехват информации в технических каналах ее возможной утечки, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;
- воздействие на аппаратные и программные системы авторизации пользователей; внедрение электронных устройств перехвата информации в технические средства и помещения.

2.2. Понятие и виды компьютерных преступлений

В последнее время так называемые «компьютерные преступления» становятся массовым явлением. Системный характер и глобальные масштабы кибератак на сегодняшний день является неоспоримым фактом, что определяется повсеместным применением средств современной компьютерной техники, сетей в различных сферах практической деятельности (банковское дело, биржевая торговля, коммерческая деятельность и т.д.)

Приведем несколько примеров.

В апреле 2009 г. газета The Wall Street Journal сообщала со ссылкой на разведслужбы и представителей правительства США, что хакеры из России и Китая атаковали компьютеры, контролирующие работу энергосетей по всей территории США. Американские разведслужбы утверждали, что взломщики не пытались нарушить работу системы энергообеспечения, однако могли внедрить программы, которые способны нарушить работу энергосетей во время кризиса или войны. Также утверждалось, что киберпреступники проникли в компьютерную систему Пентагона и похитили информацию о новом многоцелевом истребителе пятого поколения.

В ноябре и декабре 2010 года участники группы хакеров Anonymous организовали серию DDoS-атак на сайты компаний и организаций, противодействовавших деятельности ресурса WikiLeaks PayPal, Visa, MasterCard, Sony, Nintendo, PBS, сайт сената США и другие ресурсы).

В марте 2011 года хакеры взломали компьютерную сеть RSA, получив доступ к информации о технологии SecurID, которая применяется для обеспечения безопасности корпоративных компьютерных сетей, в результате чего были скомпрометированы компьютерные сети ряда компаний (Facebook, eBay, Google, Cisco, Motorola, IBM, Intel), оборонные фирмы, финансовые, исследовательские организации (Европейское космическое агентство), а в июне банковская группа Citigroup Inc сообщила о 360 тысяч пострадавших в результате хакерской атаки на базу данных о владельцах пластиковых карт банка в Северной Америке. Были украдены данные номеров счета основных держателей банковской карты, их имен и фамилий, контактной информации, а В мае 2012 г. киберпреступники из хакерской группировки Anonymous получили несанкционированный доступ к серверу министерства юстиции США, где собраны данные о всех преступлениях, совершенных на территории США. В это же время специалисты антивирусной компании "Лаборатория Касперского" обнаружили вредоносную программы Flame. По сообщениям за разработкой обнаруженного вируса Flame стояли разведывательные структуры США и Израиля. При этом вирус был нацелен на похищение промышленных чертежей с правительственных компьютеров в Иране и ряде других ближневосточных стран. 12 июня 2012 г. были предприняты DDoS-атаки на свои Интернет-ресурсы. ряда российских СМИ со стороны бот-сети, состоящей из 133 тысяч зараженных компьютеров мощностью до до 800 Мбит/с. 21 декабря 2012 г. хакеры сняли в 4,5 тысячи банкоматах 5 миллионов долларов, получив доступ к индийскому оператору предоплаченных карт Visa и MasterCard, подняв лимит снятия наличных в банке ОАЭ и

перекодировав магнитные карты в 20 странах мира. Затем 19 февраля 2013 года они похитили 40 миллионов долларов за 36 тысяч операций после взлома оператора предоплаченных карт и поднятия лимита на снятие наличных.

В феврале 2013 г. используемый для размещения фотографий Twitter-аккаунт информационного агентства Франс Пресс был взломан, после чего на нем появились документы, связанные с вооруженным конфликтом в Сирии. 21 марта хакеры сетевой группы "Сирийская электронная армия" взломали аккаунт в сети Twitter британской телерадиовещательной корпорации Би-би-си, который просматривают ежедневно около 60 тысяч пользователей и опубликовали сообщения политического характера. В марте была проведена DDoS атака, названная экспертами одна из крупнейших на сегодняшнее время. Она привела к замедлению работы Интернета в ряде европейских стран. Главной жертвой хакеров стал сайт некоммерческой организации Spamhaus, которая борется со спамерами. В мае-июле 2013 года агентство РИА Новости подверглось крупнейшим DDoS-атакам. В августе 2013 г. были взломаны ряд аккаунтов этого агентства. Хакеры разместили в аккаунтах ложную информацию о смерти президента СССР Михаила Горбачева. В июне ФБР и Microsoft провели совместную операцию по пресечению деятельности более тысячи бот-сетей, входящих в вирусную сеть. Злоумышленники "инфицировали" компьютеры пользователей и получали доступ ко всем персональным данным, в том числе, о банковских счетах. Всего за последние полтора года хакеры похитили около 500 миллионов долларов. 23 апреля был взломан аккаунт на сайте микроблогов Twitter информационного агентства Ассошиэйтед Пресс. В социальной сети было опубликовано ложное сообщение о том, что в Белом доме прогремело два взрыва, в результате чего президент США Барак Обама был ранен.

Компьютерная преступность – это умышленное нарушение чужих прав и интересов, осуществляемое с помощью компьютеров, информационных систем и телекоммуникаций или направленные против них, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства с определенными целями.

Для компьютерных преступлений характерны следующие особенности:

- высокая латентность (низкая степень раскрываемости);
- сложность процесса раскрытия, сбора доказательств и процесса доказывания в суде;
- отсутствие четкой программы и методики борьбы с компьютерными преступлениями;
- отсутствие достаточной следственной практики по расследованию компьютерных преступлений;
- транснациональный характер (как правило, с использованием телекоммуникационных систем)
- значительность материального ущерба;

- высокий уровень подготовки преступников (высококвалифицированные программисты, инженеры, специалисты в области телекоммуникационных систем, банковские работники, бывшие сотрудники спецслужб и т.д.).

Согласно отчету Центра статистической информации ГИАЦ МВД России: в Российской Федерации в 2015 году было зарегистрировано 196700 преступлений, ответственность за которые предусмотрена статьями 159.1 - 159.6 УК РФ, что превышает аналогичные показатели 2014 г. на 25%. Значительно увеличилось число случаев мошенничества в сфере компьютерной информации. В то же время их раскрываемость в 2015 году находилась на уровне всего 7,4 %.

В наиболее общем виде компьютерных преступлений можно классифицировать по способу совершения на следующие основные группы:

1. Несанкционированный доступ – реализуется путем нахождения слабых мест в защите информационной системы, определения участков в системе защиты, имеющих ошибку или неудачную логику программного строения, добавления на такие участки дополнительных команд, проникновения в информационную систему под видом легального пользователя (маскарад) и т.д.:

- подключение с воздействием на парольно-ключевые системы средств электронной защиты;
- копирование (воспроизведение точного или относительно точного оригинала информации)
- модификацию (внесение в информацию любых изменений, обусловливающих ее отличие от той, которую собственник информационного ресурса включил в систему и которой владеет);
- блокирование (обеспечение невозможности доступа к информации со стороны ее законного пользователя); несанкционированное уничтожение (полная или частичная ликвидация как самой информации, так и ее носителей).

2. Вирусная модификация – разработка, использование или распространение компьютерных вирусных программ, которые заведомо приводят к нарушению работы ЭВМ или их сетей, внесению несанкционированных собственником изменений в компьютерную информацию;

3. Перехват информации – получение информации непосредственно через подключение к коммуникационным каналам системы или линиям периферийных устройств (кабельные и проводные системы, системы, системы спутниковой связи и т.д.), а также путем приема электромагнитного и акустического излучения пассивными средствами приема.

2.3 Вредоносные программы для ПК и мобильных устройств

Считается, что первый в истории вирус был создан в 1971 году инженером американской технологической компании BBN Technologies Бобом Томасом, который был способен самостоятельно распространять свои копии в компьютерной сети. Тем не менее,

программа под названием Creeper не была вредоносной и помимо самокопирования была способна отображать надпись: "Я крипер, поймай меня, если сможешь".

В 1981 году 15-летним американский студент Ричардом Скрентой был написан вирус Elk Cloner для компьютеров Apple, который впервые заражал магнитные дискеты и после 50-го обращения к зараженному носителю выводил на дисплей надпись, а в отдельных случаях мог повредить дискету.

В 1991 году в Австралии появилась вредоносная программа Michelangelo для IBM-совместимых персональных компьютеров под управлением операционной системы MS-DOS, масштаб заражения которой составил более 1 млн. компьютеров по всему миру. Она стирала данные на главной загрузочной области жесткого диска.

По мере развития компьютерной техники, программного обеспечения, компьютерных сетей эволюционировали и компьютерные вирусы, как с точки зрения алгоритмов функционирования, так и с точки зрения вредоносных возможностей, которые приводят ко все большее возрастающим издержкам.

Современный этап характеризуется распространением вирусов через сеть Internet и их массовым использованием в преступных целях, а также в качестве кибероружия.

Так, в конце 2008 года в Сети был обнаружен вирус Conficker, который к апрелю 2009 года успел проникнуть более чем в 12 миллионов компьютеров. Похищая пароли, он использовал зараженные машины для рассылки спама или как базы для хранения украденной информации. Пострадали цифровые системы кораблей британских ВМСи Палата общин британского парламента.

В сентябре 2010 г. власти США обвинили более 60 человек в участии в глобальной хакерской атаке на банки путем использования трояна Zeus. С мая 2009 года было похищено не менее 3 миллиона долларов. В это же время компьютерный вирус впервые был использован как кибероружие. Stuxnet поразил компьютеры сотрудников АЭС в Бушере, были созданы проблемы в функционировании центрифуг комплекса по обогащению урана.

Повсеместное внедрение и использование мобильных устройств спровоцировало разработку вредоносного программного обеспечения для разнообразных мобильных платформ. Созданы и распространяются многочисленные модификации вредоносных программ, в том числе червей и троянских коней для мобильных устройств, несмотря на наличие и регулярное обновление соответствующих антивирусных баз.

Так, известны примеры массового заражения мобильных телефонов под управлением операционных систем Symbian, Android, iOS.

В обнаруженных экземплярах выявлено несколько способов распространения, к которым помимо классического для «сетевых» вирусов через Internet-каналы можно отнести и такие специфические виды «мобильных червей», как передаваемые через протокол Bluetooth, так и при помощи сервиса передачи мультимедийных сообщений MMS (например, Comwar, который рассылает себя по всей адресной книге мобильного телефона, или Cabir.k, который ожидает прихода на телефон сообщения и отправляет собственную копию в ответ на это сообщение).

Начиная с Bluetooth-червей, защита от которых по сути гарантирована самим протоколом и определяется только не соблюдением простейших требований информационной безопасности самими пользователями, современные вредоносные программы для мобильных устройств гораздо более опасны. На сегодняшний день они представлены 3-мя классами: «сетевые» и «почтовые» черви, собственно вирусы и троянские программы. Можно с большой долей вероятности предположить, что в ближайшее время появятся новые классы и разновидности компьютерных вирусов для мобильных платформ и приложений.

Классификация вредоносного программного обеспечения

Вредоносное программное обеспечение можно разделить на несколько классов по следующим критериям:

1) по среде обитания:

- резидентные - находятся и функционирует в памяти до выключения питания компьютера;
- нерезидентные - не создают своей копии в оперативной памяти, являются активными ограниченное время.

2) по способу заражения:

- файловый вирус - специально созданная компьютерная программа, которая заражает другие программы (вирусоносители) путем включения в них своей точной или модифицированной копии, которая сохраняет способность к дальнейшему размножению, а также выполняет какие-нибудь вредные действия (нарушение доступности информационной системы, уничтожение или шифрование данных, перехват паролей и т.п.);
- загрузочный вирус - специально созданная компьютерная программа, которая распространяется путем поражения сначала оперативной памяти компьютера, а затем определенных системных областей накопителей информации;
- сетевой (компьютерный червь) - компьютерная программа, которая саморазмножается, распространяется через информационную сеть и не оставляет своей копии на носителях информации, использует ее механизмы для определения потенциально уязвимого узла, который может быть заражен, а затем передает свое тело или его часть на этот узел и активизируется или ожидает наступления заданных условий;

3) по вредоносным возможностям;

- безопасные – практически не влияют на работу информационной системы и ее информационные ресурсы, однако могут уменьшать свободную память на диске в результате своего размножения;
- неопасные - уменьшают свободную память, создают звуковые, графические
- и прочие эффекты, но безопасные для данных информационной системы;
- опасные - могут привести к нарушению функционирования программ или данных системы;
- особо опасные - могут привести к или данных системы, способны нарушить работоспособность информационнй системы и привести к потере ее данных;

4) по специфике алгоритма действия.

- вирусы-«спутники» - вирусы, которые не изменяют исполняемые файлы, а создающие для них файлы-спутники, содержащие их копию;
- «паразитические» - вирусы, которые изменяют содержимое загрузочных секторов диска или файлов
- макровирус - особая разновидность компьютерных вирусов, которые заражает офисные документы в прикладных программах, имеющих средства и разрешение на исполнения совокупности последовательных команд (макрокоманд);
- троянский конь - компьютерная программа, выполняющая в дополнение к основным не описанные в документации действия при наступлении некоторого условия (даты, времени и т.д.) или по команде извне (например, сбор конфиденциальной информации, рассылка спама и т.д.);
- логическая бомба - особая разновидность компьютерного вируса в виде участка компьютерной программы, который реализует некоторые вредоносные действия при наступлении определенных условий в дате или имени файла;
- стелс-вирус (невидимка) - специально созданная компьютерная программа, которая перехватывает обращения операционной системы или программ к зараженным файлам, секторам носителей информации или оперативной памяти и подставляет вместо себя незараженные участки или содержит так называемые руткиты, позволяющие скрыть деятельность компьютерного вируса;
- полиморфные вирусы (вирусы-призраки) - особая разновидность компьютерного вируса, основное тело которого зашифровано и не имеет постоянного участка программного кода для каждой новой копии;
- бэкдор - компьютерная программа, позволяющая осуществлять скрытое и несанкционированное управление информационной системой извне.
- рекламные системы (adware) – компьютерная программа, инициирующая запуск рекламу или перенаправляющие поисковые запросы на рекламные веб-сайты без ведома и согласия пользователя;
- криптовирусы (ransomware) – особая разновидность компьютерного вируса, который шифрует все файлы определенных типов, найденные на компьютере, после чего удаляет оригиналы.

Так, в мае 2017 года до 300 тыс. компьютеров в по меньшей мере 150 странах мира подверглось атаке криптовируса-вымогателя WannaCry. Вирус шифровал файлы пользователя, которые становились недоступны, а за расшифровку данных злоумышленники требовали заплатить $600 в криптовалюте биткойн. Предполагаемый ущерб превысил $1 млрд. Аналогично действовал криптовирус Petya в июне 2017 года, распространявшийся через ссылки в сообщениях электронной почты, требуя выкуп в размере $300 в биткойнах, когда.пострадали более 80 компаний в РФ и на Украине. При этом шифровалась главная загрузочная запись (MBR) загрузочного сектора диска. Таким образом, восстановить работоспособность и запустить операционную систему можно после ее компрометации по

команде bootrec /fixMbr, однако расшифровать файлы не удастся. Для каждого диска генерируется свой ключ AES, который существует в памяти до завершения процесса шифрования. Он шифруется на открытом ключе RSA и удаляется. Восстановление содержимого после завершения требует знания закрытого ключа, таким образом, без знания ключа данные восстановить невозможно.

Также в октябре 2017 года атаке криптовируса Bad Rabbit подверглись информационные системы международных аэропортов, метрополитена и ряда других объектов в РФ, на Украине, в Турции и Германии. Он послужил причиной недоступности для пользователей сайтов ряда СМИ. Вирус блокировал рабочий стол пользователя компьютера и требовал выкуп (перевод определенной суммы денежных средств на счет злоумышленников) за ключ, разрешающий продолжить работу и вернуть расшифрованные файлы.

Контрольные вопросы по 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 по 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;

В. 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

3.1. Деятельность международных организаций в сфере информационной безопасности.
3.2. Органы государственной власти Российской Федерации в сфере информационной безопасности.
3.3. Нормативно-правовые акты в области информационной безопасности в РФ.

3.1. 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.

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].

Таблица 1

Основные задачи международных организаций в сфере информационной безопасности

Наименование международной организации	Год начала действия	Задачи, которые они решают
TU - International Telecommunication Union Международный союз электросвязи	1885г.	Множество вопросов, связанных с построением компьютерных сетей, передачей цифровых данных обработкой информации и т.д. 1. Управление и координация деятельности в сфере передачи информации и в телефонной и радиосвязи
IEEE - Institute of Electrical and Electronics Engineers Институт инженеров по электронике и электротехнике	1884г.	Множество вопросов, связанных с электротехникой, радиоэлектроникой, вычислительной техникой, информатикой, а также с некоторыми разделами математики и физики 1. проведение специализированных профессиональных конференций 2. публикация специализированных изданий 3. поддержка образовательной деятельности 4. поддержка инновационных технических и методических разработок в различных сферах 5. разработка и распространение технических стандартов
ACM - Association for Computin Machinery Ассоциация вычислительной техники	1947г.	1. поддержка образовательных проектов в сфере информационных технологий 2. организация научно-практических конференций 3. общественно- политическая работа, связанная информационными технологиями 4. публикация изданий и сборников научных трудов, посвященных проблемам современных информационных технологий
W3 Consortium Консорциум Всемирной Паутины	1989г.	1. обеспечения возможности доступа к сети Интернет для как можно большего числа людей 2. обеспечение возможности подключения к Интернет различных технических устройств 3. обеспечение возможности структурирования и формализации интернет-информации 4. обеспечение надежности и безопасности обмена информацией
ISSA - Information Systems Security Association Ассоциация безопасности информационных систем	1984г.	1. Продвижение методов управления, которые обеспечивают конфиденциальность, целостность и доступность информационных ресурсов 2. Создание более успешной среды для обеспечения безопасности глобальных информационных систем

ISO - International Organization for Standardization Международная организация по стандартизации	1946г.	С вопросами информационной безопасности также связана работа Подкомитета: 1. SC 37 "Биометрическая идентификация" 2. SC 17 "Карточки и персональная идентификация" Основные задачи: 1. Содействие развитию стандартизации и смежных видов деятельности в мире с целью обеспечения международного обмена товарами и услугами 2. Развития сотрудничества в интеллектуальной, научно-технической и экономической областях
IETF - Internet Engineering Task Force Инженерный совет интернета	1986г.	1. Развитие протоколов и архитектуры интернета 2. Идентификация проблемы предложения решений в технических аспектах организации интернета 3. Разработка спецификаций стандартов и соглашений по общим архитектурным принципам протоколов интернет 4. Вынесение рекомендаций относительно стандартизации протоколов 5. Содействие широкому распространению технологий и стандартов 6. Организация дискуссии для обмена информации в сообществе интернета между учеными, разработчиками, пользователями и производителями 7. Улучшение работы интернета через создание высококачественных технических документов, которое оказывает влияние на то, как люди разрабатывают что-либо для интернета
ICSA - International Computer Security Association Международная организация по защите компьютерной информации	1989г.	1. Повышении осведомленности о необходимости обеспечения компьютерной безопасности 2. Предоставлении образования по различным продуктам и технологиям безопасности 3. Исследования, испытания и сертифицирование продуктов безопасности включая антивирусы, файрволлы, средства криптографии, антишпионские программы
ISACA - Information Systems Audit and Control Association Ассоциация аудита и контроля информационных систем	1969г.	1. Разработка и формализация единых эффективных подходов к оценке 2. Управлению информационными технологиями, ИТ-рисками
ISA - Internet Security Alliance Альянс по безопасности сети Интернет	2001г.	1. Создание эффективных механизмов обмена информацией об уязвимостях в сети Интернет и найденных решениях проблем безопасности 2. Исследование фундаментальных проблем безопасности 3. Развитие программ профессиональной подготовки и сертификации специалистов по информационной безопасности 4. Взаимодействие с государственными органами

		законодательной и исполнительной власти
CERT Coordination Center (CERT/CC) Координационный центр CERT	1988г.	1. Обеспечению безопасности глобальной информационной инфраструктуры 2. Сбор сведений об уязвимостях в информационных системах 3. Поддержание актуальной базы знаний об уязвимостях в информационных системах 4. Развитие локальных (национальных и корпоративных) групп реагирования на инциденты
X-Force Security Intelligenceteam - Исследовательская группа X-Force	2006г. куплена IBM	1. поддержание в актуальном состоянии базы данных известных уязвимостей различных программных и аппаратных платформ 2. оказание услуг по индивидуальному анализу угроз и информированию 3. выпуск периодических информационных бюллетеней с обзорами наиболее значимых событий в сфере информационной безопасности
Альянсы крупных технологических компаний		1. Разработка новых продуктов и услуг, базовых технологий, протоколов, алгоритмов и соглашений, на основе которых такие продукты и услуги в будущем могли бы разрабатываться 2. Формирование новых рынков сбыта и поддержка существующих 3. Влияние на государственные и общественные организации, а также на сообщество пользователей информационных систем с целью обеспечения развития и более широкого использования информационных технологий и средств информационной безопасности 4. Влияние на систему профессиональной подготовки специалистов с целью обеспечения качества их обучения
Smart Card Alliance (SCA) - Альянс по смарт-картам	2001г.	1. Развитие технологий для идентификации пользователей различных сервисов и информационных систем 2. Ведение централизованной базы данных поставщиков оборудования и услуг в сфере смарт-карт 3. Организацию образовательных программ и системы сертификации специалистов 4. Издание информационных и справочных материалов технического и управленческого характера
Internet Security Alliance (ISA) -	2001г.	1. Выявление и разрешение коренных проблем

Альянс по безопасности сети Интернет		информационной безопасности 2. Разработка учебных программ по вопросам корпоративной информационной безопасности 3. Проведение своевременных семинаров по возникающим проблемам безопасности 4. Предоставление предупреждений о возникающих угрозах безопасности и и подробных отчетах об уязвимостях и угрозах
The International BiometricIndustry Association (IBIA) - Международная ассоциация компаний-производителей биометрического оборудовани	1998г.	1. Ориентация рынка потребительских систем на широкое использование биометрических технологий 2. Защита базовых интересов членов альянса в сфере стандартизации биометрических технологий и систем, использующих биометрию 3. Взаимодействие с потенциальными заказчиками их продукции с целью продвижения средств биометрической идентификации

В сфере информационной безопасности работают также специализированные международные организации и объединения.

Их функционирование имеет 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-Forcекомпании IBM.

CERT Coordination Center (CERT/CC) - Координационный центр CERT,возникшая в 1988 году как Computer security incidentresponseteam(Группа реагирования на инциденты, связанные с компьютерной безопасностью), функционирует на базе Института разработки программного обеспечения при Университете Карнеги-Мелон (Software Engineering Institute, Carnegie Mellon University) и финансируется Министерством обороны и Министерством

национальной безопасности США.

X-Forcesecurity intelligence team - Исследовательская группа X-Forceотносится к компании Internet Security Systems (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* Analysis Service (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.

Smart Card Alliance (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: Smart Card Industry Associationи Smart Card Forum.В состав альянса входят около сотни различных компаний и правительственных организаций.

Internet Security Alliance (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 (Electronic Industries Alliance, EIA). Уже к середине 2004 года в альянс входило около тридцати членов, в числе которых такие крупные компании, как Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec и 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.

The International Biometric Industry Association (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, LG Electronics, Panasonic, NEC и другие [45]

3.2. Органы государственной власти Российской Федерации в сфере информационной безопасности

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.

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.

Таблица 2

Задачи государственных органов в сфере информационной безопасности

Название	Задачи
Совет Федерации Федерального Собрания Российской Федерации	Утверждении изменений границ субъектов. Назначении выборов главы государства. Утверждении президентских Указов, вводящих военное, чрезвычайное положение. Отрешении главы страны от поста. Назначении судей КС, ВС, ВАС. Утверждении кандидатуры и снятии с поста Генпрокурора. Назначении и освобождении от должностей зампредседателя и 50% аудиторов от Счетной палаты.
Государственная Дума Федерального Собрания Российской Федерации	• дача согласия президенту Российской Федерации на назначение председателя Правительства Российской Федерации; • заслушивание ежегодных отчётов Правительства Российской Федерации о результатах его деятельности, в том числе по вопросам, поставленным Государственной думой; • решение вопроса о доверии Правительству Российской Федерации; • назначение на должность и освобождение от должности председателя Центрального банка Российской Федерации; • назначение на должность и освобождение от должности председателя Счётной палаты Российской Федерации и половины состава её аудиторов; • назначение на должность и освобождение от должности уполномоченного по правам человека, действующего в соответствии с федеральным конституционным законом; • объявление амнистии; • выдвижение обвинения против Президента Российской Федерации для отрешения его от должности. Государственная дума принимает федеральные законы большинством голосов от общего числа депутатов, если иное не

	оценка военной опасности и военной угрозы, выработка мер по их нейтрализации; 4) подготовка предложений Президенту Российской Федерации: а) о мерах по предупреждению и ликвидации чрезвычайных ситуаций и преодолению их последствий; б) о применении специальных экономических мер в целях обеспечения безопасности; в) о введении, продлении и об отмене чрезвычайного положения; 5) координация деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения безопасности; 6) оценка эффективности деятельности федеральных органов исполнительной власти в области обеспечения безопасн
федеральные органы исполнительной власти	• Разработка и реализация единой государственной политики в области защиты прав юридических лиц, индивидуальных предпринимателей при осуществлении федерального государственного контроля (надзора) в соответствующих сферах деятельности. • Организация и осуществление федерального государственного контроля (надзора) в соответствующих сферах деятельности. Перечень видов федерального государственного контроля (надзора) и федеральных органов исполнительной власти, уполномоченных на их осуществление, ведется в порядке, установленном Правительством РФ. • Разработка административных регламентов осуществления федерального государственного контроля (надзора) в соответствующих сферах деятельности. • Организация и проведение мониторинга эффективности

	федерального государственного контроля (надзора) в соответствующих сферах деятельности, показатели и методика проведения которого утверждаются Правительством РФ.
Центральный банк Российской Федерации	. **Эмиссия денег** состоит в том, что центральный банк осуществляет монопольное право выпуска неразменных кредитных денег. . **Осуществление национальной денежно-кредитной политики** . **Банкир правительства** — в этой функции на центральный банк возложено кассовое обслуживание государственного бюджета и государственного долга. Будучи банкиром правительства, центральный банк хранит на своих счетах средства госбюджета и госзаймов. . **Банк банков.** Поскольку центральный банк не работает с физическими лицами и хозяйственными структурами, тозвеном-посредником выступают коммерческие банки и специализированные кредитно-финансовые институты. Центральный банк осуществляет руководство и контроль над всей кредитно-финансовой системой. Центральный банк устанавливает **обязательные нормы резервов** для коммерческих банков, выступает для последних кредитором последней инстанции. Кроме того, центральный банк осуществляет **переучет векселей** коммерческих банков. . **Хранение золотого и валютного запаса страны**. . **Денежно-кредитное регулирование экономики**.

Военно- промышленная комиссия Российской Федерации	• Реализации государственной политики в сфере оборонно-промышленного комплекса, военно-технического обеспечения обороны страны, безопасности государства и правоохранительной деятельности. • Принимать решения, касающиеся организации, координации, совершенствования и оценки эффективности деятельности федеральных органов исполнительной власти по реализации государственной политики в сфере оборонно-промышленного комплекса, и осуществлять контроль за их исполнением. • Давать поручения федеральным органам исполнительной власти по вопросам, связанным с разработкой, производством, ремонтом и утилизацией вооружения, военной и специальной техники. • Запрашивать и получать в установленном порядке документы и материалы, необходимые для обеспечения деятельности комиссии. • Привлекать в установленном порядке для подготовки проектов решений Комиссии представителей федеральных органов государственной власти, органов государственной власти субъектов РФ. • Осуществлять контроль за выполнением решений коллегии Военно-промышленной комиссии.
органы исполнительной власти субъектов Российской Федерации	• Разработка административных регламентов осуществления регионального государственного контроля (надзора) в соответствующих сферах деятельности, а также разработка в соответствии с типовыми административными регламентами, утверждаемыми уполномоченными федеральными органами исполнительной власти, административных регламентов осуществления федерального государственного контроля (надзора),

	полномочия по осуществлению которого переданы для осуществления органам государственной власти субъектов Российской Федерации • Организация и проведение мониторинга эффективности регионального государственного контроля (надзора) в соответствующих сферах деятельности, показатели и методика проведения которого утверждаются Правительством РФ. • Реализация единой государственной политики в области защиты прав юридических лиц, индивидуальных предпринимателей и соблюдение законодательства Российской Федерации. • Организация и осуществление регионального государственного контроля (надзора) в соответствующих сферах деятельности на территории соответствующего субъекта РФ.
органы местного самоуправления	• Обеспечение участия населения в решении вопросов местного значения. • Управление муниципальной собственностью, финансовыми средствами местного самоуправления. • Обеспечение удовлетворения потребностей населения в социально-культурных, коммунально-бытовых, транспортных, торговых и иных важных для населения услугах. • Обеспечение комплексного развития территории муниципального образования. • Создание для населения благоприятной среды обитания. • Охрана общественного порядка и личная безопасность граждан. • Защита интересов и прав местного самоуправления, гарантированных Конституцией Российской Федерации

Органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности	• Законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом. • Конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности. • Соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере. • Достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз. • Соблюдение общепризнанных принципов и норм международного права, международных договоров РФ, а также законодательства Российской Федерации. • Обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере.
Задачи службы экономической безопасности	– защита законных прав и интересов предприятия и его сотрудников; – сбор, анализ, оценка данных и прогнозирование развития обстановки; – изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании; – своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности; – недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями; – противодействие техническому

	проникновению в преступных целях; – выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности; – защита сотрудников предприятия от насильственных посягательств; – обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия; – добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании; – физическая и техническая охрана зданий, сооружений, территории и транспортных средств; – формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей; – возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц; – контроль за эффективностью функционирования системы безопасности, совершенствование ее элементов.
- отдел экономической безопасности;	• Организация работы по противодействию преступности в сфере экономики. • Предупреждение, выявление, пресечение и раскрытие преступлений экономической и коррупционной направленности, в том числе совершаемых (совершённых) организованными преступными группами. • Координация деятельности. • Организационно-методическое обеспечение деятельности подчиненных подразделений экономической безопасности и противодействия коррупции. • Обеспечение экономической

	безопасности и осуществление борьбы с преступлениями экономической и коррупционной направленности, в том числе совершенными организованными группами, преступными сообществами (преступными организациями). • Документирование преступлений экономической и коррупционной направленности.
служба безопасности персонала (режимный отдел)	• Проверка кандидатов при приеме на работу, выявление возможных рисков и угроз для компании. • Обеспечение безопасности в процессе исполнения персоналом служебных обязанностей. • Предотвращение нанесения экономического ущерба и утечки информации, составляющей коммерческую тайну в случае увольнения сотрудника. • Сотрудники СБ в своей работе с персоналом используют различные методы предупредительно-профилактического характера, такие как обучение, инструктажи, санкции.

3.3. 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).

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.3.

Рис.3. 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];
- Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р;
- 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.

Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 26.07.2017)

Настоящий Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Статья 1. Сфера действия настоящего Закона

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной власти, а также организациями, наделенными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности (далее - органы государственной власти), органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Последние изменения произведены на основании Федеральный закон от 26 июля 2017 года №193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Федеральный закон "Об участии в международном информационном обмене" от 04.07.1996 N 85-ФЗ

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Цели настоящего Федерального закона - создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

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

Международный обмен конфиденциальной информацией, массовой информацией осуществляется в порядке, устанавливаемом настоящим Федеральным законом, другими федеральными законами и иными нормативными правовыми актами.

Утратил силу с 9 августа 2006 года на основании Федерального закона от 27 июля 2006 года N 149-ФЗ.

Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

Статья 1. Цели и сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

(часть 1 в ред. Федерального закона от 12.03.2014 N 35-ФЗ)

2. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

В последней редакции Федерального закона отмечается ряд статей и пунктов, утративших силу:

1. Статья 2. Законодательство Российской Федерации о коммерческой тайне (Утратила силу с 1 октября 2014 года - Федеральный закон от 12 марта 2014 года N 35-ФЗ.

2. Статья 3. Основные понятия, используемые в настоящем Федеральном законе - Пункт утратил силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ;

3. Статья 4. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации - Часть утратила силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ.

4. Статья 7. Права обладателя информации, составляющей коммерческую тайну (статья утратила силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ.)

5. Статья 8. Обладатель информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений (статья утратила силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ.)

6. Статья 9. Порядок установления режима коммерческой тайны при выполнении государственного или муниципального контракта для государственных или муниципальных нужд (статья утратила силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ.).

7. Статья 12. Охрана конфиденциальности информации в рамках гражданско-правовых отношений (статья утратила силу с 1 января 2008 года - Федеральный закон от 18 декабря 2006 года N 231-ФЗ.).

Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Статья 1. Сфера действия настоящего Федерального закона.

1. Настоящий Федеральный закон регулирует отношения, возникающие при: 1) осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации. 2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом. (Часть в редакции, введенной в действие с 1 августа 2013 года Федеральным законом от 2 июля 2013 года N 187-ФЗ. Комментарий к статье 1).

В настоящий документ вносятся изменения на основании ст. 8 Федерального закона от 31.12.2017 N 482-ФЗ с 30 июня 2018 года (далее – краткая информация по внесению изменений):

Внести в Федеральный закон от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст.3448; 2010, N 31, ст.4196; 2011, N 15, ст.2038; N 30, ст.4600; 2012, N 31, ст.4328; 2013, N 14, ст.1658; N 23, ст.2870; N 27, ст.3479; N 52, ст.6961, 6963; 2014, N 19, ст.2302; N 30, ст.4223, 4243; N 48, ст.6645; 2015, N 1, ст.84; N 27, ст.3979; N 29, ст.4389, 4390; 2016, N 26, ст.3877; N 28, ст.4558; N 52, ст.7491; 2017, N 18, ст.2664; N 24, ст.3478; N 25, ст.3596; N 27, ст.3953; N 31, ст.4790, 4825, 4827; N 48, ст.7051) следующие изменения:

1) дополнить статьей 14_1 следующего содержания: "Статья 14_1. Применение информационных технологий в целях идентификации граждан Российской Федерации» (с п. 1 по 24);

2) статью 17 дополнить частью 1_1 следующего содержания:

"1_1. Лица, виновные в нарушении требований статьи 14_1 настоящего Федерального закона в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации".

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.

Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р [58]

Целями настоящей Программы являются:

- создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное

взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан;

- создание необходимых и достаточных условий институционального и инфраструктурного характера, устранение имеющихся препятствий и ограничений для создания и (или) развития высокотехнологических бизнесов и недопущение появления новых препятствий и ограничений как в традиционных отраслях экономики, так и в новых отраслях и на высокотехнологичных рынках;
- повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики Российской Федерации, так и экономики в целом.

5 декабря 2016 года Президент России Владимир Путин подписал Указ об утверждении новой Доктрины информационной безопасности Российской Федерации [2].

Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

Положения Доктрины соответствуют актуальным тенденциям в сфере информационных технологий и информационной безопасности, действующим и вынесенным на рассмотрение нормативно-правовым актам в сфере импортозамещения, обеспечения безопасности критически важной инфраструктуры РФ, противодействия кибератакам и иным актуальным вопросам.

В частности, в новой Доктрине развиты положения Стратегии национальной безопасности РФ, касающиеся:

- возрастающего противоборства в глобальном информационном пространстве;

- угроз нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры РФ;

- деятельности, связанной с использованием информационных и коммуникационных технологий в экстремистской деятельности;

- а также импортозамещения и снижения критической зависимости от зарубежных технологий и промышленной продукции.

В целом, курс на импортозамещение прослеживается как в старой, так и новой версии документа. Однако можно отметить, что в Доктрине экономическая сфера обеспечения информационной безопасности сконцентрирована именно на необходимости развития отрасли информационных технологий и информационной безопасности.

Новый документ провозглашает ликвидацию зависимости от иностранных информационных технологий частью стратегии информационной безопасности Российской Федерации.

При этом наряду с производственными компаниями, в сферу национальных интересов попадает совершенствование деятельности компаний, оказывающих услуги в области обеспечения информационной безопасности.

Среди новых задач в рамках деятельности по обеспечению информационной безопасности, возложенных на государственные органы, можно выделить выработку и реализацию мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Таким образом, можно надеяться, что в перспективе развитие данных положений при формировании государственной политики должно перерасти в меры поддержки компаний-интеграторов в сфере информационной безопасности.

Еще одним нововведением Доктрины информационной безопасности РФ 2016 года являются задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности, среди которых:

- **укрепление** вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

- **совершенствование** форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

- **совершенствование** информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

- **повышение** эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

К мероприятиям, осуществляемым уже сейчас, либо планируемым, и соответствующим вышеперечисленным задачам, можно отнести создание ГосСОПКА, FinCERT, АПК «Безопасный город», а также создание системы распределенных ситуационных центров.

В рамках Доктрины информационной безопасности РФ, утвержденной Указом №646 2016 г., понятие «критическая информационная инфраструктура» можно определить как совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

В рамках Федерального Закона «О безопасности критической информационная инфраструктура РФ» (Проект ФЗ №47571-7) приводится следующее определение: «критическая информационная инфраструктура РФ» - совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.

В предыдущей версии документа данному аспекту информационной безопасности не было уделено столь пристальное внимание. Безусловно, это связанно с непрерывно возрастающим количеством угроз информационной безопасности критически важных объектов.

Не случайно в один день с подписанием новой Доктрины на рассмотрение Государственной Думы был вынесен законопроект, вводящий уголовную ответственность до 10 лет лишения свободы за создание программ для кибератак на инфраструктуру Российской Федерации, а также законопроект о безопасности критической информационной инфраструктуры Российской Федерации.

* Критически важная инфраструктура имеет ключевое значение для общественного порядка, экономической стабильности и национальной безопасности государств, особенно уязвимы развитые страны. Защита критической инфраструктуры затрагивает вопросы

национальной безопасности, и потому входит в компетенцию государства. Тем не менее, большая часть инфраструктур находится в собственности частного бизнеса, поэтому государство и бизнес вынуждены совместно нести ответственность за безопасность и стабильное функционирование. Значимость защиты критически важных информационных инфраструктур возрастает по ряду причин, среди которых: — широкое распространение информационных технологий, в том числе, в целях обеспечения эффективной работы большинства инфраструктур и систем государства и бизнеса;

— возрастающая зависимость общества и государства от нормального функционирования критических инфраструктур;

— рост сложности, и, следовательно, уязвимости информационной составляющей критической инфраструктуры.

Сложные информационные системы чувствительные не только в отношении информационных атак, они также подвержены сбоям в работе по причине ошибок в программном обеспечении, неточностей персонала и др. Выявить истинную причину неполадок зачастую бывает непросто.

Отметим, что главной характеристикой критической инфраструктуры является ее ключевое значение для безопасности общества и государства. Критически важные инфраструктуры могут быть военными и гражданскими объектами, а также иметь двойное назначение. В информационной сфере гражданские и военные объекты тесно переплетены.

В документе уделено пристальное внимание защите частной жизни российских граждан в ходе обработки персональных данных с использованием информационных технологий.

Инциденты, связанные с кражей баз персональных данных, как в нашей стране, так и в мире, явление далеко не редкое. При этом информация, попадающая в руки злоумышленников, может быть довольно чувствительной. Кроме того, обладание такой информацией может давать злоумышленникам возможность совершать преступления и в других сферах, например, в финансовой.

В связи с тем, что эффективное развитие рынков и отраслей (сфер деятельности) в цифровой экономике возможно только при наличии развитых платформ, технологий, институциональной и инфраструктурной сред, настоящая Программа сфокусирована на 2 нижних уровнях цифровой экономики - базовых направлениях, определяя цели и задачи развития:

- ключевых институтов, в рамках которых создаются условия для развития цифровой экономики (нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технологических заделов);

- основных инфраструктурных элементов цифровой экономики **(информационная инфраструктура, информационная безопасность).**

В Российской Федерации традиционно большое внимание уделяется вопросам обеспечения информационной безопасности объектов газоснабжения, энергоснабжения и ядерных объектов. Однако при этом две третьих российских компаний полагают, что количество преступлений в цифровой среде за 3 последних года возросло на 75 процентов, что требует совершенствования системы информационной безопасности во всех секторах экономики.

С использованием цифровых технологий изменяются повседневная жизнь человека, производственные отношения, структура экономики и образование, а также возникают новые требования к коммуникациям, вычислительным мощностям, информационным

системам и сервисам. Достижение запланированных характеристик цифровой экономики РФ на период 2018-2030 гг. [69]

Все большее число граждан Российской Федерации признает необходимость обладания цифровыми компетенциями, однако уровень использования персональных компьютеров и информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") в России все еще ниже, чем в Европе, и существует серьезный разрыв в цифровых навыках между отдельными группами населения.

Определяющее значение в происходящей трансформации приобретают исследования и разработки, что требует создания системы управления исследованиями и разработками в области цифровой экономики, обеспечивающей координацию усилий заинтересованных сторон - представителей федеральных органов исполнительной власти, компаний, высших учебных заведений и научных организаций.

Целью направления, касающегося **информационной безопасности**, является достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации в условиях цифровой экономики, что предполагает:

- **обеспечение** единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры Российской Федерации на всех уровнях информационного пространства ;

- **обеспечение** организационной и правовой защиты личности, бизнеса и государственных интересов при взаимодействии в условиях цифровой экономики;

- **создание** условий для лидирующих позиций России в области экспорта услуг и технологий информационной безопасности, а также учет национальных интересов в международных документах по вопросам информационной безопасности.

Разработка и реализация мероприятий настоящей Программы базируется на основополагающих принципах информационной безопасности, включающих:

- **использование** российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки;

- **преимущественное использование** отечественного программного обеспечения и оборудования; применение технологий защиты информации с использованием российских криптографических стандартов.

Достижение запланированных характеристик цифровой экономики Российской Федерации обеспечивается за счет достижения ряда показателей к 2024 году , в том числе:

- в отношении информационной инфраструктуры: доля домашних хозяйств, имеющих широкополосный доступ к сети "Интернет" (100 мбит/с), в общем числе домашних хозяйств - 97 процентов; во всех крупных городах (1 млн. человек и более) устойчивое покрытие 5G и выше;

- в отношении информационной безопасности: доля субъектов, использующих стандарты безопасного информационного взаимодействия государственных и общественных институтов, - 75 процентов; доля внутреннего сетевого трафика российского сегмента сети "Интернет", маршрутизируемая через иностранные серверы, - 5 процентов.

Для управления развитием цифровой экономики формируется **"дорожная карта",** которая по основным направлениям включает описание целей, ключевых вех и задач

настоящей Программы, а также сроков их достижения. Далее представлены данные интересующих нас направлений, а именно:

	Информационная инфраструктура
2018	Определен частотный ресурс для развертывания сетей 5G, утверждена генеральная схема размещения центров обработки данных и создана система льгот и преференций, создающих условия для вложения частных инвестиций во все объекты информационной инфраструктуры (сети связи, в том числе спутниковые, центры обработки данных, "сквозные" цифровые платформы и инфраструктура пространственных данных)
2020	Все федеральные автомобильные дороги покрыты сетями связи с возможностью беспроводной передачи данных, сети связи 5G внедрены во всех городах с численностью населения более 1 млн. человек, созданы "сквозные" цифровые платформы, предоставляющие субъектам цифровой экономики максимально широкий набор инструментов и интерфейсов, обеспечивающих обработку различного вида данных и предоставление цифровых услуг, и развернута современная отечественная инфраструктура сбора, обработки, хранения и предоставления потребителям пространственных данных
2024	Широкополосный доступ к сети "Интернет" имеют 97 процентов домашних хозяйств, также 100 процентов лечебно-профилактических учреждений, учреждений сферы образования, другие общественно- значимые объекты инфраструктуры, осуществляется широкое коммерческое использование сетей 5G, экспортируются услуги по обработке и хранению данных, внедрены отечественные методы и программные средства автоматизированной обработки, распознавания и дешифрирования пространственных данных, получаемых посредством дистанционного зондирования Земли (съемки из космоса, съемки с воздушных, в том числе беспилотных летательных аппаратов, лазерного сканирования и др.)
	Информационная безопасность
2018	Решены наиболее актуальные проблемы защиты прав и свобод граждан в цифровом пространстве
2020	Создан каркас инфраструктуры безопасности цифровой экономики, в том числе в области новейших технологий, обеспечен цифровой суверенитет Российской Федерации
2024	Российская Федерация является одним из мировых лидеров в области информационной безопасности

Задачи направления «Информационная инфраструктура», сроки реализации:

1. Обеспечить возможность широкополосного доступа к сети "Интернет" для населения (срок реализации – с IV квартал 2017 г. по 2024).

2. Обеспечить широкополосный доступ лечебно-профилактических учреждений к сети "Интернет" (срок реализации – с III квартал 2017 г по IV квартал 2018 г.)

3. Обеспечить широкополосный доступ образовательных учреждений и другие общественно значимых объектов к сети "Интернет" (срок реализации – со II квартал 2018 г. по 2024г.)

4. Обеспечить широкополосный доступ к сети "Интернет" всех органов государственной власти и местного самоуправления (срок реализации – со II квартал 2018 г по IV квартал 2020 г.)

5. Обеспечено покрытие всех федеральных автомобильных дорог сетями связи с возможностью беспроводной передачи данных, необходимой для развития современных интеллектуальных логистических и транспортных технологий (срок реализации – со II квартал 2018 г. по IV квартал 2020 г.)

6. Внедрить технологию подвижной и фиксированной связи 5G в городах с численностью населения более 1 млн. чел.(срок реализации – с IV квартал 2017 г. по 2024)

7. Построение федеральной сети узкополосной связи по технологии LPWAN для сбора и обработки телематической информации (срок реализации – с IV квартал 2017 г.по 2024)

8. Создать дополнительный механизм стимулирования инвестиционной активности операторов для развития сетей связи на основе передовых технологий (срок реализации – с I квартал 2018 г. по IV квартал 2018 г.)

9. Обеспечить доступность услуг по хранению и обработке данных на всей территории России для граждан, бизнеса и власти(срок реализации – II квартал 2018 г.. по IV квартал 2020 г.)

10. Обеспечить хранение и обработку всей информации, создаваемой органами государственной власти и местного самоуправления, в государственной единой облачной платформе (срок реализации - I квартал 2018 г. по IV квартал 2020 г.)

11. Усовершенствовать техническое регулирование центров обработки данных (далее - ЦОД) в целях обеспечения устойчивости, безопасности и экономической эффективности их функционирования (срок реализации - II квартал 2018 г. по IV квартал 2018 г.)

12. Определить состав необходимых отечественных цифровых платформ и обеспечить их внедрение (IV квартал 2017 г. по IV квартал 2024 г.)

13. Обеспечить возможность использования данных в цифровых платформах (IV квартал 2018 г. по II квартал 2020 г)

14. Создать отечественную цифровую платформу сбора, обработки и распространения пространственных данных для нужд картографии и геодезии, обеспечивающую потребности граждан, бизнеса и власти (IV квартал 2017 г. по IV квартал 2020 г.)

15. Создать отечественную цифровую платформу сбора, обработки, хранения и распространения данных, дистанционного зондирования Земли, обеспечивающую потребности граждан, бизнеса и власти (проект "Цифровая Земля" из космоса) (IV квартал 2017 г. по IV квартал 2020 г.).

Задачи направления «Информационная безопасность», сроки реализации:

1. Обеспечить устойчивость и безопасность функционирования единой сети электросвязи Российской Федерации - II квартал 2018 г. по IV квартал 2022 г.

2. Обеспечить управляемость и надежность функционирования российского сегмента сети "Интернет" - III квартал 2018 г. по I квартал 2020 г.

3. Обеспечить технологическую независимость и безопасность функционирования аппаратных средств и инфраструктуры обработки данных - I квартал 2018 г. по IV квартал 2024 г.

4. Обеспечить устойчивость и безопасность функционирования информационных систем и технологий - I квартал 2018 г. по IV квартал 2020 г.

5. Обеспечить правовой режим и технические инструменты функционирования сервисов и использования данных - II квартал 2018 г. по IV квартал 2022 г.

6. Обеспечить правовой режим межмашинного взаимодействия для киберфизических систем - I квартал 2018 г. по 2022 г.

7. Обеспечить правовой режим функционирования машинных и когнитивных интерфейсов, включая интернет вещей - II квартал 2018 г. по 2022 г.

8. Обеспечить защиту прав, свобод и законных интересов личности в условиях цифровой экономики - I квартал 2018 г. по IV квартал 2020 г.

9. Создать технические инструменты, обеспечивающие безопасное информационное взаимодействие граждан в условиях цифровой экономики - IV квартал 2018 г. по I квартал 2020 г.

10. Обеспечить защиту прав и законных интересов бизнеса в условиях цифровой экономики - I квартал 2018 г. по 2024 г.

11. Обеспечить организационную и правовую защиту государственных интересов в условиях цифровой экономики - II квартал 2018 г. по 2024 г.

12. Создать эффективные механизмы государственного регулирования и поддержки в области информационной безопасности при интеграции национальной цифровой экономики в международную экономику - I квартал 2018 г. по 2024 г.

13. Создать основы для построения доверенной среды ЕАЭС, обеспечивающей коллективную информационную безопасность - II квартал 2018 г. по 2023 г.

14. Обеспечить участие России в подготовке и реализации международных документов по вопросам информационной безопасности, относящимся к цифровой экономике - I квартал 2018 г. по 2022 г.

Итак, основные правовые документы в сфере информационной безопасности:

- Конституция РФ (http://constitutionrf.ru/);
- 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/);
- 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);
- 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/);
- 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/);
- 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/);
- 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/);
- Федеральный закон от 06 апреля 2011 №63 «Об электронной подписи» (с изменениями на 23.06.16 г.) (http://docs.cntd.ru/document/902271495);

- 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);
- Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р (http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf).

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. АСМ;

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

4.1. Политика безопасности и ее принципы.

4.2. Подходы, принципы, методы и средства обеспечения ИБ.

4.1. 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 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 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.

4.2. Подходы, принципы, методы и средства обеспечения ИБ

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

Существует два подхода к обеспечению информационной 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.3) 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 ИС. Недостатком данного подхода является высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления.

Комплексный подход является системным подходом. 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 для создания системы защиты.

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.

Принцип 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.

Принцип полноты 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.

Принцип 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.

Принцип контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

Принцип экономической целесообразности 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 представлены на рис. 3.

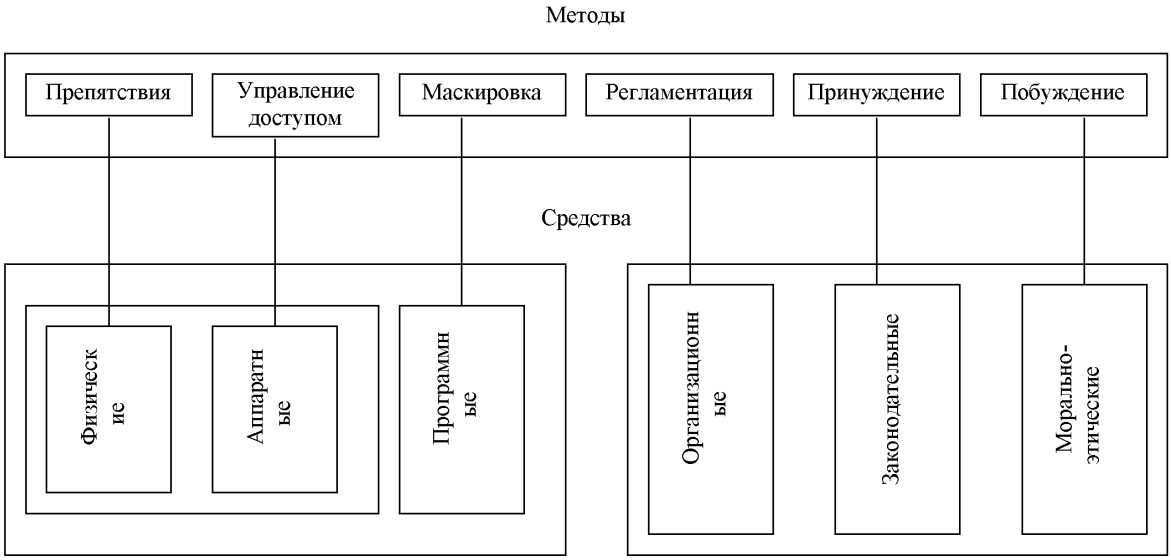


Рис. 3. Методы и средства информационной безопасности

Методами обеспечения защиты информации 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. 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 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 организационноправовые 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 называется открытым. Для предотвращения несанкционированного доступа к сообщению оно зашифровывается. Санкционированный пользователь, получив сообщение, дешифрует или раскрывает его посредством обратного преобразования криптограммы. Вследствие чего получается исходный открытый текст.

Шифрование может быть *симметричным* и *асимметричным* (несимметричным).

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;

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 идентификации 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.

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

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

5.1. Организационное обеспечение информационной безопасности.
5.2. Защита информации в Интернет.
5.3. Защита от компьютерных вирусов.
5.4. Этапы построения системы защиты информации.

5.1. 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. 3 изложены организационные мероприятия, обеспечивающие защиту документальной информации.

Таблица 3

Обеспечение информационной безопасности организации

Составные части делопроизводства	**Функции обеспечения ИБ при работе с документами**	**Способы выполнения**
Документирование	Предупреждение: - необоснованного изготовления документов; - включение в документы избыточной конфиденциальной информации; - необоснованного завышения степени конфиденциальности документов; - необоснованной рассылки	Определение перечня документов Осуществление контроля за содержанием документов и степени конфиденциальности содержания Определение реальной степени конфиденциальности сведений, включенных в документ Осуществление контроля за размножением и рассылкой документов
Учет документов	Предупреждение утраты (хищения) документов	Контроль за местонахождением документа
Организация документооборота	Предупреждение: - необоснованного ознакомления с документами; - неконтролируемой передачи документов	Установление разрешительной системы доступа исполнителей к документам Установление порядка приема-передачи документов между сотрудниками
Хранение документов	Обеспечение сохранности документов Исключение из оборота документов, потерявших ценность	Выделение специально оборудованных помещений для хранения документов, исключающих доступ к ним посторонних лиц Установление порядка подготовки документов для уничтожения
Уничтожение документов	Исключение доступа к бумажной «стружке»	Обеспечение необходимых условий уничтожения Осуществление контроля за правильностью и своевременностью уничтожения документов
Контроль наличия, своевременности и правильности исполнения документов	Контроль наличия документов, выполнения требований обработки, учета, исполнения и сдачи	Установление порядка проведения наличия документов и порядка их обработки

При выборе и оборудовании специальных защищенных помещений для размещения СКТ и связи, а также хранения носителей информации рекомендуется придерживаться следующих требований. 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. 4 приведена классификация методов обеспечения информационной безопасности, основанных на использовании инженерно-технических средств.

Рис. 4. 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. 5 [57].

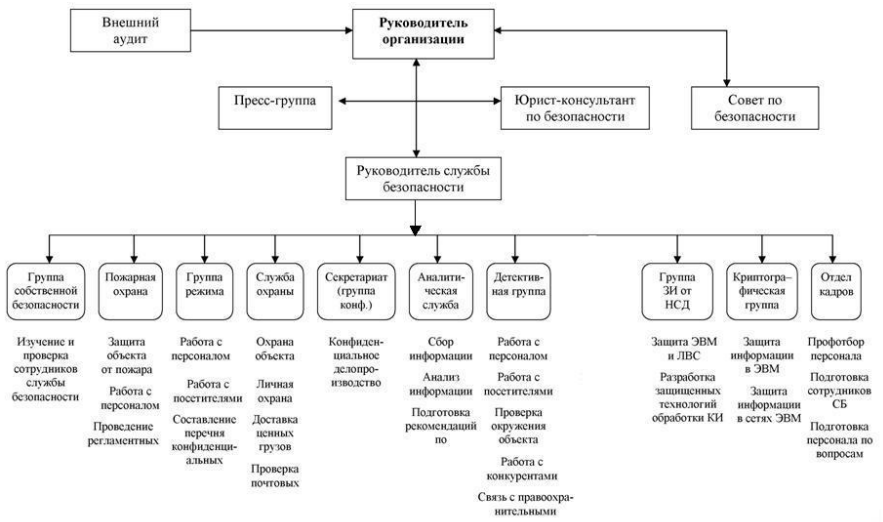


Рис. 5. Структура и задачи службы безопасности

5.2. Защита информации в Интернет

Защита информации в Интернет

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 [46] 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;

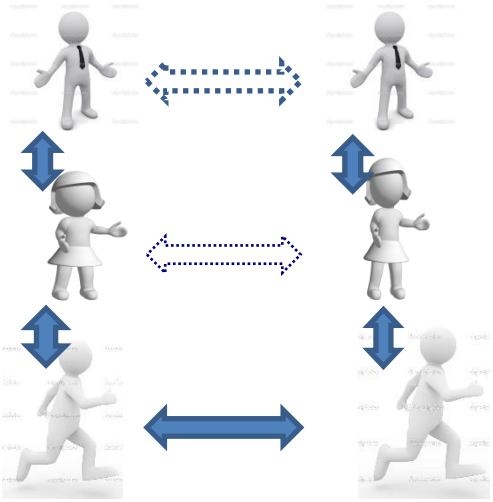
2) использование брандмауэров или файерволов (firewall), выполняющих функцию межсетевых экранов (они занимают положение между локальной сетью и глобальной, не позволяя просматривать извне состав программного обеспечения на сервере, и не пропуская несанкционированные команды и данные).

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).

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);

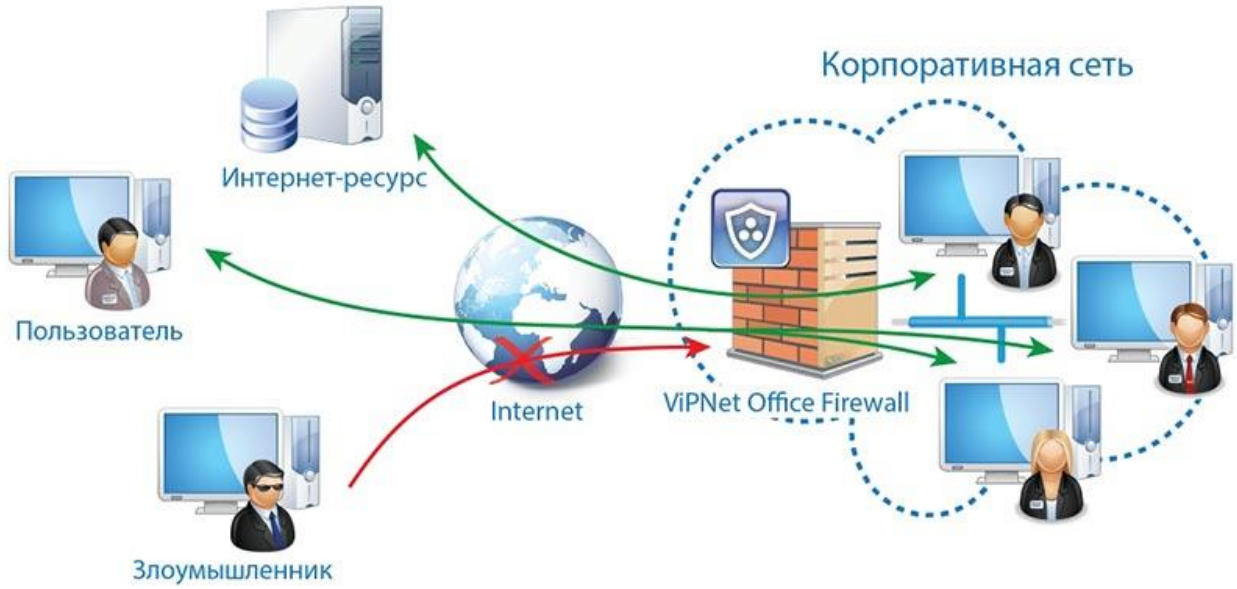
Дополнительные защитные функции:

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.).

В качестве примера современного файервола рассмотрим **ViPNet Office Firewall** компании ИнфоТеКС [59]. Это программный межсетевой экран, предназначенный для контроля и управления трафиком и преобразования трафика между сегментами локальных сетей при их взаимодействии, а также при взаимодействии узлов локальных сетей с ресурсами сетей общего пользования.



Системные требования, предъявляемые к компьютеру для установки файервола:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
- Объем оперативной памяти — не менее 1 Гбайт;
- Свободное место на жестком диске — не менее 300 Мбайт;
- Операционная система — Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2, Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012.

Помимо защиты компьютеров локальной сети от несанкционированного доступа по сетевому соединению, ViPNet Office Firewall позволяет запретить работу с Интернетом для определенных компьютеров локальной сети, пользователям которых такой доступ для служебных нужд не требуется, или разрешить отдельным компьютерам работать в сети только с определенными сервисами, например, почтовыми серверами. ViPNet Office Firewall обеспечивает работу с несколькими сетевыми интерфейсами, позволяя объединять сегменты подсетей и для каждого сетевого адаптера можно задать свой режим работы и свои фильтры. Также имеется возможность организации так называемой «демилитаризованной зоны» (ДМЗ), в которой можно разместить серверы, открытые для доступа из Интернета. При этом исходящий трафик из ДМЗ в локальные сети, подключенные к другим внутренним адаптерам, можно полностью заблокировать.

Динамическая трансляция сетевых адресов позволяет работать множеству внутренних клиентов под одним внешним IP-адресом. Реализована также статическая трансляция сетевых адресов, что позволяет публиковать во внешней сети (Интернете) серверы, находящиеся во внутренней сети, например, почтовый сервер.

Специальная функция обработки прикладных протоколов обеспечивает активацию разрешающего сетевого фильтра для дополнительного соединения на случайно выбранный порт, открываемый прикладным протоколом.

Имеется возможность группировать объекты. Группы объектов — это средство, позволяющее упростить создание сетевых фильтров и правил трансляции адресов. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров фильтра или правила вместо отдельных объектов.

Можно фильтровать широковещательные IP-пакеты по адресам конкретных отправителей.

Существует возможность применения правил фильтрации по заранее заданному расписанию, позволяющая гибко управлять и ограничивать расходы на оплату каналов связи.

В программе реализованы средства регистрации и отображения результатов (событий) обработки IP-пакетов. Поддерживается автоматическая архивация журналов и экспорт данных в формат html или MS Excel.

Можно создавать различные конфигурации с разными наборами фильтров и оперативно переключаться между ними.

В последнее время все чаще появляются устройства, совмещающие функции межсетевых экранов и прокси-серверов. В качестве примера такого устройства рассмотрим шлюз безопасности ViPNet Coordinator HW5000 компании ИнфоТеКС [59].

Программно-аппаратный комплекс ViPNet Coordinator HW5000 — шлюз безопасности для защиты высокоскоростных каналов связи (до 10 Гб/сек). Устройство позволяет

организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру.

ПАК ViPNet Coordinator HW5000 предоставляет широкий спектр возможностей.

Сервер в защищенной сети ViPNet:

- ViPNet VPN-шлюз сетевого уровня (L3): защита соединений сетевого уровня (OSI) с шифрованием и аутентификацией;
- ViPNet VPN-шлюз канального уровня (L2): защита соединений канального уровня (OSI) с шифрованием и аутентификацией;
- Сервер IP-адресов (оповещение защищенных узлов о параметрах доступа друг к другу);
- Маршрутизатор VPN-пакетов (маршрутизация и контроль целостности зашифрованных IP-пакетов, передаваемых между сегментами защищенной сети);
- Маскирование структуры трафика за счет инкапсуляция в UDP, TCP.

Фильтрация трафика (межсетевой экран):

- Межсетевой экран с контролем состояния сессий и инспекцией прикладных протоколов. Раздельная настройка фильтрации для открытого и шифруемого IP-трафика;
- NAT/PAT;
- Антиспуфинг;
- Сервер Открытого Интернета (организация безопасного подключения компьютеров корпоративной сети к Интернету);
- Прокси-сервер.

Сетевые функции:

- Статическая маршрутизация;
- Динамическая маршрутизация;
- Резервирование и балансировка WAN каналов;
- Поддержка VLAN (dot1q);
- Агрегирование интерфейсов (bonding, EtherChannel(LACP)): резервирование и балансировка;
- Поддержка классификации и приоритезации трафика (QoS, ToS, DiffServ).

Сервисные функции:

- DNS-сервер;
- NTP-сервер;
- DHCP-сервер;
- DHCP-Relay;
- Поддержка ИБП (UPS);
- Кластер горячего резервирования: отказоустойчивый координатор в конфигурации ViPNet Failover.

Совместно с другими программными продуктами линейки ViPNet Network Security, ViPNet Coordinator HW5000 обеспечивает эффективную реализацию множества сценариев защиты информации, например:

- Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site);
- Защищенный доступ удаленных и мобильных пользователей;
- Взаимодействие с сетями ViPNet других организаций;
- Защита магистральных каналов, соединяющих ЦОДы;
- Защита мультисервисных сетей (включая IP-телефонию и видео-конференц-связь);

• Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ);

• Защищенный контролируемый доступ в Интернет;

• Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.

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 алгоритмов преобразования информации.

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].

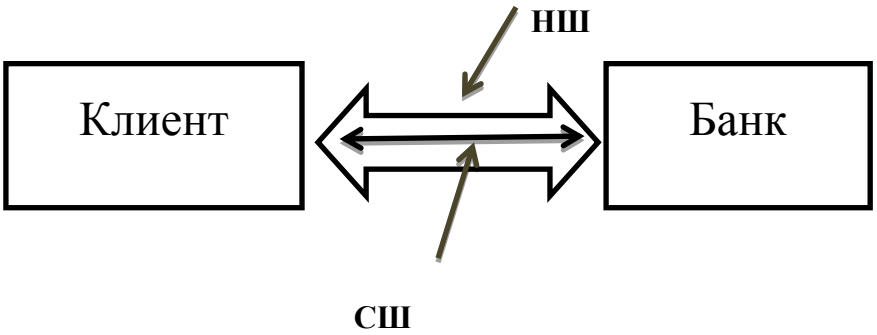
Программные средства, реализующие протокол SSL, базируются на гибридной криптографической системе, в которой сочетаются несимметричные (НШ) и симметричные (СШ) алгоритмы шифрования.

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.

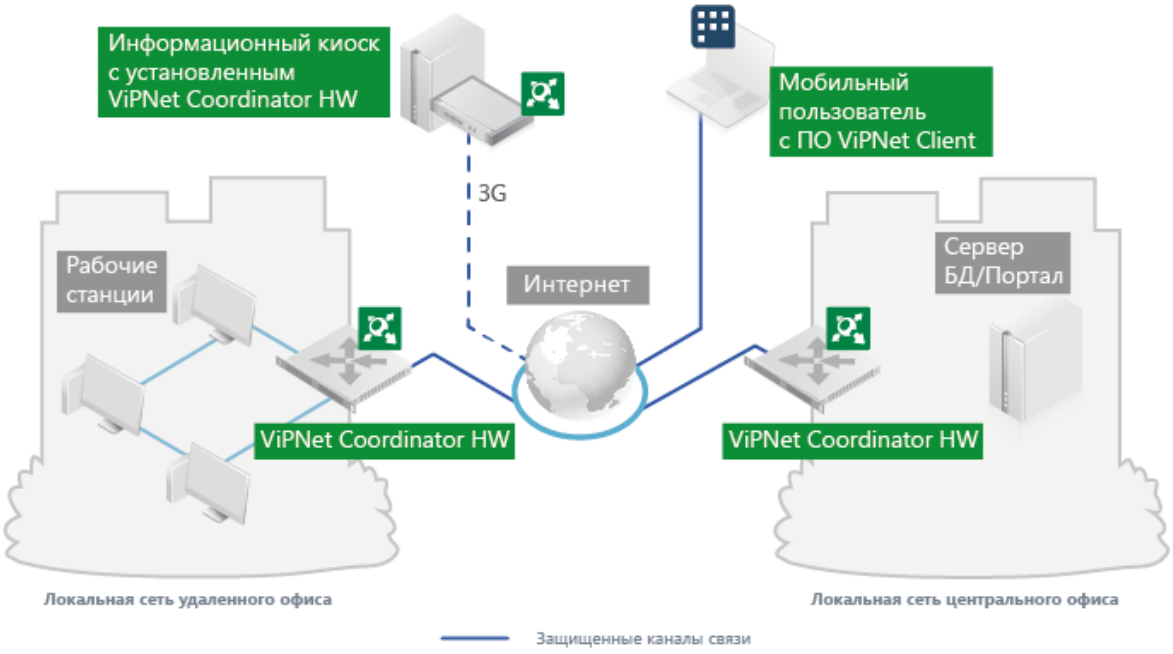
DKIM (Domain Keys Identified Mail, Сообщение, идентифицированное ключами домена) — технология удостоверения подлинности отправителя при помощи цифровой подписи, связанной с именем домена. Наличие данной подписи подтверждает, что письмо не было перехвачено и изменено после отправки с почтового сервера 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. Они базируются на каналах связи сети Интернет, которые являются открытыми. Возникает проблема защиты корпоративной конфиденциальной информации, передаваемой по таким каналам. Создание виртуальных частных сетей (virtual private networks, VPN) позволяет разрешить ее. Реализацию VPN рассмотрим на примере линейки устройств российской компании ИнфоТеКС [59].

Корпоративная сеть представляет собой совокупность локальных офисных сетей, мобильных пользователей и т.д., взаимосвязанных между собой по каналам связи Интернета.



Для организации защищенной VPN используются специальные серверные компоненты, пользовательские компоненты и система управления и мониторинга. Рассмотрим их подробнее.

Серверные компоненты выполняют функции шлюзов безопасности и устанавливаются на стыках локальных сетей и глобальной сети. На схеме, приведенной выше, эту функцию выполняет **ViPNet Coordinator HW**, который обеспечивает построение защищенных каналов связи между офисами компании, защищенный доступ удаленных и мобильных пользователей, межсетевые взаимодействия, разграничение доступа к информации в локальной сети, защищенный контролируемый доступ в Интернет из локальной сети и другие возможности (полный список см. выше при описании ViPNet Coordinator HW5000).

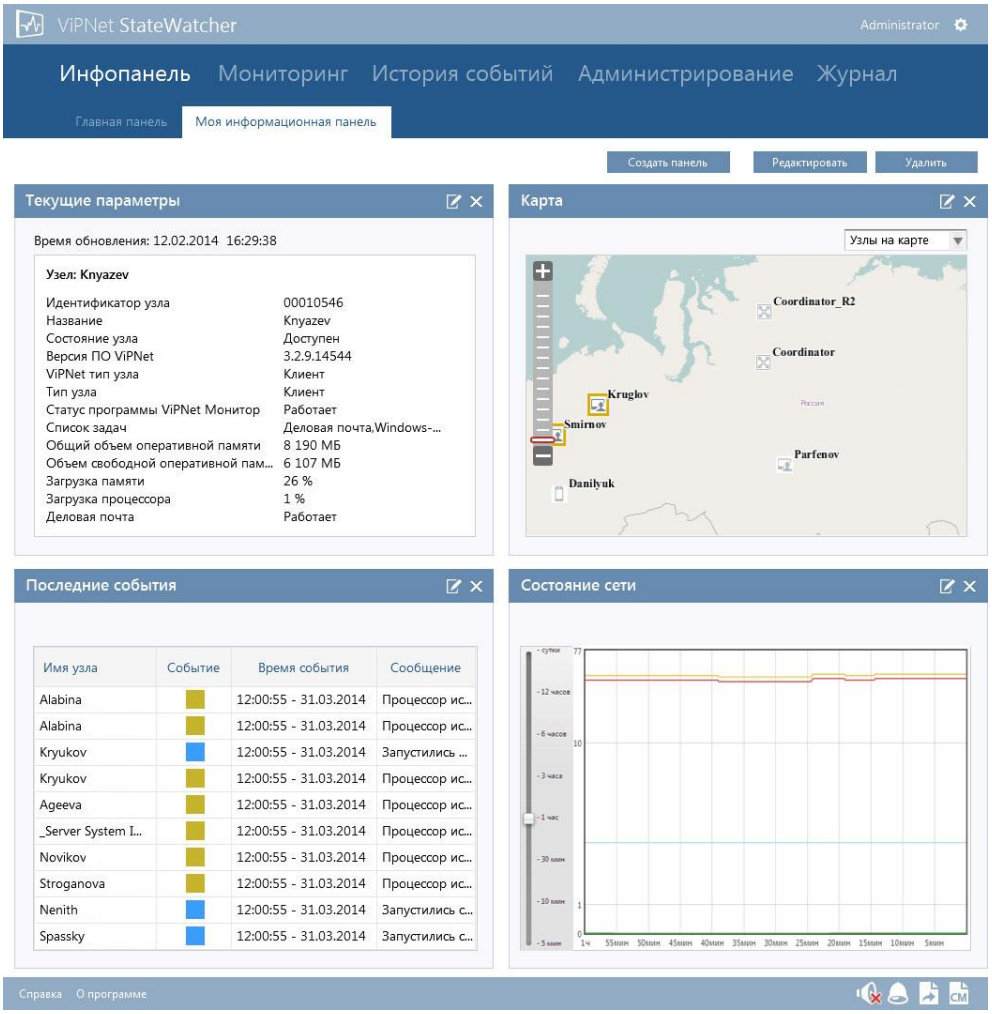
Пользовательские компоненты представляют собой ПО, устанавливаемое на терминальном устройстве (компьютер или смартфон работника компании). Оно отвечает за:

- шифрование трафика,
- сетевое экранирование,
- обмен файлами,
- фильтрацию трафика по различным параметрам,
- реализацию режима «stealth», позволяющего сделать устройство невидимым из открытой сети,
- контроль сетевой активности приложений и компонентов операционной системы устройства.

Система управления и мониторинга располагается в центральном офисе и представляет собой программный комплекс, предназначенный для управления защищенной сетью и включающий в себя следующие компоненты:

- Центр Управления Сетью для конфигурирования VPN,
- Ключевой и Удостоверяющий Центр для выработки криптографических ключей и обеспечения инфраструктуры открытых ключей,
- Программный комплекс для централизованного мониторинга событий безопасности и других событий, происходящих на узлах сети, а также для выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах.

На рисунках приведены интерфейсы и информационные панели комплекса мониторинга.

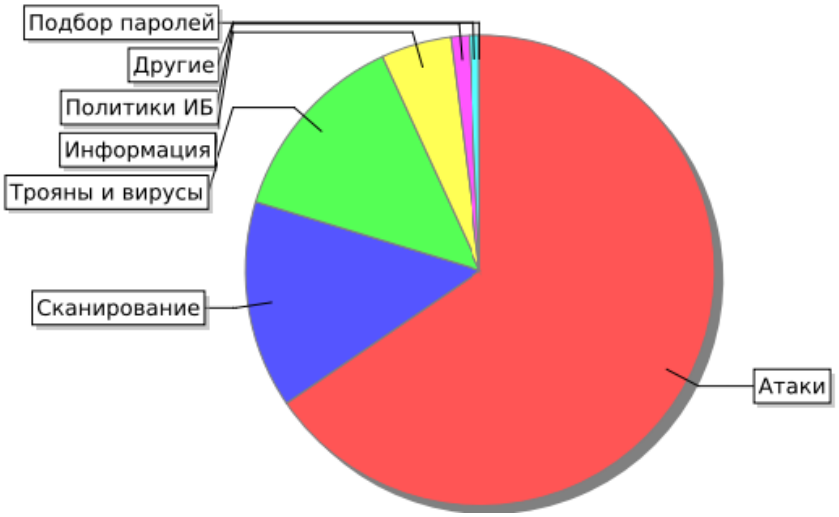


Статистика по событиям

Распределение событий по категориям

События с 9/15/16 4:50 PM по 9/16/16 3:57 PM

Наименование	Количество
Атаки	28008
Сканирование	6097
Трояны и вирусы	5745
Информация	2071
Политики ИБ	537
Другие	314
Подбор паролей	14



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».

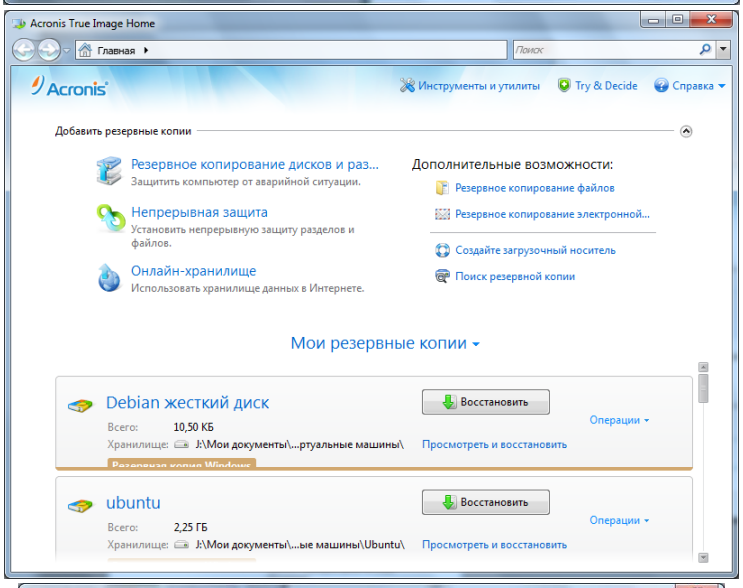
Надежная работа с компьютерной информацией достигается только тогда, когда любое неожиданное событие не приведет к катастрофическим последствиям.

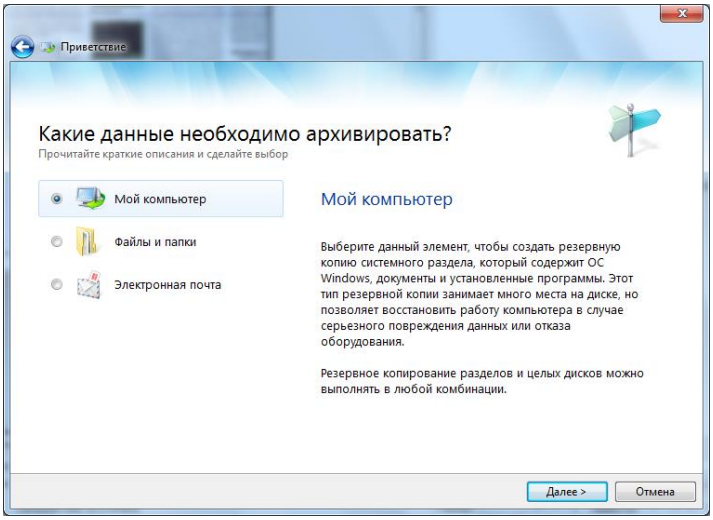
Для этого применяют:

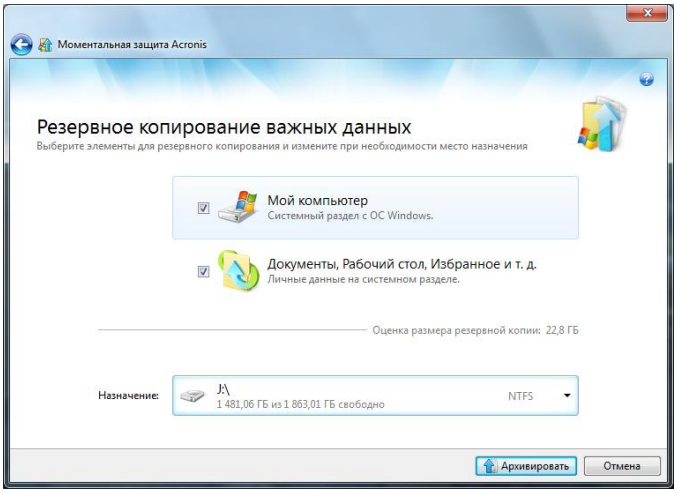
1. Резервное копирование наиболее ценных данных.

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).







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

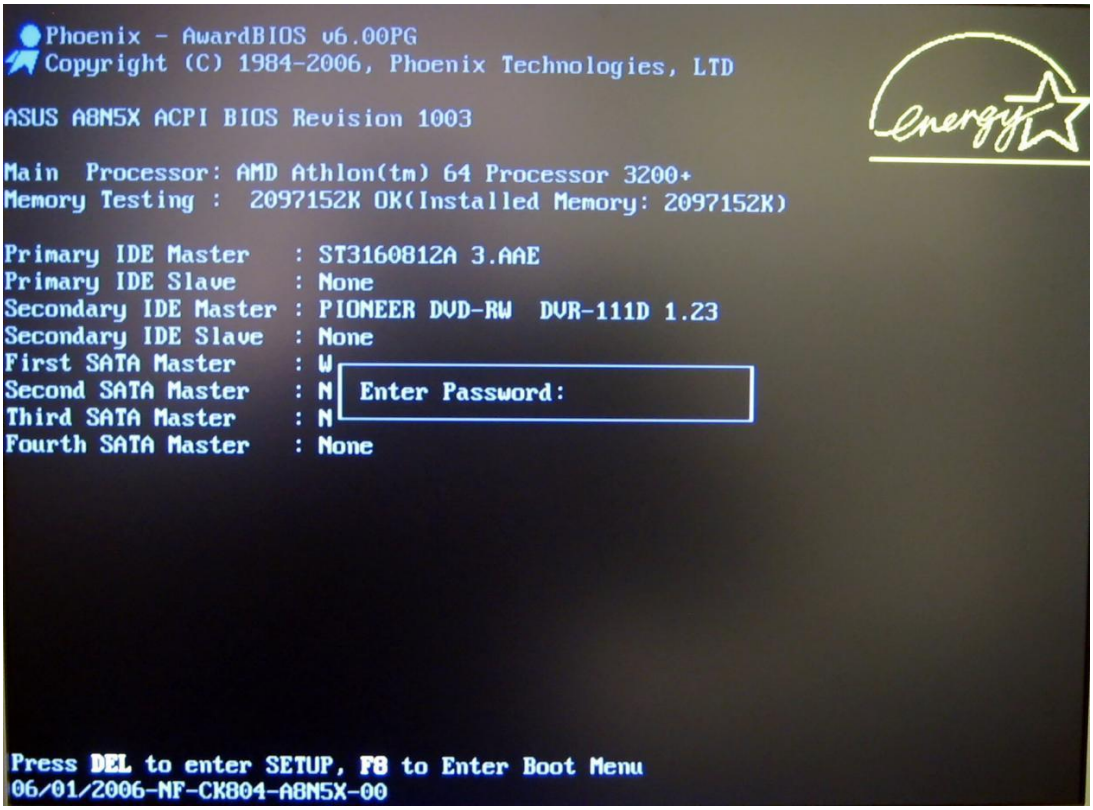
«Неправильные» пароли:

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.

5.3. 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]

5.4. 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 (**Net Present Value – NPV**). По сути, это текущая стоимость будущих денежных потоков инвестиционного проекта с учетом дисконтирования и за вычетом инвестиций. Этот показатель рассчитывается по следующей формуле:

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

Где

CF_i – чистый денежный поток для *i*-го периода $

CF_0 – начальные инвестиции $

n – ставка дисконтирования (стоимость капитала, привлеченного для инвестиционного проекта).

При значении NPV большем или равном нулю, считается, что вложение капитала эффективно. При сравнении нескольких проектов принимается тот из них, который имеет большее значение NPV, если только оно положительное.

Предположим, некой компании требуется оценить проект по защите одного из сегментов сети своей информационной системы при помощи системы обнаружения вторжений (IDS). Допустим, известна величина риска, исчисляемая в денежном выражении (20000 долл. за год), которая учитывает потери от реализации тех или иных атак и вероятности их осуществления. Также известно, что величина риска после внедрения IDS сократится на 70%. Стоимость IDS составляет 15000 долл. Ставку дисконтирования возьмем среднюю для ИТ рынка – 30 %. Подробнее потоки денежных средств по данному проекту представлены в таблице 4.

Таблица 4

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

6.1. Менеджмент и аудит информационной безопасности на уровне предприятия.
6.2. Аудит информационной безопасности электронной коммерции.
6.3. Менеджмент информационной безопасности электронной коммерции.

6.1. 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.

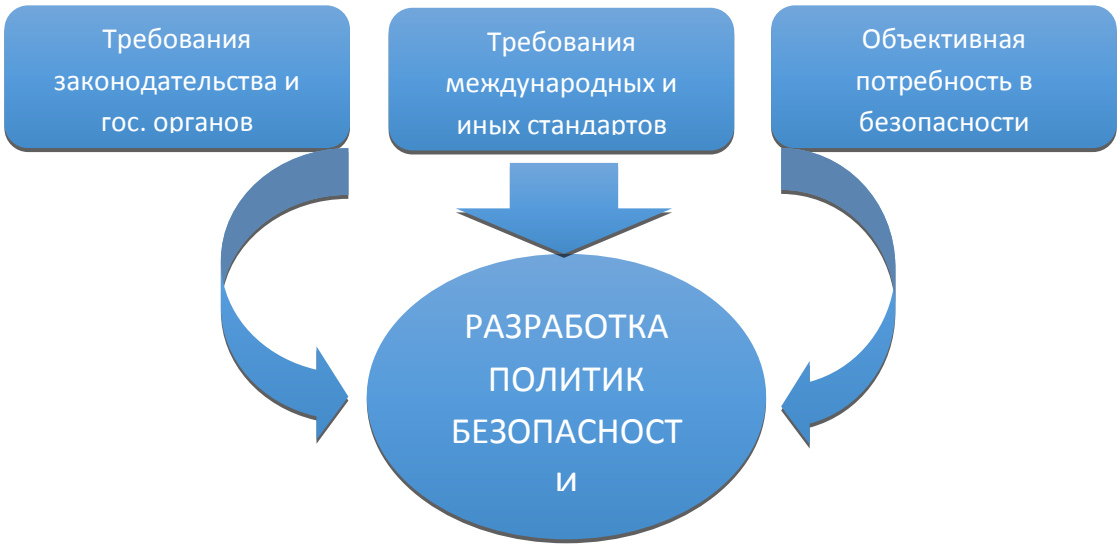


Рис. 7. Предпосылки разработки политики безопасности предприятия.

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]

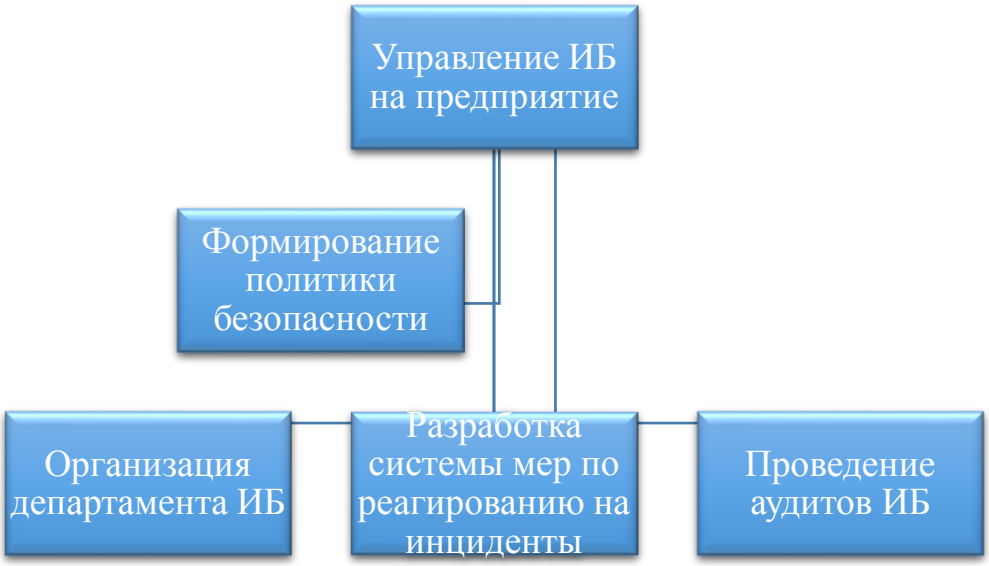


Рис. 8. Структура организационной деятельности в сфере информационной безопасности

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.

6.2. 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.

Data pro Information Services Group провела почтовый опрос среди случайно выбранных менеджеров информационных систем. Целью опроса явилось выяснение состояния дел в области защиты. Было получено 1153 анкеты, на основе которых получены приводимые ниже результаты:

- около 25% всех нарушений составляют 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.

о Управление внутренними ресурсами.

о Управление сетями.

6.Безопасность носителей данных.

7. Контроль доступа.

о Бизнес требования для контроля доступа.

о Управление доступом пользователя.

о Ответственность пользователей.

о Контроль и управление удаленного (сетевого) доступа.

о Контроль и управление доступом к приложениям.

о Мобильные пользователи.

8. Криптография.

о Безопасность системных файлов.

9. Управление непрерывностью бизнеса.

о Непрерывность бизнеса и анализ воздействий.

о Создание и внедрение плана непрерывного ведения бизнеса.

10. Соответствие системы основным требованиям.

о Соответствие требованиям законодательства.

о Анализ соответствия политики безопасности.

о 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.

6.3. 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.

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.

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.

58. Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р (http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf).

59. Продукты и решения компании ИНФОНЕКС. [Электронный ресурс]: http: // www.infotecs.ru.

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.

Приложение 1

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

24 средствами вычислительной и организационной техники.

25 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28 Назначение, виды, структура и технология функционирования системы защиты информации.

29 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30 Аналитическая работа по выявлению каналов утечки информации фирмы.

31 Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32 Направления и методы защиты профессиональной тайны.

33 Направления и методы защиты служебной тайны.

34 Направления и методы защиты персональных данных о гражданах.

35 Методы защиты личной и семейной тайны.

36 Построение и функционирование защищенного документооборота.

37 Защита секретов в дореволюционной России.

38 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 (от 2016 года).
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.