МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Ю.А. Гатчин, Е.В. Климова

ВВЕДЕНИЕ В КОМПЛЕКСНУЮ ЗАЩИТУ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Учебное пособие

Санкт-Петербург

2011

Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.

Целью данного учебного пособия является ознакомление студентов с основами организации комплексной защиты объектов информатизации.
Рассматриваются принципы создания, этапы разработки и весь процесс проектирования комплексных систем защиты информации на предприятии.
Пособие предназначено для бакалавров и магистров, обучающихся по направлению Информационная безопасность, курс Основы информационной безопасности, а также слушателей факультета повышения квалификации.
Рекомендовано к печати Ученым советом факультета Компьютерных технологий и управления, 18.10.11, протокол № 8.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого были определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Содержание

Сокращения и условные обозначения

АС – автоматизированная система
АСОД – автоматизированная система обработки данных
ГОСТ – государственный стандарт
ГТК – гостехкомиссия
ЗИ – защита информации
ИБ – информационная безопасность
ИТ – информационные технологии
КСЗИ – комплексная система защиты информации
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОИ – объект информатизации
ОС – операционная система
ПК – персональный компьютер
ПО – программное обеспечение
ПС – программные средства
РД – руководящие документы
СЗИ – система защиты информации
СУБД – система управления базами данных
ТЗИ – техническая защита информации
ТС – техническое средство
ФАПСИ – Федеральное Агентство Правительственной Связи и Информации
ФСТЭК – Федеральная служба по техническому и экспортному контролю

Введение

Важнейшим ресурсом современного общества является информация, проблема защиты которой весьма актуальна как для различных стран, сообществ и организаций, так и для каждого человека в отдельности. Острота и важность защиты информации определяется следующими факторами:

– повышением важности и общественной значимости информации, усилением ее влияния на все без исключения стороны общественной жизни;

– увеличением объемов информации, накапливаемой, хранимой и обрабатываемой с помощью средств вычислительной техники (ВТ);

– усложнением режимов функционирования технических средств обработки информации (внедрением мультипрограммного режима и режима разделения времени);

– сосредоточением в единых банках данных информации различного назначения и принадлежности;

– резким увеличением числа пользователей, имеющих непосредственный доступ к информационным ресурсам и массивам данных;

– совершенствованием способов доступа к информации и интенсификацией информационного обмена между пользователями;

– многообразием и расширением круга угроз и каналов несанкционированного доступа (НСД) к информации.

Финансовые потери в результате каждого электронного преступления оцениваются специалистами от 100 - 400 тыс. до 1,5 млн. дол. Аналитиками были выделены следующие общие тенденции развития рынка компьютерных преступлений в 2010 году:

– увеличение степени профессионализации его участников;

– расширение рынка за счет появления новых участников и, как следствие, снижение цен на востребованные услуги;

– рост внутреннего рынка киберпреступности, охватывающего так называемые услуги Cybercrime to Cybercrime (C2C), когда хакеры оказывают услуги своим же коллегам;

– направленность на сверхмонетизацию, т.е. получение сверхприбыли.

Приведенный рисунок иллюстрирует тенденции роста доходов хакеров в России.

По мнению экспертов компании Group-IB, за 2010 год основными угрозами со стороны хакеров стали:

– галопирующий рост количества и сложности DDoS-атак (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»);

– направленные атаки на финансовый сектор;

– резкий всплеск случаев смс-мошенничества на территории стран СНГ;

– использование приемов социальной инженерии в целях хищения персональной информации и интернет-мошенничества;

– целевые атаки на объекты критической инфраструктуры.

Компьютерные преступления совершают, как правило, люди с незапятнанной репутацией и хорошо владеющие тонкостями информационных технологий (ИТ), что затрудняет их раскрытие. Сотрудник компании Прайм компьютер инкорпорейтед Дик Гилмет сформулировал правило 10-10-80, в соответствии с которым:

– 10% людей - никогда не совершают преступлений (краж);

– 10% - людей - совершают их при каждом удобном случае;

– 80% - не совершают краж, кроме случаев, когда есть такая возможность и гарантия безнаказанности.

В Приложении к учебному пособию приведены уголовные наказания за совершение преступлений в сфере компьютерной информации, предусмотренные главой 28-ой УК РФ, а также подробная классификация компьютерных преступлений по кодификатору Интерпола.

Преступления в сфере компьютерной информации – это своеобразная плата за прогресс в информационной и технической сферах. С ростом совершенства компьютерной техники возрастает изощренный характер компьютерной преступности. Опасность несанкционированных, злоумышленных действий в вычислительных средствах и системах является весьма реальной.

Соответственно должны совершенствоваться способы борьбы с этим видом преступлений, которые должны носить системный характер, а также учитывать причины и условия совершения преступлений данного вида.

Всё это обуславливает необходимость углубленного изучения принципов организации комплексных систем защиты информации (КСЗИ); способов анализа и оценки угроз безопасности информации; критериев и условий отнесения информации к защищаемой по видам тайн и степеням конфиденциальности и др.

1. Основные понятия, термины и определения

Основные понятия в области обеспечения безопасности информации определены в ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения (взамен ГОСТ Р 50922-96).

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от их формы и представления.

Данные – факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации.

Защита информации (ЗИ) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Формы защиты информации:

правовая – ЗИ правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по ЗИ, применение этих документов (актов), а также надзор и контроль за их исполнением.

техническая (ТЗИ) – ЗИ, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

криптографическая – ЗИ с помощью ее криптографического преобразования.

физическая – ЗИ путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Организационные мероприятия по обеспечению физической ЗИ предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К *объектам ЗИ* могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Способ ЗИ – порядок и правила применения определенных принципов и средств защиты информации.

Различают защиту информации от:

утечки – ЗИ, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

несанкционированного воздействия – ЗИ, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

непреднамеренного воздействия – ЗИ, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств ИС, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

разглашения – ЗИ, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

несанкционированного доступа (НСД) – ЗИ, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

преднамеренного воздействия – ЗИ, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

[иностранной] разведки – ЗИ, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Замысел ЗИ – основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Цель ЗИ – выявление, предотвращение, нейтрализация, пресечение, локализация, отражение и уничтожение угроз.

Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Система защиты информации – совокупность органов и/или исполнителей, используемой ими техники ЗИ, а также объектов ЗИ, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области ЗИ.

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Угрозы проявляются в нарушении:

– конфиденциальности (разглашение, утечка, НСД),

– достоверности (фальсификация, подделка, мошенничество),

– целостности (искажения, ошибки, потери),

– доступности (нарушение связи, воспрещение получения) информации.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации**.**

Аудиторская проверка (*аудит)* **ИБ в организации** – периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению ИБ.

Аудит ИБ в организации может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит).

Мониторинг безопасности информации – постоянное наблюдение за процессом обеспечения безопасности информации в ИС с целью установить его соответствие требованиям безопасности информации.

2. Виды и свойства защищаемой информации

К защищаемой информации относят:

– секретные сведения, содержащие государственную тайну;

– конфиденциальную информацию, содержащую коммерческую тайну;

– персональные данные о личной жизни или деятельности граждан.

Таким образом, под защищаемой информацией понимают сведения, использование и распространение которых ограничены их собственниками, т.е. субъектами информационных отношений.

Под *субъектами* информационных отношений понимают:

– государство в целом или его отдельные органы и организации;

– общественные или коммерческие организации и предприятия (юридические лица);

– отдельные лица (физические лица).

В процессе работы субъекты производственно-хозяйственных отношений вступают друг с другом в информационные отношения, связанные с получением, хранением, обработкой, распределением и использованием информации и рассчитывают при этом на соблюдение своих законных прав и интересов.

Различные субъекты по отношению к определенной информации могут выступать в качестве: источников, пользователей, собственников (владельцев) информации; физических и юридических лиц; владельцев систем сбора и обработки информации, а также участников процессов обработки и передачи информации и т.д.

Для удовлетворения законных прав и интересов субъектов информационных отношений необходимо постоянно поддерживать следующие основные свойства информации: *доступность*, *целостность* и *конфиденциальность*.

Доступность информации – возможность за разумное время получить требуемую информационную услугу при наличии соответствующих полномочий;

Целостность информации – неизменность вида и качества информации в условиях случайных или преднамеренных искажений или разрушающих воздействий;

Конфиденциальность информации – известность информации только прошедшим проверку (авторизованным) субъектам.

В случае нарушения этих свойств, субъектам информационных отношений может быть нанесен значительный материальный или моральный ущерб.

Защищаемую информацию можно классифицировать по трем основным признакам: 1) принадлежности; 2) степени секретности; 3) содержанию.

Признак принадлежности определяет собственников (владельцев) защищаемой информации, которыми могу быть:

– государство и его структуры. В этом случае к защищаемой информации относятся сведения, представляющие собой государственную или служебную тайну (в их числе могут быть и сведения, являющиеся коммерческой тайной);

– предприятия, акционерные общества, товарищества и другие образования, обладающие сведениями, составляющими коммерческую тайну;

– общественные организации (партии, фонды, партнерства), в которых также может существовать государственная или коммерческая тайна;

– граждане государства, заинтересованные в сохранении тайны переписки; телефонных и телеграфных сообщений; врачебной и семейной тайн и др.

Признак степени секретности подразделяет защищаемую информацию по уровням ее важности и секретности для собственника.

По уровню *важности* информация может быть:

– жизненно важная незаменимая информация, наличие которой необходимо для функционирования организации;

– важная – информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами;

– полезная – информация, которую трудно восстановить, однако организация может эффективно существовать и без нее;

– несущественная – информация, которая больше не нужна организации.

На практике отнесение информации к одной из категорий важности осложняется субъективизмом в ее оценке. Важность информации, как и ее ценность, обычно изменяется со временем и зависит от степени отношения к ней различных групп потребителей и потенциальных нарушителей.

Ценность информации может рассматриваться с 2-х позиций: ценность для получателя по отношению к будущей прибыльности (потребительская ценность) и ценность с точки зрения понесенных затрат. Информация, в отличие от товара, при передаче остается у источника (продавца).

По уровню *секретности* информация может быть: особой важности, совершенно секретной, секретной, для служебного пользования, несекретной.

Признак содержания позволяет подразделять защищаемую информацию на политическую, экономическую, военную, разведывательную (контрразведывательную), научно-техническую, технологическую, деловую и коммерческую.

3. Факторы, воздействующие на защищаемую информацию

Под факторами, воздействующими на защищаемую информацию, подразумевают явления, действия или процессы, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации или блокирование доступа к ней.

Различают объективные и субъективные факторы и в каждом классе выделяют внешние и внутренние факторы. Подробный перечень факторов можно найти в ГОСТ Р 51275-2006 (взамен ГОСТ Р 51275-99) [6], который распространяется на требования по организации ЗИ при создании и эксплуатации объектов информатизации, используемых в различных областях деятельности (обороны, экономики, науки и других областях).

Значение некоторых используемых терминов:

побочное электромагнитное излучение – излучение, возникающее при работе технических средств обработки информации;

паразитное электромагнитное излучение – излучение, вызванное паразитной генерацией в электрических цепях технических средств обработки информации;

«*маскарад*» – маскировка под зарегистрированного пользователя.

В приведенной ниже таблице перечислены наиболее существенные факторы, воздействующие на защищаемую информацию.

Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на ЗИ на ОИ.

Полнота и достоверность выявленных факторов достигаются путем рассмотрения полного множества факторов, воздействующих на все элементы ОИ (технические и программные средства обработки информации, средства обеспечения ОИ и т.д.) и на всех этапах обработки информации.

Выявление факторов, воздействующих на защищаемую информацию, должно осуществляться с учетом следующих требований:

- достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющих формировать их полное множество;

- гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры классификации.

Факторы, воздействующие на защищаемую информацию		
Объективные	*Внутренние*	Передача сигналов по проводным и оптико-волоконным линиям связи Излучения акустических, речевых и неречевых сигналов Излучения в радио- и оптическом диапазонах Побочное и паразитное электромагнитные излучения Различные наводки Дефекты, сбои, отказы, аварии ТС, систем и ПО
	Внешние	Явления техногенного характера. Электромагнитные и радиационные облучения Сбои, отказы и аварии систем обеспечения ОИ Природные явления, стихийные бедствия Термические (пожары и т.д.) Климатические (наводнения и т.д.) Механические (землетрясения и т.д.) Электромагнитные (грозовые разряды и т.д.) Биологические (микробы, грызуны и т.д.) Химические факторы (химически агрессивные среды и т.д.)
Субъективные	*Внутренние*	Разглашение информации, опубликование в СМИ Передача, утрата, хищение, копирование носителей информации Несанкционированные доступ, изменение, копирование Несанкционированное использование ПО («маскарад», использование дефектов, применение вирусов) Неправильная организация ЗИ (ошибки в задании требований, в организации контроля, несоблюдение требований) Ошибки обслуживающего персонала (при эксплуатации ТС/ПС/средств и систем ЗИ)
	Внешние	Доступ к защищаемой информации с применением технических средств *разведки* (радио- и оптико-электронной, фото, визуальной, гидроакустической, компьютерной) и *съема информации* Несанкционированное подключение к ТС и системам Использование ПО ТС ОИ («маскарад», использование дефектов, применение вирусов) Несанкционированный физический доступ на ОИ, хищение носителя Блокирование доступа к защищаемой информации Преступные действия и диверсии в отношении ОИ

4. Сущность и задачи комплексной системы защиты информации

Современные предприятия представляют собой сложные системы. Их отличительными особенностями являются: сложная организационная структура; многофункциональность; высокая техническая оснащённость; большие объемы поступающей информации, требующие современных методов передачи, хранения и обработки; обширные внешние связи; работа в условиях самых разнообразных угроз информационной безопасности.

Обеспечение безопасности функционирования таких предприятий требует привлечения всего арсенала имеющихся средств защиты во всех структурных подразделениях производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект может быть достигнут только в том случае, когда все используемые средства, методы и меры объединяются в единый целостный механизм – комплексную систему защиты информации. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

Комплексная система защиты информации (КСЗИ) – это совокупность организационно-правовых и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа.

Организационно-правовые мероприятия включают в себя создание концепции информационной безопасности, а также:

– составление должностных инструкций для пользователей и обслуживающего персонала;

– создание правил администрирования компонент информационной системы, учета, хранения, размножения, уничтожения носителей информации, идентификации пользователей;

– разработку планов действий в случае выявления попыток несанкционированного доступа к информационным ресурсам системы, выхода из строя средств защиты, возникновения чрезвычайной ситуации;

–обучение правилам информационной безопасности пользователей.

В случае необходимости, в рамках проведения организационно-правовых мероприятий может быть создана служба информационной безопасности, режимно-пропускной отдел, проведена реорганизация системы делопроизводства и хранения документов.

Инженерно-технические мероприятия – это совокупность специальных технических средств и их использование для защиты информации. Выбор инженерно-технических мероприятий зависит от уровня защищенности информации, который необходимо обеспечить.

Инженерно-технические мероприятия, проводимые для защиты информационной инфраструктуры организации, могут включать использование защищенных подключений, межсетевых экранов, разграничение потоков информации между сегментами сети, использование средств шифрования и защиты от несанкционированного доступа.

В случае необходимости, в рамках проведения инженерно-технических мероприятий, может осуществляться установка в помещениях систем охранно-пожарной сигнализации, систем контроля и управления доступом. Отдельные помещения могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

Комплексный (системный) подход – это принцип рассмотрения проекта, при котором анализируется система в целом, а не ее отдельные части. Его задача – оптимизация всей системы.

Комплексный подход к построению любой системы включает в себя:

– постановку задачи (проблемы): определение объекта исследования, постановку целей, задание критериев для изучения объекта и управления им;

– очерчивание границ изучаемой системы и ее первичную структуризацию. На этом этапе вся совокупность объектов и процессов, имеющих отношение к поставленной цели, разбивается на два класса – собственно изучаемая система и внешняя среда как источник угроз безопасности;

– составление математической модели изучаемой системы: параметризация системы, задание области определения параметров, установление зависимостей между введенными параметрами;

– исследование построенной модели: прогноз развития изучаемой системы на основе ее модели, анализ результатов моделирования, оценку экономической целесообразности;

– выбор оптимального управления для приведения системы в желаемое (целевое) состояние.

Задачи КСЗИ

Основными задачами, которые должны решаться комплексной системой защиты информации, являются:

– управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (с превышением предоставленных полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации и пользователей;

– защита данных, передаваемых по каналам связи;

– регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;

– контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;

– контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

– обеспечение замкнутой среды проверенного ПО с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

– управление средствами системы защиты.

5. Принципы организации КСЗИ

Построение современных систем защиты информации и их функционирование должны осуществляться в соответствии со следующими принципами [15, 21, 26]:

– *законность*: предполагает осуществление защитных мероприятий и разработку системы безопасности информации АС организации в соответствии с действующим законодательством;

– *системность*: системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для понимания и решения проблемы обеспечения безопасности информации;

– *комплексность*: комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на

стыках отдельных ее компонентов, защита должна строиться эшелонировано. Принцип эшелонированной (многоуровневой) защиты предполагает создание ряда последовательных уровней защиты, что обеспечивает ограничение в рамках каждого уровня (эшелона) последствий вероятных отказов ТС и ошибок персонала;

– *централизованность управления*: связана с необходимостью проведения единой политики в области безопасности информационных ресурсов;

– *унифицированность*: использование стандартных компонент при создании блочной архитектуры КСЗИ;

– *непрерывность* защиты: непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС;

– *своевременность*: предполагает упреждающий характер мер для обеспечения безопасности информации;

– *преемственность* и совершенствование: предполагают постоянное совершенствование мер и средств защиты информации по мере совершенствования информационных технологий и увеличения числа пользователей;

– *разумная достаточность* (экономическая целесообразность): предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба;

– *персональная ответственность*: предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий;

– *минимизации полномочий*: означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью;

– *гибкость системы защиты*: для обеспечения возможности варьирования уровня защищенности при изменении внешних условий и требований с течением времени средства защиты должны обладать определенной гибкостью;

– *открытость алгоритмов и механизмов защиты*: суть данного принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна;

– *простота применения средств защиты:* механизмы защиты должны быть интуитивно понятны и просты в использовании, без привлечения значительных дополнительных трудозатрат;

– *научная обоснованность и техническая реализуемость*: информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации;

– *обязательность контроля*: предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности;

– *специализация и профессионализм*: предполагает привлечение к разработке средств и реализаций мер защиты информации специализированных организаций, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами;

– *взаимодействие и сотрудничество*: предполагает создание благоприятной атмосферы в коллективах подразделений;

– *дружественность интерфейса*: для обеспечения удобства использования на уровне ассоциативного мышления пользователя.

6. Роль системного подхода в создании КСЗИ

Сущность системного подхода состоит в том, что объект проектирования или управления рассматривается как система, т.е. как единство взаимосвязанных элементов, которые образуют единое целое и действуют в интересах реализации единой цели. Системный подход требует рассматривать каждый элемент системы во взаимосвязи и взаимозависимости с другими элементами, вскрывать закономерности, присущие данной конкретной системе, выявлять оптимальный режим ее функционирования. Прежде всего, системный подход проявляется в попытке создать целостную картину исследуемого или управляемого объекта. Исследование или описание отдельных элементов при этом не является определяющим, а производится с учетом роли и места элемента во всей системе.

ЗИ представляет собой реализацию регулярного процесса, осуществляемого на всех этапах жизненного цикла систем обработки информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для ЗИ, наиболее рациональным образом объединяются в единый целостный механизм.

На основе теоретических исследований и практических работ в области ЗИ сформулирован системно-концептуальный подход к защите информации, в котором определяется системность:

– *целевая*, т.е. защищенность информации рассматривается как составная часть общего понятия качества информации. Качество информации – совокупность свойств, отражающих степень пригодности конкретной информации для достижения определенных целей и решения конкретных задач, стоящих перед пользователем;

– *пространственная*, предполагающая взаимоувязанное решение всех вопросов защиты во всех компонентах отдельно взятой АСОД, во всех АСОД учреждения (заведения, ведомства), расположенных на некоторой территории;

– *временная*, означающая непрерывность работ по защите информации, осуществляемых по взаимоувязанным планам;

– *организационная*, означающая единство организации всех работ по защите информации и управления их осуществлением.

Учитывая все вышесказанное можно сформулировать четыре пункта постулата системы защиты:

1) система ЗИ может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты, сочетающая в себе такие направления защиты, как правовая, организационная и инженерно-техническая;

2) никакая система ЗИ не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты;

3) никакую систему защиты нельзя считать абсолютно надежной, т.к. всегда может найтись злоумышленник, который найдет лазейку для доступа к информации (действия злоумышленника всегда носят комплексный характер, т.к. он любыми средствами стремится добыть важную информацию);

4) система защиты должна быть адаптируемой (приспосабливающейся) к изменяющимся условиям.

Центральным звеном методологии системного подхода является определение целей. Проектировщикам важно четко представлять себе, что требуется от будущей системы, какие результаты необходимо получить. Поэтому необхо-

димо иметь определенный набор требований к системе, и прежде всего, четко сформулированную цель проектирования.

7. Требования к КСЗИ

С позиций системного подхода для реализации приведенных выше принципов система защиты информации должны отвечать некоторой совокупности требований [28 ,34, 35].

Защита информации должна быть:

эффективной – обеспечивать выполнение АС своих основных функций без существенного ухудшения характеристик последней;

централизованной – необходимо иметь в виду, что процесс управления всегда централизован, в то время как структура системы, реализующей этот процесс, должна соответствовать структуре защищаемого объекта;

плановой – планирование осуществляется для организации взаимодействия всех подразделений объекта в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;

конкретной и целенаправленной – защите подлежат абсолютно конкретные информационной ресурсы, могущие представлять интерес для конкурентов;

активной – защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом “обнаружить и устранить” принцип “предвидеть и предотвратить”;

надежной и универсальной – охватывать весь технологический комплекс информационной деятельности объекта; методы и средства защиты должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам НСД независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;

нестандартной (по сравнению с другими организациями), разнообразной по используемым средствам;

открытой для изменения, дополнения и совершенствования мер обеспечения безопасности информации в соответствии с условиями эксплуатации и конфигурации защищаемого объекта;

экономически целесообразной – затраты на систему защиты не должны превышать размеры возможного ущерба.

Наряду с основными требованиями существует ряд устоявшихся рекомендаций, которые будут не бесполезны создателям КСЗИ:

– средства защиты должны быть просты для технического обслуживания и “прозрачны” для пользователей;

– применение системы защиты не должно ухудшать экологическую обстановку, не вызывать психологического противодействия и желания обойтись без нее;

– каждый пользователь должен иметь минимальный набор привилегий, необходимых для работы и строго соблюдать установленные правила разграничения доступа;

– возможность отключения защиты в особых случаях, например, когда механизмы защиты реально мешают выполнению работ;

– независимость системы защиты от субъектов защиты;

– разработчики должны предполагать, что пользователи имеют наихудшие намерения (враждебность окружения), что они будут совершать серьезные ошибки и искать пути обхода механизмов защиты;

– отсутствие на предприятии излишней информации о существовании механизмов защиты.

8. Обобщенная модель защищенной системы

Системы защиты информации существовали уже в глубокой древности. В те далекие времена особое внимание уделялось организационным методам защиты: контроль доступа на территорию; применение наказаний к нарушителям; использование закрытых мест для тайных совещаний и декорирование их особыми растениями, реагирующими на яды; выбор надёжных участников и ограничение их количества; применение криптографии; многорубежная структура – несколько охраняемых периметров.

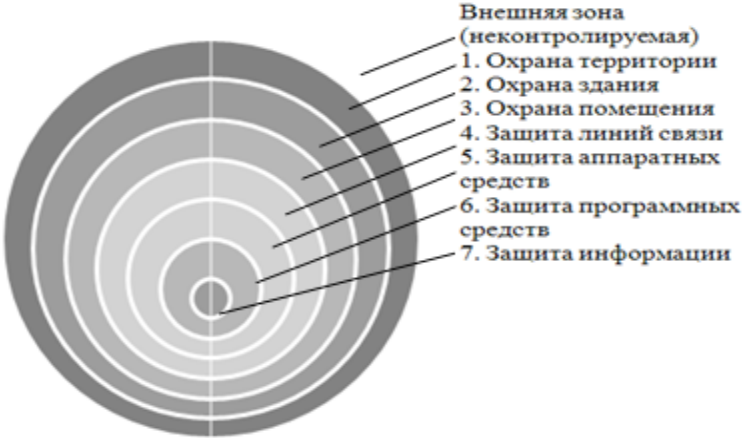
В современных условиях комплексная система защиты информации также должна иметь несколько уровней защиты, перекрывающих друг друга [26]. Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни.

На каждом рубеже угрозы нарушению безопасности должны быть обнаружены и по возможности ликвидированы, а в случае невозможности ликвида-

ции, их распространению должны препятствовать последующие рубежи. При этом, чем сложнее защита каждого рубежа, тем больше времени потребуется злоумышленнику для его преодоления и тем вероятнее его обнаружение. Из этого следует, что защита каждого рубежа должна взаимно дополнять друг друга и эффективность всей системы защиты будет оцениваться как минимальное время, которое злоумышленник должен затратить на преодоление всех её рубежей. За это время (безопасное время) он должен быть обнаружен и обезврежен сотрудниками службы безопасности.

Количество и пространственное расположение зон и рубежей выбираются таким образом, чтобы обеспечить требуемый уровень безопасности защищаемой информации, как от внешних, так и внутренних злоумышленников и сотрудников. Чем более ценной является защищаемая информация, тем большим количеством рубежей и зон целесообразно окружать ее источник и тем сложнее злоумышленнику обеспечить разведывательный контакт с ее носителями.

Модель КСЗИ подразумевает наличие внешней неконтролируемой зоны – территории вокруг АСОД, на которой персоналом и средствами АСОД не применяются никакие средства, и не осуществляется никакие мероприятия для ЗИ. Кроме того, в модели КСЗИ можно выделить следующие зоны (рубежи, барьеры) защиты:



1) территория, занимаемая организацией;

2) здание (здания) на территории, в котором расположена (расположены) АСОД;

3) помещения внутри здания, в которых расположены ресурсы автоматизированных систем и защищаемая информация. Это могут быть: служебные помещения, кабинеты, комнаты для переговоров, залы, технические помещения, склады, сейфы, шкафы и др.;

4) линии (каналы) связи и источники питания, находящиеся как в пределах одного и того же здания, так и проходящие между различными зданиями на охраняемой территории и выходящие за пределы объекта. Например, соедине-

ния с Интернетом должны защищаться межсетевыми экранами (брандмауэрами) для предотвращения удалённого доступа через сеть;

5) аппаратные средства (терминалы пользователей, устройства ввода-вывода данных, центральные процессоры, аппаратные средства шифрования и дешифрования данных, внешние запоминающие устройства, устройства уничтожения информации, другое периферийное оборудование;

6) программные средства, в том числе операционная система и специальные программы, осуществляющие функции защиты и тестовый контроль механизма защиты в КСЗИ;

7) файлы и данные (включая бумажную информацию).

Для каждой из приведенных выше зон возможны четыре степени защиты информации:

– *предотвращение* - доступ к информации и технологии имеет только персонал, который получил допуск от собственника информации;

– *обнаружение* - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;

– *ограничение* - уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению;

– *восстановление* - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

9. Концепция информационной безопасности

Под *Концепцией информационной безопасности* (далее – Концепция) понимается взаимоувязанный комплекс организационно-технических мер, методологических указаний, регламентов, комплектов форм типовых документов и т.д., решающих задачи защиты конфиденциальной информации.

В автоматизированной системе организации Концепция определяет систему взглядов на проблему обеспечения безопасности информации организации, и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации.

Основные положения и требования Концепции распространяются на все структурные подразделения организации, в которых осуществляется автомати-

зированная обработка информации, подлежащей защите, а также сопровождение, обслуживание и обеспечение нормального функционирования АС.

Правовой основой Концепции должны являться Конституция РФ, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы, документы Гостехкомиссии при Президенте РФ, ФАПСИ и другие нормативные документы, регламентирующие вопросы ЗИ в АС.

При разработке Концепции должны учитываться основные принципы создания КСЗИ, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Положения Концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в АС двух относительно самостоятельных направлений, объединенных единым замыслом:

– защита информации от утечки по техническим каналам;

– защита информации в АС от несанкционированного доступа.

В Концепции информационной безопасности должны быть отражены следующие вопросы:

– характеристика АС организации, как объекта информационной безопасности (объекта защиты):

• назначение, цели создания и эксплуатации АС организации,

• структура, состав и размещение основных элементов АС организации, информационные связи с другими объектами,

• категории информационных ресурсов, подлежащих защите,

• категории пользователей АС организации, режимы использования и уровни доступа к информации,

• интересы затрагиваемых при эксплуатации ас организации субъектов информационных отношений;

– уязвимость основных компонентов АС организации

• цели и задачи обеспечения информационной безопасности организации и основные пути их достижения (решения задач системы защиты)

– перечень основных опасных воздействующих факторов и значимых угроз информационной безопасности:

• внешние и внутренние воздействующие факторы, угрозы безопасности информации и их источники,

• пути реализации непреднамеренных субъективных угроз безопасности информации в АС организации,

• умышленные действия сторонних лиц, зарегистрированных пользователей и обслуживающего персонала,

• утечка информации по техническим каналам,

• неформальная модель возможных нарушителей

• подход к оценке риска в АС организации;

• основные положения технической политики в области обеспечения безопасности информации АС организации

• принципы обеспечения информационной безопасности организации;

• основные меры и методы (способы) защиты от угроз, средства обеспечения требуемого уровня защищенности ресурсов АС:

• организационные (административные) меры защиты,

• структура, функции и полномочия подразделения обеспечения информационной безопасности;

• физические средства защиты,

• технические (программно-аппаратные) средства защиты,

• управление системой обеспечения безопасности информации

• контроль эффективности системы защиты

• первоочередные мероприятия по обеспечению безопасности информации АС организации

• перечень нормативных документов, регламентирующих деятельность в области защиты информации

• основные термины и определения.

10. Этапы разработки и жизненный цикл КСЗИ

КСЗИ относятся к классу сложных систем. Поэтому при их построении могут использоваться основные типовые этапы построения сложных систем с учетом специфики решаемых задач.

В зависимости от особенностей компьютерной системы, условий ее эксплуатации и требований к защите информации процесс создания КСЗИ может не содержать отдельных этапов, или их содержание может несколько отличаться от общепринятых норм при разработке сложных аппаратно-программных систем [4, 19, 20, 27].

Разработка конкретной КСЗИ может включать следующие этапы:

1. Проведение предварительного обследования состояния объекта и организации защиты информации. Определение факторов, анализ условий и осуществление выбора и обоснования требований по защите информации на заданном объекте. На стадии обследования организации:

– изучается состав защищаемой информации и объекты защиты;

– устанавливается наличие секретной (конфиденциальной) информации в разрабатываемой КСЗИ, оценивается уровень конфиденциальности и объемы;

– определяются режимы обработки информации (диалоговый, телеобработки и режим реального времени), состав комплекса технических средств, общесистемные программные средства и т.д.;

– анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;

– определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;

– определяются мероприятия по обеспечению режима секретности на стадии разработки.

2. Определение функций защиты, обеспечивающих требуемый уровень в потенциально возможных условиях функционирования объекта.

3. Выявление потенциально возможных угроз информации и вероятностей их появления. Формирование на их основе модели угроз и определение уровня возможного ущерба (незначительный, малый, средний, большой, очень большой и т.п.) и соответствующего уровня требований к защищенности.

При определении уровня наносимого ущерба необходимо учитывать:

• стоимость возможных потерь при получении информации конкурентом;

• стоимость восстановления информации при ее утрате;

• затраты на восстановление нормального процесса функционирования АС и т.д.

4. Составление модели потенциально возможных нарушителей. Потенциальными правонарушителями прежде всего могут быть сотрудники организации, имеющие значительные материальные затруднения; склонные к азартным играм, к пьянству, наркотической зависимости; имеющие тяжело больных близких родственников; часто меняющие место работы; психически неуравновешенные.

5. Выявление каналов утечки защищаемой информации и определение возможностей и основных каналов НСД к защищаемой информации.

6. Формулирование стратегии КСЗИ (оборонительная, наступательная, упреждающая).

7. Разработка политики безопасности, организационно-распорядительных документов и мероприятий по обеспечению ИБ. Обоснование перечня задач защиты информации, их классификации и эффективности их реализации с точки зрения предотвращения возможных сбоев АС.

8. Обоснование структуры и технологии функционирования КСЗИ. Определение состава технического, математического, программного, информационного и лингвистического обеспечения, нормативно-методических документов и организационно-технических мероприятий по защите информации.

9. Моделирование КСЗИ.

10. Проектирование КСЗИ.

11. Тестирование КСЗИ. Проверяется реакция системы в целом и отдельных ее компонентов на возможные отказы:

– отдельного компонента;

– группы компонентов;

– основных модулей;

– «жесткий» сбой (отказ питания).

12. Внедрение КСЗИ. Определение эффективности защиты информации с помощью оценки степени ее защищенности. Сравнение полученных результатов с их требуемыми значениями и анализ стоимостных затрат на обеспечение защиты.

13. Корректировка, уточнение, внесение необходимых изменений.

14. Подготовка и передача технической и эксплуатационной документации. Обучение пользователей правилам работы с КСЗИ;

15. Эксплуатация КСЗИ и сопровождение. Постоянный мониторинг состояния защищенности информационных ресурсов и выработка предложений по ее совершенствованию. Периодический пересмотр следующих положений политики безопасности:

– эффективность политики, определяемая по характеру, числу и воздействию зарегистрированных инцидентов, касающихся безопасности;

– стоимости средств обеспечения безопасности на показатели эффективности функционирования КС;

– влияние изменений на безопасность технологии.

Развитие КСЗИ во времени отражает такая категория, как жизненный цикл (ЖЦ) – одно из базовых понятий методологии проектирования ИС.

Жизненный цикл КСЗИ – это непрерывный процесс, который начинается с момента принятия решения о необходимости создания системы и заканчивается в момент ее полного изъятия из эксплуатации (обычно в результате морального устаревания).

Процесс создания и сопровождения системы представляется как некоторая последовательность этапов и выполняемых на них процессов. Для каждого этапа определяются состав и последовательность выполняемых работ, получаемые результаты, методы и средства, необходимые для выполнения работ, роли и ответственность участников и т.д. Такое формальное описание ЖЦ позволяет спланировать и организовать процесс коллективной разработки и обеспечить управление этим процессом.

В жизненном цикле выделяют следующие стадии: 1) разработка требований; 2) проектирование; 3) реализация и тестирование; 4) внедрение; 5) сопровождение.

Жизненный цикл носит итеративный характер: реализованные этапы ЖЦ, начиная с самих ранних, циклически повторяются в соответствии с новыми требованиями и изменениями внешних условий. На каждом этапе ЖЦ формируется набор документов и технических решений, которые являются исходными для последующих решений.

Наибольшее распространение получили три модели ЖЦ:

– *каскадная* модель, в которой переход на следующий этап означает полное завершение работ на предыдущем этапе. Основным недостатком этого подхода является существенное запаздывание с получением результата;

– *поэтапная* модель с промежуточным контролем - итерационная модель разработки системы с циклами обратных связей между этапами, допускающие возвраты к предыдущему этапу. В результате каждый из этапов может растянуться на весь период разработки;

– *спиральная* модель, в которой каждый виток спирали соответствует созданию работоспособного фрагмента или версии системы. Это позволяет уточнить требования, цели и характеристики проекта, определить качество разработки, спланировать работы следующего витка спирали и в результате выбрать оптимальный вариант системы, удовлетворяющий требованиям заказчика, и довести его до реализации. Основная проблема – определение момента перехода на следующий этап.

11. Определение и нормативное закрепление состава защищаемой информации

Необходимым условием при создании КСЗИ на предприятии является определение состава защищаемой информации.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации.

В соответствии со ст. 5 Федерального закона от 27 июля 2006 г. N 149-ФЗ. "Об информации, информационных технологиях и о защите информации" информация подразделяется на:

– свободно распространяемую;

– предоставляемую по соглашению сторон;

– подлежащую предоставлению или распространению по закону;

– имеющую статус ограниченного или запрещенного доступа.

Отнесение информации к защищаемой определяется следующими нормативно-правовыми актами:

1. ФЗ РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне" (ред. от 01.12.2007).

2. ФЗ РФ от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне».

3. ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».

4. ФЗ РФ от 2 декабря 1990 г. N 395-I "О банках и банковской деятельности" (ред. от 7 февраля 2011 г.).

5. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера" (в ред. от 23.09.2005). В соответствии с этим Перечнем к *профессиональной тайне* относят: врачебную, нотариальную, адвокатскую тайну, тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д. Необходимость соблюдения перечисленных тайн вытекает из доверительного характера отдельных профессий.

Основная особенность *служебной тайны* заключается в том, что обязанность ее соблюдения вытекает из интересов службы: служебные сведения, военная и судебная тайны, тайна следствия и т.п.

Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в Уставе (учредительном договоре) в виде следующих положений:

– предприятие имеет право определять состав, объем, сроки и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;

– предприятие обязано обеспечить сохранность конфиденциальной информации.

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение ИБ. К таким документам относятся:

– Положение о сохранении конфиденциальной информации;

– Перечень сведений, составляющих конфиденциальную информацию;

– Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;

– Обязательство сотрудника о сохранении конфиденциальной информации;

– Положение о специальном делопроизводстве и документообороте;

– Перечень сведений, разрешенных к опубликованию в открытой печати;

– Положение о работе с иностранными фирмами и их представителями;

– Памятка сотруднику о сохранении коммерческой тайны.

Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). Трудовой договор – это правовая основа к тому, чтобы пресечь неверные или противоправные действия работника

Кроме того, на каждом предприятии постепенно накапливается коммерчески ценная информация, которая позволяет предприятию успешно работать и противостоять конкурентам. Условно эту информацию разделяют на:

– производственные секреты (научно-технические, технологические, организационные);

– деловые секреты (ноу-хау): знаю, какой товар надо делать, знаю, как его делать, знаю, как продвигать на рынке и продавать этот товар, и т.п.

Сведения, составляющие коммерческую тайну предприятия, ***должны***:

– являться собственностью предприятия;

– иметь действительную или потенциальную коммерческую ценность;

и ***не должны***:

– являться общеизвестными и общедоступными;

– являться открытыми, защищаемыми на законных основаниях;

– относиться к составляющим государственную тайну;

– иметь ограничений на отнесение сведений на законном основании к коммерческой тайне (КТ);

– использовать открыто сведения, разглашение которых может нанести предприятию ущерб.

Кроме того, при принятии решения о включении сведений в перечень рекомендуется учитывать следующие факторы:

– величину ущерба о разглашения информации;

– преимущества открытого использования информации;

– величину затрат на защиту информации.

Для формирования перечня сведений, составляющих коммерческую тайну, необходимо:

1. Разработать приказ (план) по организации работы по формированию перечня.

2. Сформировать и утвердить список лиц (рабочую группу), наделяемых полномочиями по отнесению сведений к коммерческой тайне.

3. Создать и утвердить состав экспертной комиссии для анализа предварительного и формирования окончательного перечня, периодического его обновления и экспертизы документов, подготавливаемых к открытой печати, на предмет выявления и изъятия сведений, составляющих КТ.

4. Разработать положение о порядке формирования перечня – методическое руководство для руководителей структурных подразделений, членов рабочей группы и экспертной комиссии.

5. Разослать положение руководителям структурных подразделений и членам экспертной комиссии для ознакомления и подготовки замечаний.

6. Согласовать и утвердить положение.

7. Разослать положение исполнителям и провести инструктаж членов рабочей группы и экспертной комиссии.

8. Внести в предварительный перечень предложения членов рабочей группы.

9. Членам экспертной комиссии рассмотреть предварительный перечень в соответствии с положением и сформировать проект окончательного варианта.

10. Согласовать перечень с руководителями структурных подразделений и утвердить руководителем предприятия.

12. Издать приказ о введении перечня в действие.

12. Определение объектов защиты

Объект защиты – это информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту от нежелательного несанкционированного вмешательства, а также от попыток хищения, незаконной модификации и/или разрушения.

В соответствии с семирубежной моделью ЗИ при организации КСЗИ на предприятии в качестве объектов защиты рассматриваются:

1) прилегающая к предприятию территория;

2) здания предприятия;

3) рабочие помещения и помещения, предназначенные для обработки информации с ограниченным доступом; помещения, предназначенные для ведения переговоров, в ходе которых оглашаются сведения ограниченного доступа; хранилища носителей информации;

4) физические поля (электромагнитные, оптические, ультрафиолетовые, инфракрасные, рентгеновские и др.); системы, линии и средства связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом;

5) аппаратные средства (серверы, рабочие станции, периферийное оборудование), средства и системы информатизации и другие технические средства защиты информации;

6) программные средства (операционные системы, специальное ПО, СУБД, интерфейсное и сетевое ПО);

7) информационные ресурсы, содержащие конфиденциальную информацию (в частности персональные данные); сведения, отнесенные любому виду тайн; носители информации и средства их транспортировки;

Кроме того, объектами защиты должны быть:

– средства отображения, обработки, воспроизведения и передачи конфиденциальной информации, в том числе: ЭВМ, средства видео-, звукозаписывающей и воспроизводящей техники;

– системы обеспечения функционирования предприятия (электро-, водоснабжение, кондиционирование и др.);

– выпускаемая продукция (конкретные изделия, предметы, технические решения) и технологические процессы ее изготовления и используемые при этом средства производства;

– сотрудники организации.

13. Анализ и оценка угроз безопасности информации

Под *угрозой безопасности* понимаются потенциально возможные воздействия, события, процессы или явления, которые прямо или косвенно могут нанести ущерб интересам субъектов информационных отношений.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в компьютерной системе (КС). С понятием угрозы безопасности тесно связано понятие уязвимости КС.

Уязвимость КС - это некоторое наиболее ранимое свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака - это реализация угрозы безопасности.

Основная *цель защиты* КС - противодействие угрозам безопасности.

По цели воздействия различают следующие основные *типы угроз безопасности*:

- нарушение конфиденциальности (раскрытие) информации;
- нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация);
- нарушение (частичное или полное) работоспособности системы. Вывод из строя или неправомерное изменение режимов работы компонентов системы обработки информации, их модификация или подмена могут приводить к получению неверных результатов расчетов, отказам системы от потока информации (непризнанию одной из взаимодействующих сторон факта передачи или приема сообщений) и/или отказам в обслуживании конечных пользователей;
- несанкционированное тиражирование открытой информации (не являющейся конфиденциальной), например, программ, баз данных, разного рода документации, литературных произведений и т.д. в нарушение прав собственников информации, авторских прав и т.п. Информация, обладая

свойствами материальных объектов, имеет такую особенность, как неисчерпаемость ресурса, что существенно затрудняет контроль за ее тиражированием.

Источники угроз безопасности

Основными ***источниками угроз безопасности*** КС и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т. п.);
- сбои и отказы оборудования (технических средств) КС;
- последствия ошибок проектирования и разработки компонентов КС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Естественные угрозы - это угрозы, вызванные воздействиями на КС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы КС, вызванные деятельностью человека. Среди искусственных угроз, исходя из мотивации действий, можно выделить:

- ***непреднамеренные (неумышленные, случайные) угрозы***, вызванные ошибками в проектировании КС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- ***преднамеренные (умышленные) угрозы***, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к КС могут быть внешними или внутренними (компоненты самой КС - ее аппаратура, программы, персонал).

13.1. Основные непреднамеренные искусственные угрозы

Основные непреднамеренные искусственные угрозы КС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) [3]:

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ре-

сурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при работе в системе;

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13) пересылка данных по ошибочному адресу абонента (устройства);

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

13.2. Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

3) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

4) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

5) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

10) несанкционированное копирование носителей информации;

11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

13) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

14) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора,

путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

16) вскрытие шифров криптозащиты информации;

17) внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

18) незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

19) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

13.3. Классификация угроз безопасности

Выше мы рассмотрели два основных класса потенциальных угроз по природе их возникновения: естественные и искусственные. Но наряду с этим угрозы можно классифицировать и по различным аспектам реализации, наиболее полно изложенным в [3, 24], и показывающим возможный спектр угроз безопасности КС.

Классификация угроз по цели:

- несанкционированное чтение информации,
- несанкционированное изменение информации,
- несанкционированное уничтожение информации,

полное или частичное разрушение КС (от кратковременного вывода из строя отдельных модулей до физического стирания системных файлов);

Классификация угроз по принципу воздействия на КС:

- использование легальных каналов получения информации (например, несанкционированное чтение из файла),
- использование скрытых каналов получения информации (например, недокументированных возможностей ОС),
- создание новых каналов получения информации (например, с помощью программных закладок).

Классификация угроз по характеру воздействия на КС:

- активное воздействие – несанкционированные действия в системе,
- пассивное воздействие – несанкционированное наблюдение за процессами в системе.

Классификация угроз по типу используемой слабости защиты:

- неадекватная политика безопасности (в том числе ошибки администратора),
- ошибки и недокументированные возможности ПО (так называемые «люки» - встроенные в систему специальные входы, предназначенные для тестирования или отладки, но случайно оставленные, что позволяет обходить систему защиты),
- ранее внедренные программные закладки.

Классификация угроз по способу воздействия на объект атаки:

- непосредственное превышение пользователем своих полномочий,
- работа от имени другого пользователя или перехват результатов его работы.

Классификация угроз по способу действий нарушителя (злоумышленника):

- в интерактивном режиме (вручную),
- в пакетном режиме (с помощью специальных программ, без участия пользователя).

Классификация угроз по используемым средствам атаки:

- штатные средства без использования дополнительного ПО,
- ПО третьих фирм (вирусы, вредоносные программы; ПО, разработанное для других целей – отладчики, сетевые мониторы и т. д.).

Классификация угроз по объекту атаки:

- аппаратные средства (оборудование),
- программное обеспечение,
- данные,
- персонал.

Возможные пути реализации угроз безопасности для перечисленных объектов атаки представлены в приведенной ниже таблице [3]:

Пути реализации угроз безопасности			
Объекты воздействия	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
Аппаратные средства	НСД - подключение; использование ресурсов; хищение носителей	НСД - подключение; использование ресурсов; модификация, изменение режимов	НСД - изменение режимов; вывод из строя: разрушение
ПО	НСД - копирование; хищение; перехват	НСД, внедрение "троянского коня", "вирусов", "червей"	НСД – искажение; удаление: подмена
Данные	НСД - копирование; хищение; перехват	НСД - искажение; модификация	НСД - искажение; удаление; подмена
Персонал	Разглашение; передача сведений о защите; халатность	"Маскарад": вербовка; подкуп персонала	Уход с рабочего места: физическое устранение

13.4. Источники, виды и способы дестабилизирующего воздействия на информацию

Определяющим признаком угрозы является ее направленность, результат, к которому может привести дестабилизирующее воздействие (ДВ) на информацию - нарушение ее статуса.

Таким образом, угроза защищаемой информации – это совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

К явлениям, т.е. сущностным проявлениям угрозы, относятся:

– источники ДВ на информацию (от кого или от чего исходит дестабилизирующее воздействие);

– виды ДВ на информацию (каким образом, по каким направлениям происходит ДВ);

– способы ДВ на информацию (какими приемами, действиями реализуются виды ДВ).

Помимо причин и обстоятельств, к факторам следует отнести наличие каналов и методов НСД к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешенного доступа.

Источниками ДВ на информацию являются:

– люди;

– технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи;

– системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;

– технологические процессы отдельных категорий промышленных объектов;

– природные явления.

В нижеприведенной таблице отражена взаимосвязь видов и способов ДВ на защищаемую информацию с источниками ДВ [34]

Виды воздействия	Способы дестабилизирующего воздействия	Результат воздействия на информацию
1. Со стороны людей		
Непосредственное воздействие на носители защищаемой информации	-физическое разрушение; -создание аварийных ситуаций для носителей; -удаление информации с носителей; -создание искусственных магнитных полей для размагничивания носителей; -внесение фальсифицированной информации в носители.	Уничтожение, искажение, блокирование
Несанкционированное распространение конфиденциальной информации	-словесная передача (сообщение) информации; -передача копий(снимков) носителей информации; -показ носителей информации; -ввод информации в вычислительные сети; -опубликование информации в открытой печати; -использование информации в публичных выступлениях.	разглашение
Вывод из строя технических средств (ТС) при работе с информацией и средств связи	-неправильный монтаж ТС; -поломка(разрушение) ТС. В т.ч. разрыв (повреждение) кабельных линий связи; -создание аварийных ситуаций для ТС; -отключение ТС от сетей питания; -вывод из строя систем обеспечения функционирования ТС; -вмонтирование в ЭВМ разрушающих радио и программных закладок.	Уничтожение, искажение, блокирование

Нарушение режима работы ТС и технологии обработки информации	- повреждение отдельных элементов ТС; - нарушение правил эксплуатации ТС; - внесение изменений в порядок обработки информации; - заражение программ обработки информации вредоносными вирусами; - выдача неправильных программных команд; - превышение расчетного числа запросов; - создание помех в радиоэфире с помощью дополнительного звукового или шумового фона; - передача ложных сигналов; - подключение подавляющих фильтров в информационные цепи, цепи питания и заземления; - нарушение, изменение режима работы систем обеспечения функционирования ТС.	Уничтожение, искажение, блокирование
Вывод из строя и нарушение режима работы систем обеспечения функционирования ТС	- неправильный монтаж систем; - поломка, разрушение систем или их элементов; - создание аварийных ситуаций для систем; - отключения систем от источников питания; - нарушение правил эксплуатации систем.	Уничтожение, искажение, блокирование
2. Со стороны технических средств при работе с информацией и средств связи		
Выход ТС из строя	-техническая поломка, авария (без вмешательства людей); - возгорание, затопление (без вмешательства людей); - выход из строя систем обеспечения функционирования ТС; - воздействие природных явлений; - воздействие измененной структуры окружающего магнитного поля; - заражение программ обработки носителя информации, в том числе размагничивание магнитного слоя диска(ленты) из-за осыпания магнитного порошка.	Уничтожение, искажение, блокирование
Создание электромагнитных излучений	- запись электромагнитных излучений.	Хищение
3. Со стороны систем обеспечения функционирования ТС при работе с информацией		
Выход систем из строя	- техническая поломка, авария(без вмешательства людей); - возгорание, затопление (без вмешательства людей); - выход из строя источников питания; - воздействие природных явлений.	Уничтожение, искажение, блокирование
Сбои в работе систем	- появление технических неисправностей элементов систем; - воздействие природных явлений; - нарушение режима работы источников питания.	Уничтожение. Искажение, блокирование
4. Со стороны технологических процессов отдельных промышленных объектов		

Изменение структуры окружающей среды	- изменение естественного радиационного фона окружающей среды при функционировании объектов ядерной энергетики; - изменение естественного химического состава окружающей среды при функционировании объектов химической промышленности; - изменения локальной структуры магнитного поля из-за деятельности объектов радиоэлектроники и изготовлению некоторых видов вооружения и военной техники.	Хищение
5. Со стороны природных явлений		
Землетрясение, наводнение, ураган (смерч), шторм, оползни, лавины, извержения вулканов	- разрушение (поломка), затопление, сожжение носителей информации, ТС работы с информацией, кабельных средств связи, систем обеспечения функционирования ТС; - нарушение режима работы ТС и систем обеспечения функционирования ТС; - нарушение технологии обработки.	Потеря, уничтожение, искажение, блокирование, хищение
Гроза, дождь, снег, перепады температуры и влажности. Магнитные бури		

13.5. Описание модели гипотетического нарушителя

Важной составляющей успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты информации является подготовка гипотетической модели потенциального нарушителя. При этом необходимо учитывать, что [28]:

• квалификация нарушителя может быть на уровне разработчика данной системы;

• нарушителем может быть как постороннее лицо, так и законный пользователь системы;

• нарушителю известна информация о принципах работы системы;

• нарушитель выберет наиболее слабое звено в защите.

При разработке модели нарушителя необходимо:

1) определить, к какой категории лиц он может принадлежать:

• из числа *внутренних* субъектов – непосредственный персонал системы. Это может лицо из следующих категорий персонала:

– пользователи (операторы) системы;

– персонал, обслуживающий технические средства (инженеры, техники);

– сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

– технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);

– сотрудники службы безопасности АС;

– руководители различных уровней должностной иерархии.

• из числа *внешних* (посторонних) лиц. Это могут быть:

– клиенты (представители организаций, граждане);

– уволенные сотрудники, осведомленные о защитных мерах и правах доступа к защищаемой информации;

– посетители (приглашенные по какому-либо поводу);

– представители фирм, поставляющих технику, ПО, услуги и т. п.;

– представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);

– представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

– лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС), или проникшие в информационные сети организации (хакеры);

– любые случайные лица за пределами контролируемой территории;

2) выявить цели и мотивы действий нарушителя (безответственность, самоутверждение, корыстный интерес, вандализм, принуждение, месть, идейные соображения);

3) попытаться оценить уровень квалификации нарушителя и его техническую оснащенность (используемые для совершения нарушения методы и средства);

4) учесть возможные ограничения на действия нарушителя.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АС (во время работы системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону данных (баз данных, архивов и т.п.);

- с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;
- НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Возможный ущерб АС и обрабатываемой информации при НСД зависит от уровня возможностей нарушителя (злоумышленника), который может обладать правами: разработчика, программиста, пользователя, администратора АС. Результатом реализации угроз информации может быть ее утрата (разрушение, уничтожение), утечка (извлечение, копирование), искажение (модификация, подделка) или блокирование.

14. Определение потенциальных каналов, методов и возможностей НСД к информации

Любая система связи (система передачи информации) состоит из источника информации, передатчика, канала передачи информации, приемника и получателя сведений.

Под ***каналом утечки информации*** понимается физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения канала утечки информации необходимы определенные про-

странственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

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

– *визуально-оптические* (непосредственное или удаленное, в том числе и телевизионное, наблюдение);

– *акустические* (включая и акустико-преобразовательные) – механические колебания стен, перекрытий, трубопроводов, окон и т.д.;

– *электромагнитные* (включая магнитные и электрические) – побочные электромагнитные излучения и наводки;

– *материально-вещественные* (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные, отходы делопроизводства).

Очевидно, что каждый источник конфиденциальной информации может обладать в той или иной степени какой-то совокупностью каналов утечки информации.

К *методам* НСД к конфиденциальной информации относятся:

1. Установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации. Наибольшая опасность может исходить от уволенных, недовольных (заработком, руководством, продвижением по службе) или отстраненных от конфиденциальной информации лиц, а также от эмигрантов и перебежчиков, недовольных государственным устройством.

Контакт с этими людьми может быть установлен различными путями, например на семинарах, выставках, конференциях и других публичных мероприятиях. Опосредованный контакт, осуществляемый через посредников (без прямого общения, диалога), устанавливается через коллег, родственников, знакомых, которые и выступают в роли посредников. При этом используются следующие способы НСД к информации:

– выведывание информации под благовидным предлогом;

– переманивание сотрудников конкурирующих предприятий;

– покупка конфиденциальной информации;

– шантаж, угрозы, физическое насилие; убеждение, лесть, посулы, обман, в том числе с использованием национальных, политических, религиозных факторов.

2. Вербовка и (или) внедрение агентов. С помощью агентов разведывательные службы стремятся получить доступ к такой информации, которую

нельзя добыть через другой, менее опасный канал. Использование агентурной разведки (шпионажа) позволяет получать не только служебную конфиденциальную информацию, но и иную, используя различные методы НСД, а также оказывать дестабилизирующее воздействие на информацию (искажение, блокирование, уничтожение).

3. Организация физического проникновения к носителям конфиденциальной информации. При этом сначала необходимо проникнуть на охраняемый объект, а затем завладеть носителями конфиденциальной информации.

Для проникновения на территорию объекта возможны разные способы:

– использование подложного, украденного или купленного (в том числе и на время) пропуска;

– маскировка под другое лицо;

– проход под видом внешнего обслуживающего персонала;

– скрытый проезд в автотранспорте;

– отвлечение внимания охраны для прохода незамеченным (путем создания чрезвычайных ситуаций, с помощью коллеги и т. д.);

– изоляция или уничтожение охраны;

– преодоление заграждающих барьеров (заборов), минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

Проникновение к носителям конфиденциальной информации с целью ее получения, искажения, уничтожения или блокирования может осуществляться во время транспортировки носителей, а также путем взлома хранилищ или проникновения в помещения, предназначенные для обработки конфиденциальных документов.

4. Подключение к средствам отображения, хранения, обработки, воспроизведения и передачи информации средствам связи.

Несанкционированное подключение, а следовательно, и НСД к конфиденциальной информации может производиться:

– с ПК с использованием телефонного набора или с несанкционированного терминала со взломом парольно-ключевых систем защиты или без взлома с помощью маскировки под зарегистрированного пользователя;

– с помощью программных и радиоэлектронных устройств;

– путем прямого присоединения к кабельным линиям связи, в том числе с использованием параллельных телефонных аппаратов;

– за счет электромагнитных наводок на параллельно проложенные провода или методов высокочастотного навязывания.

5. Прослушивание речевой конфиденциальной информации. Использование современных технических средств позволяет осуществлять прослушивание на значительных расстояниях путем:

– подслушивания непосредственных разговоров лиц, допущенных к данной информации;

– прослушивания речевой информации, зафиксированной на носителе, с помощью подключения к средствам ее звуковоспроизведения.

6. Визуальный съем конфиденциальной информации. Для этого используются:

– чтение документов и остаточной информации на рабочих местах пользователей (в том числе с экранов дисплеев, с печатающих и множительных устройств);

– осмотр продукции, наблюдение за технологическими процессами изготовления продукции и обработки информации;

– просмотр информации, воспроизводимой средствами видеовоспроизводящей техники (видеокамеры, цифровые камеры, телевизоры).

7. Перехват электромагнитных излучений, включающий поиск сигналов, выделение из них сигналов, несущих конфиденциальную информацию, съем с них информации, ее обработку и анализ.

Этот метод, по сравнению с другими каналами, имеет следующие преимущества: большой объем и высокая достоверность получаемой информации, оперативность ее получения и возможность съема в любое время, скрытность получения, возможность обнародования без угрозы перекрытия канала.

8. Исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации, реализуемое путем:

– приобретения и разборки (расчленение, выделение отдельных составных частей, элементов) выпускаемых изделий, их химический и физический анализ (обратный инжиниринг) с целью исследования конструкции, компонентов и других характеристик;

– сбор и изучение сломанных изделий, макетов изделий, бракованных узлов, блоков, устройств, деталей, созданных на стадии опытно-конструкторских разработок, а также руды и шлаков, позволяющих определить состав материалов, а нередко и технологию изготовления продукции;

– сбор и прочтение черновиков и проектов конфиденциальных документов, копировальной бумаги, красящей ленты печатающих устройств, прокладок, испорченных магнитных дискет.

Эти методы возможны, как правило, при нарушении требований по хранению носителей конфиденциальной информации и обращению с ними.

9. Получение конфиденциальных сведений из доступных источников информации. Для этого заинтересованными лицами:

– изучаются научные публикации, проспекты и каталоги выставок, базы данных предприятий;

– прослушиваются и просматриваются сообщения СМИ, выступления на конференциях и семинарах.

10. Подключение к системам обеспечения производственной деятельности предприятия;

11. Замеры и взятие проб окружающей объект среды;

12. Анализ архитектурных особенностей некоторых категорий объектов.

Состав реальных для конкретного предприятия каналов НСД к конфиденциальной информации и степень их опасности зависят от вида деятельности предприятия, категорий носителей, способов обработки информации, системы ее защиты, а также от возможностей конкурентов. Однако даже если соперники известны, определить их намерения и возможности практически не удается, поэтому защита должна предусматривать перекрытие всех потенциально существующих для конкретного предприятия каналов.

Использование того или другого канала осуществляется с помощью определенных, присущих конкретному каналу методов и технологий несанкционированного доступа.

15. Классификация мер обеспечения безопасности компьютерных систем

Среди мер обеспечения информационной безопасности АС обычно выделяют следующие: нормативно-правовые (законодательные), морально-этические, административные, физические, программно-аппаратные [3, 16].

15.1. Нормативно-правовые меры

К *нормативно-правовым* мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем са-

мым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Нормативно-правовые меры направлены на решение следующих вопросов [3]:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий по доступу к информации;
- права должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

На Гостехкомиссию России по защите информации, созданную в 1992 г., были возложены обязанности по координации, организационно-методическому руководству, разработке и финансированию научно-технических программ, лицензированию деятельности предприятий и сертификации продукции.

В настоящее время защита секретной информации в автоматизированных системах осуществляется Федеральной службой по техническому и экспортному контролю (ФСТЭК), созданной по Указу Президента РФ от 09.03.2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти».

В состав государственной системы ЗИ входят системы лицензирования деятельности предприятий по оказанию услуг в области защиты информации и сертификации продукции по требованиям безопасности информации.

Система лицензирования направлена на создание условий, при которых право заниматься работами по защите информации предоставляется только организациям, имеющим соответствующее разрешение (лицензию) на этот вид деятельности. А система сертификации технических и программных средств по требованиям безопасности информации направлена на защиту потребителя продукции и услуг от недобросовестной работы исполнителя. К сожалению, в этих вопросах Россия значительно отстала от развитых зарубежных стран.

Важным организационным документом системы защиты информации (СЗИ) является «Положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ». Этим документом установлен единый в стране порядок исследований, разработок, введения в действие и эксплуатации защищенных от НСД средств автоматизации.

Исходя из практических потребностей, в Положении определены различные варианты разработки защищенных средств ВТ, среди которых предусматривается:

- разработка защищенного общепрограммного обеспечения (ОПО) – ОС, СУБД, сетевого ПО;

- разработка защищенных программных средств (ПС) на базе ОПО, находящегося в эксплуатации и поставляемого вместе с незащищенными СВТ;

- разработка защищенных ПС на базе импортных программных прототипов.

В Положении изложен также порядок разработки, внедрения и эксплуатации средств криптозащиты информации.

Кроме перечисленных правовых и нормативных подзаконных актов государственной СЗИ, для нормальной деятельности в области безопасности информации необходим пакет нормативных документов технического характера – стандартов, руководящих документов, инструкций.

В США с 1984 г. сертификация СВТ по требованиям ЗИ от НСД осуществляется в соответствии с «Оранжевой книгой» - государственного стандарта «Критерии оценки надежных компьютерных систем» (Trusted Computer Systems Evaluation Criteria, TCSEC). В Европе в 1991 г. принят собственный стандарт «Критерии оценки безопасности информационных технологий – гармонизированные критерии Франции, Германии, Голландии и Великобритании», построенный на аналогичных принципах.

Отечественным аналогом «Оранжевой книги» является разработанный в 1992 г. РД «СВТ. Защита от НСД информации. Показатели защищенности от НСД к информации».

Этот документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Он может использоваться как методический материал при разработке СЗИ, или как нормативно-методический материал при их сертификации.

Кроме того, в настоящее время в законодательной сфере РФ создана правовая основа для регулирования сбора, хранения и использования информации. В УК РФ включена отдельная глава, посвященная компьютерным преступлениям. Защита интеллектуальной собственности отражена в уголовном и гражданском кодексах.

С начала 1990-х годов действует Закон РФ «О правовой охране программ для ЭВМ и баз данных», федеральный закон «Об информации, информатизации и ЗИ», Закон РФ «Об авторском праве и смежных правах» и ряд других нормативных актов.

Важнейшие законодательные нормативно-правовые документы разработаны с учетом следующих видов тайн:

- *государственная тайна* – Закон о государственной тайне, ст. 275, 276, 283, 284 УК РФ;

- *служебная и коммерческая тайна* – ст. 139 и 727 ГК РФ, ст. 155 и 183 УК РФ;

- *банковская тайна* – ст. 25 Закона о банках и банковской деятельности в РСФСР, ст. 857 ГК, ст. 183 УК РФ;

- *личная и семейная тайна* – ст. 150 ГК, ст. 137 УК РФ;

- *тайна переписки и телефонных переговоров* – ст. 138 УК РФ;

- *тайна голосования* - ст. 142 УК РФ.

Все перечисленные выше руководящие документы не исчерпывают потребностей, возникающих в ходе практических работ в области защиты информации. Это лишь необходимая основа организационной, нормативно-технической и методической документации, без которой невозможно нормальное существование и развитие информатики, и обеспечение безопасности информационных ресурсов самих СВТ.

15.2. Морально-этические меры

К *морально-этическим* мерам противодействия угрозам безопасности относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, но их несоблюдение обычно ведет к падению престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаными (например, общепризнанные нормы честности, патриотизма и т.д.), так и оформленными в некий свод (кодекс) правил или предписаний. Например, "Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США" рассматривает как неэтичные действия, которые умышленно или неумышленно:

• нарушают нормальную работу компьютерных систем;

• вызывают неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т.п.);

• нарушают целостность информации (хранимой и обрабатываемой);

• нарушают интересы других законных пользователей и т.п.

Социально-психологическое обеспечение ЗИ во многом зависит также от своевременной проверки благонадежности, от расстановки работников в соответствии с их способностями и личными качествами, формирования у каждого члена коллектива осознанного понимания важности и необходимости соблюдения требований режима конфиденциальности. Идеальным считается работник, обладающий такими личными качествами, как честность, принципиальность (строгое следование основным правилам), исполнительность, дисциплинированность, эмоциональная устойчивость (самообладание), стремление к успеху и порядку в работе, самоконтроль в поступках и действиях, правильная оценка собственных возможностей и способностей, умеренная склонность к риску, осторожность, умение хранить секреты, тренированное внимание, неплохая память.

Меньше всего утечек информации наблюдается в Японии, что связано с системой «пожизненного найма», и воспитанием чувств преданности и патернализма, когда работники одной организации считают себя членами единой, большой семьи.

В целом, нормативно-правовая база и моральные устои современного общества оказались не готовы к столь быстрому скачку в развитии информационных технологий, что проявилось прежде всего при интеграции России в единое информационное пространство Европы и мира с использованием сетей типа Интернет. В настоящее время отсутствуют способы и средства контроля ценности информационных ресурсов, транслируемых через границы (происходит утечка технологий и «ноу-хау»).

Для отработки механизма взаимодействия в информационном пространстве необходимо разработать законы, регулирующие отношения в этой области.

15.3. Административные меры

Административные меры защиты – это меры организационного характера. Они регламентируют:

- процессы функционирования системы обработки данных,
- использование ее ресурсов,

- деятельность персонала,
- порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Административные меры включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;
- мероприятия, осуществляемые при подборе и подготовке персонала системы, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию охраны и надежного пропускного режима с целью исключения возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей с конфиденциальной информацией;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и ПО и т.п.

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. В каждом конкретном случае эти мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты должно быть возложено на специальную службу – службу компьютерной безопасности.

Обязанности должностных лиц должны быть определены таким образом, чтобы при эффективной реализации ими своих функций, обеспечивалось разделение их полномочий и ответственности.

15.4. Физические меры

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

15.5. Технические (программно-аппаратные) меры

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов),
- разграничение доступа к ресурсам,
- регистрацию и анализ событий,
- криптографическое закрытие информации,
- резервирование ресурсов и компонентов систем обработки информации и др.

Взаимосвязь перечисленных мер обеспечения безопасности можно пояснить следующим образом:

1. Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации.

2. Воплощение организационных мер требует создания нормативных документов.

3. Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами.

4. Применение и использование технических средств защиты требует соответствующей организационной поддержки.

Программные меры защиты основаны на использовании антивирусных средств.

На сегодняшний день известно огромное количество антивирусных программ, разработанных различными отечественными и зарубежными антивирусными лабораториями. К наиболее популярным антивирусным средствам относятся:

Антивирус Касперского 6.0 имеет четыре компонента защиты: 1) файловый антивирус, обеспечивающий безопасность файлов; 2) почтовый антивирус; 3) веб-антивирус, контролирующий серфинг в Интернете; 4) проактивная защита – контроль работы макросов и блокировка опасных макрокоманд.

В версии 7.0 представлена новая концепция тройной защиты: проверка баз по сигнатурам, проактивный и эвристический механизмы.

Антивирус компании ESET – **NOD32** уже в течение 7 лет признается лучшим средством защиты от новых вирусов и атак благодаря мощному эвристическому анализатору. Основные преимущества: высокий уровень защиты, низкая ресурсоемкость, высокая скорость работы.

Российская компания «Доктор Веб» является поставщиком антивирусных продуктов **Doctor Web**, эвристический анализатор которого в сочетании с ежедневно обновляющимися вирусными базами обеспечивает защиту от вирусов и макровирусов, «троянских программ», почтового червя и других видов вредоносного программного кода.

Одним из известных иностранных антивирусов в России является **Norton Antivirus** компании Symantec. Он успешно борется с вирусами, троянскими компонентами и интернет-червями. Кроме Norton Antivirus компания разработала и другие средства для защиты от угроз, распространяемых через Интернет.

Panda Antivirus 2007. Большинство защитных продуктов полагаются на часто обновляемые локальные базы знаний. Технология Panda работает по другому принципу - большинство сигнатур злонамеренных кодов находятся в удаленной базе данных, которая обновляется в режиме реального времени. Новый антиспам Panda также полагается на механизм коллективного разума, в котором есть необходимые дефиниции для сортировки писем.

В этой версии есть также система эвристического сканирования, предотвращающая хищение персональных данных. Этот механизм особенно эффективен в борьбе с банковскими троянами.

16. Определение компонентов КСЗИ

16.1. Требования к подсистемам ЗИ

Требования к подсистемам определяются в соответствии с документами Гостехкомиссии России в зависимости от класса защищенности, определяемого минимальной совокупностью требований к защите информации.

Устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N – номер группы (от 1 до 3). Затем идет класс NБ и т. д.

Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса: 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа. Группа содержит пять классов: 1Д, 1Г, 1В, 1Б и 1А.

В приведенной ниже таблице собраны требования ко всем 9-ти классам защищенности АС, где приняты следующие обозначения:

"- " – нет требований к данному классу;

"+" – есть требования к данному классу;

СЗИ НСД – система ЗИ от несанкционированного доступа.

Для правильного определения класса АС необходимо знать:

1) тип АС (одно- или многопользовательская);

2) права пользователей по допуску к информации (допуск ко всей/части информации);

3) размещение информации на носителях (одного/разного уровней конфиденциальности);

4) гриф секретности информации: **Д –** несекретно; **Г** – конфиденциально; **В** – секретно; **Б** – совершенно секретно; **А** – особой важности.

Классы	**Подсистемы и требования**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей ОП ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа на разных ключах	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности									

4.1. ПС и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана СВТ и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+

Структура КСЗИ состоит из комплекса подсистем, защищающих ИС организации на разных уровнях. Вне зависимости от вида деятельности и размера организации, базовыми подсистемами ИБ являются 4 подсистемы: управления доступом, регистрации и учета, обеспечения целостности и криптографическая.

Создание КСЗИ для конкретной организации в зависимости от класса защищенности, может потребовать разработки ряда дополнительных подсистем.

Ниже приведено описание требований к некоторым подсистемам КСЗИ достаточно представительного класса защищенности - 1В. Этому классу соответствует минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность защищаемой информации. Реальные АС часто не соответствуют данному классу.

№ п/п	**Наименование подсистемы**	**Назначение**
1	Управления доступом	Управление доступом к информационным ресурсам
2	Регистрации и учета	Регистрация и учет действий пользователей и процессов
3	Обеспечения целостности	Сохранение целостности и доступности информационных ресурсов
4	Криптографическая	Обеспечение конфиденциальности и аутентичности информации
5	Антивирусной защиты	Защита программ и данных от вирусов и вредоносных программ
6	Межсетевого экранирования	Контроль и фильтрации сетевых пакетов, защита сетей от НСД
7	Резервного копирования	Резервное копирование и восстановление информации
8	Обнаружения и предотвращения атак	Выявление и блокирование сетевых атак и подозрительных действий

9	Обеспечение отказоустойчивости	Обеспечение бесперебойной работы системы
10	Централизованного управления ИБ	Централизованный мониторинг и аудит событий

16.2. Подсистема управления доступом

(идентификации и аутентификации пользователей)

Аутентификация - это процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает.

Идентификация - это процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нем.

При входе пользователя в систему первым делом происходит его аутентификация. Если введенные пользователем логин и пароль совпадают с хранимыми в системе на сервере, то он успешно входит в систему, иначе ему отказывается в доступе. При этом желательно контролировать количество попыток, чтобы избежать подбора паролей.

Требования к функциям подсистемы управления доступом [25]:

– должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее 6 буквенно-цифровых символов;

– должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);

– должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

– должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

16.3. Подсистема регистрации и учета

Основные требования к подсистеме:

– должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

– должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц);

– должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

– должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– должна осуществляться регистрация попыток доступа ПС к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;

– должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

– должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

– учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

– должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

– должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка

осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

16.4. Подсистема обеспечения целостности

Основные требования к подсистеме:

– должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

– должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью видеонаблюдения, использование строгого пропускного режима, специальное оборудование помещений АС;

– должен быть предусмотрен администратор (служба) ЗИ, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;

– должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД, их периодическое обновление и контроль работоспособности;

– должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

16.5. Криптографическая подсистема

Криптографическая подсистема предназначена для обеспечения *конфиденциальности* (невозможности прочтения информации посторонним) и *аутентичности* (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Основные требования к подсистеме:

– должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

– доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

– должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

При обмене электронными документами по сети возникает проблема аутентификации автора документа и самого документа, т.е. установления подлинности автора и отсутствия изменений в полученном документе. Для решения этой проблемы используется электронная цифровая подпись.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП.

Электронная цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ. Кроме этого, использование электронной цифровой подписи позволяет осуществить:

– доказательное подтверждение авторства документа;

– контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа изменится подпись, следовательно, она станет недействительной;

– защиту от изменений (подделки) документа;

– невозможность отказа от авторства.

ЭЦП формируется на основе самого документа и представляет собой относительно небольшое количество дополнительной информации, передаваемой вместе с подписываемым текстом.

Существует несколько схем построения цифровой подписи, например, на основе алгоритмов симметричного и асимметричного шифрования.

При формировании ЭЦП используются две процедуры: 1) процедуру постановки подписи; 2) процедуру проверки подписи.

Прежде всего, отправитель вычисляет хэш-функцию h(M) подписываемого текста M. Вычисленное значение хэш-функции h(M) представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Затем число m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

Хэш-функция (англ. hash – мелко измельчать и перемешивать) предназначена для сжатия подписываемого документа до нескольких десятков или сотен бит. Значение хэш-функции h(M) сложным образом зависит от документа M и не позволяет восстановить сам документ M.

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию m = h(M) принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

16.6. Подсистема антивирусной защиты

В соответствии с ГОСТ Р 51188–98 – Защита информации. Испытание программных средств на наличие компьютерных вирусов эта подсистема должна отвечать следующим требованиям:

– организация мониторинга антивирусной активности;

– создание двухуровневой антивирусной защиты с применением антивирусного ПО различных производителей;

– обеспечение антивирусной защиты серверного оборудования.

Компьютерный вирус – специально написанная небольшая программа, которая может сама присоединяться к другим программам для выполнения каких-либо вредоносных действий. Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения.

Самые распространённые каналы заражения: дискеты, флеш-накопители, электронная почта, системы обмена мгновенными сообщениями, веб-страницы, Интернет и локальные сети.

Вирусы принято разделять:

а) *по среде обитания* – загрузочные, файловые, файлово-загрузочные, сетевые;

б) *по степени воздействия* – безвредные, неопасные, опасные, разрушительные;

в) *по способам заражения*: резидентные, нерезидентные;

г) *по алгоритмическим особенностям* – репликаторы (черви), троянский конь, логическая бомба, мутанты, стелс-вирусы (невидимки), макровирусы.

В настоящее время существует большое разнообразие антивирусных программ:

- *программы-детекторы* могут находить только известные им вирусы (AidsTest Д.Н. Лозинского, Dr. Web А.И. Данилова);

- *программы-доктора* или *фаги*, а также *программы-вакцины* не только находят зараженные файлы, но и удаляют из файла тело программы-вируса. Среди фагов выделяют *полифаги*, предназначенные для поиска и уничтожения большого количества вирусов (AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web);

- *программы-ревизоры*. Самое надежное средство защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска, а затем периодически сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на видеомонитор (ADinf, ADinf32);

- *программы-фильтры* или *«сторожа»* – небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера (AVP, Norton Antivirus, McAfee Virus Scan 95);

- *антивирусные комплексы***,** выполняющие обнаружение, лечение, блокирование, восстановление, регистрацию, обеспечение целостности, обновление базы данных компьютерных вирусов (Norton Antivirus, пакет AVR (Anti Viral Toolkit Pro) –лаборатории Е. Касперского).

Выделяют также следующие разновидности антивирусных программ:

- *антивирусные сканеры* – пионеры антивирусного движения, которые ищут в файлах, памяти, и загрузочных секторах вирусные маски (описания) известных вирусов, хранящиеся в специальной базе данных. Проверка файлов производится только по инициативе пользователя после запуска программ;

- *антивирусные мониторы* (файловые, для почтовых программ, для специальных приложений) – осуществляют автоматическую проверку всех используемых файлов в масштабе реального времени. В случае обнаружения вредоносной программы, монитор, в зависимости от настроек, вылечит файл, заблокирует его выполнение или изолирует, переместив в специальную карантинную директорию для дальнейшего исследования;

- *программа-брандмауэр*, предназначенная для защиты компьютера от злоумышленников и вредоносного сетевого трафика.

Рекомендации по профилактике заражения:

- проверять на наличие вирусов все поступающие извне данные;

- периодически проверять все жесткие диски ПК на наличие вирусов;

- использовать лицензионные программные продукты;

- ограничить доступ к ПК других пользователей;

- защищать свои гибкие диски от записи при работе на других ПК;

- не оставлять в кармане дисковода дискету при включении или перезагрузке ПК, чтобы исключить заражение ПК загрузочными вирусами;

- регулярно обновлять антивирусные программы.

16.7. Подсистема межсетевого экранирования

Межсетевой экран (МЭ) или *сетевой экран* — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Кроме того, МЭ позволяют разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую.

Некоторые сетевые экраны позволяют осуществлять трансляцию адресов – динамическую замену внутрисетевых адресов или портов на внешние, используемые за пределами ЛВС.

Сетевые экраны часто называют *фильтрами*, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Фильтрация может осуществляться на любом уровне модели OSI . В качестве критериев может выступать информация с разных уровней: адреса отправителя/получателя, номера портов, содержимое поля данных.

Эквивалентными термину межсетевой экран являются названия:

– брандмауэр (нем. Brandmauer) – стена из огнеупорного материала, возводимая на пути распространения пожара;

– файерволл (англ. Firewall) – горящая стена (fire - огонь, wall - стена).

Модель OSI (Open System Interconnection reference model) или модель взаимодействия открытых систем – это многоуровневая система, отражающая взаимодействие программного и аппаратного обеспечения при осуществлении сеанса связи в сети.

В модели OSI сетевые функции распределены между 7 уровнями.

Каждому уровню соответствуют различные сетевые операции, оборудование и протоколы. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями.

Различают следующие уровни (сверху вниз): 1) прикладной; 2) представления; 3) сеансовый; 4) транспортный; 5) сетевой; 6) канальный; 7) физический.

Безопасное межсетевое взаимодействие для информационных систем достигается путем применения средств межсетевого экранирования (межсетевых экранов), которые обеспечивают в соответствии с приказом 58 ФСТЭК:

– фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

– регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ);

– контроль целостности своей программной и информационной части; – фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– восстановление свойств МЭ после сбоев и отказов оборудования;

– регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора МЭ, процесса регистрации действий администратора МЭ, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

16.8. Подсистема резервного копирования и архивирования

Подсистемы резервного копирования это программно-аппаратные комплексы, предназначенные для:

– проведения регулярного автоматического копирования, как системных данных, так и данных, создаваемых пользователями, на специально предназначенные для этого накопители;

– оперативного восстановления данных (в случае утери или по каким-то другим причинам).

Подсистема должна соответствовать следующим требованиям:

– поддержка всех основных сетевых и клиентских ОС;

– наличие документов и инструкций, регламентирующих процесс резервного копирования и архивирования в соответствии с производственной необходимостью;

– ведение подробных журналов выполняемых операций и сообщений;

– организация резервного копирования для всех серверов, указанных в регламентах резервного копирования;

– разработка процедуры и регулярное проведение тестирования резервных копий.

– простота использования.

16.9. Подсистема обнаружения атак

Подсистема обнаружения атак предназначена для своевременного обнаружения и предотвращения атак на узлы сети.

В функции подсистемы входит:

– обнаружение враждебной деятельности и распознавание атак на узлы сети;

– захват сетевого трафика;

– обработка сетевого трафика на основе заданной политики и имеющейся базы данных сигнатур атак. *Сигнатура атаки* (вируса) – характерные признаки атаки или вируса, используемые для их обнаружения. Наряду с *сигнатурными* методами необходимо использовать и *поведенческие* методы анализа информации. Поведенческие методы используется для выявления атак на основе обнаружения отклонений от штатного поведения ИС. Наиболее часто поведенческий метод реализуется на основе статистических моделей;

– блокирование сетевых атак посредством фильтрации потенциально опасных пакетов данных;

– использование методов активного и пассивного реагирования. Пассивное реагирование предполагает оповещение администратора о выявленной атаке, активное – блокирование попытки реализации атаки.

Серьезной проблемой при разработке подсистемы обнаружения атак является борьба с ложными срабатываниями (false positive).

16.10. Подсистема обеспечения отказоустойчивости

Отказоустойчивость (fault tolerance) - это способность системы сохранять работоспособность при отказах отдельных устройств, блоков, схем. В отказоустойчивой системе отказ одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову.

С понятием отказоустойчивости тесно связаны вопросы надежности СЗИ. Применительно к СЗИ от НСД надежность – это свойство системы защиты обеспечивать защиту информации от НСД в течение заданного промежутка времени.

Подсистема обеспечения отказоустойчивости должна обеспечивать бесперебойную работу:

– внешних дисковых подсистем в случае выхода из строя жесткого диска;

– серверов;

– АРМ пользователей.

16.11. Подсистема централизованного управления ИБ

Управление – это совокупность целенаправленных действий, включающих в себя оценку ситуации и состояния объектов управления, выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности).

Эффективность КСЗИ во многом зависит от наличия в ее составе средств, обеспечивающих сбор, анализ, хранение информации о состоянии системы ИБ, а также централизованного управления всеми ее составляющими.

Вся система в целом, как и каждая из ее подсистем, должны соответствовать общей политике безопасности. Для отслеживания работоспособности отдельных подсистем, организации мониторинга, определения и своевременного реагирования на угрозы ИБ и других событий предназначена подсистема централизованного управления компонентами системы, выполняющая следующие функции:

– мониторинг и аудит данных о событиях безопасности;

– оперативное оповещение об инцидентах безопасности;

– генерацию сводных отчётов с рекомендациями по управлению ИБ.

Кроме того, распределенная атака на ИС в некоторых случаях может быть зафиксирована и предотвращена только при получении данных из многих точек сети, как от средств защиты, так и от серверов, сетевого оборудования, приложений. Зафиксировать такую атаку можно, имея средства консолидации собираемых данных и корреляции регистрируемых событий.

17. Определение условий функционирования КСЗИ

При определении условий функционирования КСЗИ необходимо располагать следующей информацией [35]:

1) об организации процесса функционирования объекта защиты. В состав этих данных входят сведения, характеризующие:

– график работы объекта и его отдельных подразделений;

– правила и процедуры доступа на объект, в отдельные помещения и к оборудованию персонала и посетителей (регулярный, случайный, ограниченный доступ), а также правила его эксплуатации;

– численность и состав сотрудников и посетителей объекта (постоянный штат, персонал, работающий по контракту, клиенты);

– процедуру доступа на территорию транспортных средств.

Для получения этих данных можно применять следующие способы: анкетирование или опрос сотрудников; личное наблюдение; изучение директивных и инструктивных документов. Следует иметь в виду, что ни один из этих способов не дает объективной информации: каждый имеет свои достоинства и недостатки. Поэтому их применяют вместе, в совокупности;

2) об организации транспортных и информационных потоков. В состав этих данных входят сведения, характеризующие:

– пути и организацию перевозки и хранения материальных ценностей на территории объекта; уровни конфиденциальности информации, пути и способы ее обработки и транспортировки (документы, телефонная и радиосвязь и т. п.);

3) об условиях функционирования объекта. В состав этих данных входят сведения, характеризующие:

– пространство, непосредственно прилегающее к территории объекта;

– ограждение периметра территории и проходы;

– инженерные коммуникации, подземные хранилища и сооружения на территории;

– размещение подразделений и сотрудников по отдельным помещениям (с поэтажными планами);

– инженерные коммуникации в помещениях;

– состояние подвальных и чердачных помещений;

– размещение, конструкции и состояние входов, дверей, окон;

– существующую систему защиты;

– состав и настроение населения, экономические факторы и криминогенную обстановку на прилегающей территории.

На основе результатов анализа всех перечисленных сведений должны быть определены: назначение и основные функции системы защиты; основные виды возможных угроз и субъекты угроз; внешняя среда; условия функционирования системы защиты (наличие энергетических и других ресурсов, естественные преграды и т. п.).

Эти данные рекомендуется систематизировать в виде пояснительной записки, структурных схем и планов.

Целесообразно иметь следующие планы:

1) план территории объекта с указанием расположения всех зданий и других наземных сооружений; подземных сооружений; всех коммуникаций и мест их выхода за территорию объекта; всех ограждений, в том числе по периметру территории объекта, с обозначением их технического состояния на момент обследования; средств защиты (существующей системы, если она имеется);

2) поэтажные планы с указанием расположения всех помещений, с обозначением дверных и оконных проемов, внутренних и наружных (пожарных) лестниц, толщины материала стен и существующих средств защиты; всех коммуникаций с обозначением коммуникационных шкафов и других мест санкционированного доступа к каналам связи и жизнеобеспечения;

3) планы помещений с указанием:

– мест размещения оборудования и других технических средств (телефонов, персональных ЭВМ, принтеров и т. д.);

– расположения коммуникаций и мест размещения коммутационного оборудования (коробки, розетки и т. п.);

– функционального назначения и степени конфиденциальности получаемой и обрабатываемой информации;

– особенностей технологического процесса (для производственных помещений), важных с точки зрения обеспечения безопасности.

На основе этих планов целесообразно подготовить структурные схемы:

– ограждения каждого помещения, указав на ней (схематично) все стены и другие инженерно-технические сооружения, окружающие помещение;

– документооборота (для документов с ограниченным доступом), указав источник и приемники документа; его связи с другими документами; место хранения; способ подготовки (ручной, машинный); способ транспортировки (с курьером, по телефону, по факсу, по компьютерной сети и т.п.).

18. Разработка модели КСЗИ

Моделирование является одним из самых наглядных и эффективных инструментов исследования сложных систем, объектов или процессов. Значение моделирования особенно велико в системах, где натурные эксперименты невозможны по целому ряду причин: сложность, большие материальные затраты, уникальность или длительность эксперимента.

Модель – это некий новый материальный или абстрактный объект, который отражает существенные особенности изучаемого объекта, процесса или явления.

Степень соответствия модели исходному объекту характеризует уровень ее *адекватности*. Процедура установления адекватности (истинности) модели исходному объекту называется *верификацией* модели. Процесс разделения модели на подмодели называется *декомпозицией*.

Для одного и того же объекта можно создать разные модели. В то же время разные объекты могут описываться одной моделью.

В процессе моделирования КСЗИ решаются следующие задачи [9, 23]:

– определение основных параметров ЗИ;

– выбор показателей защищенности информации и критериев эффективности КСЗИ;

– уточнение требований к организационным, инженерно-техническим и программным мерам ЗИ;

– анализ функционирования КСЗИ;

– синтез структуры КСЗИ и оптимальное распределение средств защиты;

– поиск оптимальных решений по управлению безопасностью;

– оценка эффективности использования различных подсистем и мероприятий по ЗИ и др.

Для КСЗИ могут быть созданы различные модели, предназначенные для:

– анализа исследуемых процессов систем и подсистем;

– синтеза (построения различных систем, подсистем и мероприятий);

– управления исследуемыми процессами (подсистемами) с целью поиска оптимальных управленческих решений.

При этом рассматриваются как общие модели (в масштабе всей КСЗИ или подсистемы), так и частные модели с целью определения отдельных параметров функционирования КСЗИ (подсистемы).

Среди *методов моделирования* выделяют следующие классы:

– *аналитические* (методы классической математики – интегральное, дифференциальное и вариационное исчисление, методы поиска экстремумов функций, методы математического программирования, теории игр и т. п.);

– *статистические* (включают теоретические разделы математики - теорию вероятностей, математическую статистику, и направления прикладной математики, использующие стохастические представления - теорию массового обслуживания, методы статистических испытаний, основанные на методе Монте-Карло, методы выдвижения и проверки статистических гипотез А. Вальда и другие методы статистического имитационного моделирования);

– *теоретико-множественные, логические, лингвистические, семиотические представления* (разделы дискретной математики, составляющие теоретическую основу разработки разного рода языков моделирования, автоматизации проектирования, информационно-поисковых языков);

– *графические* (включают теорию графов и разного рода графические представления информации типа диаграмм, графиков, гистограмм и т.п.);

– *экспертные* или *эвристические* (используют человека в качестве «измерительного прибора» – эксперта для получения количественных оценок процессов и суждений, которые из-за неполноты и недостоверности имеющейся информации не поддаются непосредственному измерению). Для оценки адекватности моделей (правильности решений) в рассматриваемых условиях необходимо привлекать квалифицированных (опытных) экспертов по защите информации.

Основными разновидностями процесса моделирования можно считать два его вида – имитационное (математическое) и натурное (физическое).

Имитационное моделирование — это метод исследования, при котором изучаемая система заменяется моделью с достаточной точностью описывающей реальную систему и с ней проводятся эксперименты с целью получения информации об этой системе. Модели чаще всего реализуются в виде компьютерных программ, которые шаг за шагом воспроизводит события, происходящие в реальной системе.

Натурным моделированием называют проведение исследования на реальном объекте с последующей обработкой результатов эксперимента на основе теории подобия.

В таблице приведены некоторые виды моделей, используемые при моделировании КСЗИ:

Характеристики	**Виды моделей**		
	Аналитические	**Имитационные**	**Экспертные**
Решаемые задачи ЗИ	- определение уязвимостей в системе ЗИ; - вероятностное оценивание всех процессов, включая экономическую оценку; - обоснование мер ЗИ	-исследование объекта; - оценка влияния различных факторов; - процессы обучения	- оценка уровней безопасности; - сравнение вариантов по ЗИ; - анализ последствий реализации угроз
Достоинства	- достаточный уровень формализации ЗИ; - формульное представление моделей; - количественная оценка		- естественный язык моделирования; - моделирование слабоформализуемых задач
Недостатки	- сложность учета большого количества факторов; - нестационарный характер анализируемых процессов		- субъективный характер оценки; - трудность получения количественных характеристик

При моделировании *слабоформализуемых задач* используются утверждения, основанные на экспериментальных данных, интуиции. Цель их применения – найти не точное математическое, а наиболее рациональное путем исключения заранее непригодных решений.

На практике при моделировании, как правило, используется сочетание различных видов моделей. В результате создается *обобщенная* модель, представляющая собой совокупность частных моделей отдельных компонентов, входящих в КСЗИ, модель воздействия внешней среды и модель нарушителя. Эта модель позволяет обосновывать стратегические решения (стратегии) по ЗИ на основе перспективных планов развития предприятия.

При построении *модели нарушителя* необходимо учитывать:

– мотивы и цели, преследуемые нарушителем;

– степень его воздействия на информационную среду;

– квалификацию нарушителя и возможные места проникновения в КСЗИ;

– информационные ресурсы, доступные нарушителю;

– характер последствий от действий нарушителя.

Во избежание поспешных и непродуманных решений необходимо помнить, что:

1) моделями должен пользоваться только квалифицированный специалист-профессионал по ЗИ;

2) исходные данные, имеющие высокую степень неопределенности, необходимо постоянно уточнять.

19. Технологическое и организационное построение КСЗИ

Технологическое и организационное построение КСЗИ – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз [35].

Организационное направление работ по созданию КСЗИ предусматривает *организацию*:

– режима и охраны. Их цель – исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;

– работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, изучение их деловых и моральных качеств, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

– использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

– работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

– работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей. Организационные средства защиты ПЭВМ и информационных сетей применяются:

– при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы;

– при подборе и подготовке персонала. В этом случае предусматриваются проверка принимаемых на работу, создание условий, при которых персонал был бы заинтересован в сохранности данных, обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты и др.;

– при хранении и использовании документов и других носителей;

– при соблюдении надежного пропускного режима к техническим средствам, к ПЭВМ и информационным системам при сменной работе;

– при внесении изменений в программное обеспечение;

– при подготовке и контроле работы пользователей.

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в виде администратора безопасности сети и администратора распределенных баз и банков данных, содержащих сведения конфиденциального характера.

Организационные мероприятия являются той основой, которая объединяет различные меры защиты в единую систему. Они включают:

– разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

– мероприятия, проводимые при осуществлении или возникновении определенных изменений в защищаемой АС или внешней среде (по необходимости);

– периодически проводимые (через определенное время) мероприятия;

– постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Технологическое направление работ по созданию КСЗИ.

В нашем случае под технологией следует понимать совокупность операций и производственных процессов, объединенных в технологическую цепочку, обеспечивающих работу по обеспечению ЗИ.

Технологическая схема процессов реализует связи между функциональными и обеспечивающими подсистемами КСЗИ:

– определяет, каким образом, и в какой последовательности выполняются задачи по ЗИ в технологической среде ее обработки и передачи;

– обеспечивает:

- дифференцированный подход к защите различных АРМ и подсистем;
- унификацию различных вариантов средств ЗИ;
- реализацию разрешительной системы доступа к ресурсам АС;
- согласованность действий различных подразделений КСЗИ;
- учет динамики развития АС;
- минимизацию необходимого числа специалистов отдела ЗИ.

20. Кадровое обеспечение функционирования КСЗИ

Количественный состав и структура службы ЗИ определяется после завершения разработки КСЗИ с учетом ее технической структуры и режимов функционирования.

Организационно-штатная структура определяет количество подразделений, их подчиненность, перечень должностей. Каждому должностному лицу устанавливаются его права и обязанности в соответствии с занимаемой должностью.

Обязанности персонала предприятия по ЗИ определяются в коллективном договоре, трудовых договорах и должностных инструкциях.

При *отборе персонала* используются следующие методы: тестирование; ознакомление с личными делами, рекомендациями, отзывами с предыдущих мест работы; проведение конкурсов на замещение вакансий; аттестация сотрудников; проверка наличия судимостей и других правонарушений; изучение кредитных историй; собеседование и психофизиологическое исследование на полиграфе (детекторе лжи).

Ответственность за нарушения в области ИБ (юридический аспект):

– в Уставе организации и в функциональных (технологических) обязанностях всех сотрудников, участвующих в процессах автоматизированной обработки информации, необходимо отразить требования по обеспечению ИБ при работе в АС;

– при приеме на работу каждый сотрудник должен подписать Соглашение-обязательство о соблюдении установленных требований по сохранению государственной, служебной и коммерческой тайны, а также об ответственности за нарушение правил работы с защищаемой информацией в АС;

– все пользователи, руководящий и обслуживающий персонал АС должны быть ознакомлены с перечнем сведений, подлежащих защите, в части их касающейся (в соответствии со своим уровнем полномочий);

– доведение требований организационно-распорядительных документов по вопросам ИБ до лиц, допущенных к обработке защищаемой информации, должно осуществляться руководителями подразделений под роспись.

Сотрудники организации несут ответственность по действующему законодательству за разглашение сведений, составляющих (государственную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших им известными по роду работы.

Любое грубое нарушение порядка и правил работы в АС сотрудниками структурных подразделений должно расследоваться. К виновным должны применяться адекватные меры воздействия.

Нарушения установленных правил и требований по ИБ являются основанием для применения к сотруднику административных мер наказания, вплоть до увольнения и привлечения к уголовной ответственности (ст. 81 ТК РФ).

Мера ответственности сотрудников за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться с учетом нанесенного ущерба, наличия злого умысла и других факторов по усмотрению руководства.

Для реализации *принципа персональной ответственности* сотрудников за свои действия необходимы:

– индивидуальная идентификация сотрудников и инициированных ими процессов при работе в АС, т.е. установление за ними уникальных идентификаторов пользователей, на основе которых будет осуществлять разграничение доступа и регистрация событий;

– проверка подлинности соответствия пользователей и сотрудников (аутентификация) на основе паролей, ключей, специальных устройств, биометрических характеристик личности сотрудников и т.п.;

– регистрация (протоколирование) работы механизмов контроля доступа пользователей к ресурсам ИС с указанием даты, времени, идентификаторов пользователя, запрашиваемых им ресурсов, вида взаимодействия и его результата;

– оперативная реакция на попытки НСД (сигнализация, блокировка и т.д.).

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, ПО и данным АС **обязан**:

– производить обработку защищаемой информации в подсистемах АС в строгом соответствии с утвержденными технологическими инструкциями для данных подсистем;

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

– знать и строго выполнять правила работы со средствами ЗИ, установленными на его рабочей станции;

– хранить в тайне свой пароль. Периодически в соответствии с «Инструкцией по организации парольной защиты АС» менять свой пароль;

– передавать для хранения установленным порядком свое индивидуальное устройство идентификации (Touch Memory , Smart Card , Proximity и т.п.) и другие реквизиты разграничения доступа и носители ключевой информации только руководителю своего подразделения или ответственному за ИБ в подразделении (в пенале, опечатанном своей личной печатью);

– надежно хранить и никому не передавать личную печать и использовать ее только для опечатывания пенала с реквизитами доступа и носителями ключевой информации;

– если сотруднику (исполнителю) предоставлено право защиты (подтверждения подлинности и авторства) документов, передаваемых по технологическим цепочкам в АС, при помощи ЭЦП, то он дополнительно обязан соблюдать все требования «Порядка работы с ключевыми носителями (дискетами)»;

– выполнять требования «Инструкции по организации антивирусной защиты в АС» в части касающейся действий пользователей рабочих станций (РС);

– немедленно ставить в известность ответственного за безопасность информации и руководителя подразделения в случае утери носителей ключевой информации, индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

• нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах или иных фактов совершения в его отсутствие попыток НСД к закрепленной за ним защищенной рабочей станции;

• некорректного функционирования установленных на РС технических средств защиты;

• несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств РС ;

• непредусмотренных формуляром РС отводов кабелей и подключённых устройств;

• отклонений в нормальной работе системного и прикладного ПО, затрудняющего эксплуатацию РС, выхода из строя или неустойчивого функционирования узлов РС или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

– присутствовать при работах по изменению аппаратно-программной конфигурации закрепленной за ним РС, по завершении таких работ проверять ее работоспособность.

Категорически **запрещается**:

• использовать компоненты программного и аппаратного обеспечения АС не по назначению (в неслужебных целях);

• самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств РС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами РС;

• осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

• записывать и хранить конфиденциальную информацию (сведения ограниченного распространения) на неучтенных носителях;

• оставлять включенной без присмотра свой компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

• передавать кому-либо свой персональный ключевой носитель (дискету, Touch Memory и т.п.) кроме ответственного за ИБ или руководителя своего подразделения установленным порядком, делать неучтенные копии ключевого носителя, снимать с него защиту записи и вносить какие-либо изменения в записанные на носитель файлы;

• использовать свои ключи ЭЦП для формирования цифровой подписи любых электронных документов, кроме электронных документов, регламентированных технологическим процессом на его рабочем месте;

• оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители ключевой информации, носители и распечатки, содержащие сведения ограниченного распространения;

• умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты, которые могут привести к нарушениям ИБ и возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность ответственного за безопасность информации и руководителя своего подразделения.

Для других сотрудников группы безопасности (руководителя, администратора) также должны быть подробно разработаны их права и обязанности; документы, определяющие порядок работы с носителями ключевой информации и устанавливающие ответственность за нарушения.

Для обучения персонала вопросам ЗИ в современных условиях наиболее важной и эффективной формой является организация занятий непосредственно на предприятии под руководством опытных сотрудников службы защиты информации.

21. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ

Материально-техническое обеспечение (МТО) позволяет удовлетворить потребность в расходных материалах, запасных изделиях и приборах, инструментах и других материальных средствах, необходимых для эксплуатации КСЗИ.

Состав МТО КСЗИ зависит от ее структуры и определяется [8]:

1) при планировании и осуществлении работы объектов материально-технической базы службы ЗИ;

2) при определении потребности, приобретении, учете и хранении всех видов материальных средств, их распределении, выдаче (отправке, передаче) по назначению, обеспечении правильного и экономного расходования и ведении отчетности;

3) при накоплении и содержании установленных запасов материальных средств, обеспечении их сохранности;

4) при эксплуатации, сбережении, своевременном техническом обслуживании и ремонте;

5) при создании условий для организации и проведения мероприятий ЗИ;

6) при строительстве, ремонте и эксплуатации зданий и помещений;

7) при изучении положения дел, выявлении внутренних и внешних факторов, оказывающих влияние на МТО КСЗИ;

8) при выявлении нарушений, ошибок в МТО и оперативном принятии мер по их устранению.

При работе с МТО КСЗИ на предприятии необходимо:

– разработать нормативные акты по вопросам МТО КСЗИ;

– уметь определять потребность материально-технических средств для обеспечения нормального функционирования КСЗИ;

– знать наличие, состояние и порядок хранения материальных средств ЗИ;

– своевременно пополнять МТО КСЗИ;

– вести учет, правильное хранение, сбережение запасов материальных средств КСЗИ, а также их эксплуатацию, ремонт и техническое обслуживание;

– рационально и экономно расходовать материальные средства;

– осуществлять контроль за использованием МТО КСЗИ.

Состав *нормативно-методического обеспечения* КСЗИ определяют:

– *законодательные* акты – законы, указы президента, постановления правительства, кодексы (гражданский, уголовный, административный), ГОСТы;

– *руководящие* методические документы – документы министерств и ведомств (Гостехкомиссия, ФСБ), а также документы, разработанные на предприятиях по вопросам ЗИ;

– *информационно-справочная* база – словари, каталоги, специализированные журналы, справочники, электронные БД.

Нормативные документы, определяющие правила безопасности должны удовлетворять следующим требованиям:

– соответствовать структуре, целям и задачам ИС;

– описывать общую программу обеспечения безопасности сети, включая вопросы эксплуатации и усовершенствования;

– перечислять возможные угрозы информации и каналы утечки;

– перечислять рекомендуемые защитные меры;

– определять ответственных за внедрение и эксплуатацию всех средств защиты;

– определять права и обязанности пользователей;

– содержать перечень и классификацию возможных кризисных ситуаций;

– определять порядок разрешения споров в случае возникновения конфликтов.

В комплект внутренних нормативных и методических документов по обеспечению функционирования КСЗИ на предприятии должны входить документы, регламентирующие:

– перечень сведений, подлежащих защите;

– порядок обращения сотрудников с конфиденциальной информацией;

– меры по предотвращению НСД к информационным ресурсам и АС;

– обмен информацией со сторонними организациями;

– пропускной и внутриобъектный режим;

– порядок эксплуатации АС предприятия;

– действия должностных лиц и персонала предприятия в условиях ЧС, обеспечения бесперебойной работы и восстановления;

– планы защиты АС;

– порядок разработки, испытания и сдачи в эксплуатацию ПС;

– порядок закупки программных и аппаратных средств (в том числе средств ЗИ);

– порядок эксплуатации технических средств связи и телекоммуникации.

22. Назначение, структура и содержание управления КСЗИ

Управление – это процесс осуществления информационных воздействий на объекты управления для формирования их целенаправленного поведения.

Сущность управления КСЗИ заключается в целенаправленной деятельности руководства предприятия, должностных лиц и службы ЗИ, направленной на достижение целей защиты информации.

Основными *функциями* управления в КСЗИ являются:

– планирование (оценка обстановки, выработка замысла разрешения сложившейся ситуации, выработка возможных вариантов решения, принятие решения руководителем, разработка плана в соответствии с принятым решением);

– руководство выполнением принятого плана (решения);

– управление КСЗИ в условиях ЧС;

– контроль и коррекция реализуемого плана (решения).

Управление КСЗИ является частью функционирования предприятия в целом. В связи с этим практическая реализация КСЗИ предусматривает наличие следующих функций управления:

1. Организаторская: органы управления КСЗИ выдают приказы исполнителям на выполнение каких-либо действий.

2. Аналитическая: анализ состояний окружающей среды по вопросам обеспечения ИБ.

3. Целеуказательная: определение целей, частных функций и задач КСЗИ в целом и отдельных её подсистем.

4. Контрольная: контроль результатов выполнения принятых решений.

Процесс управление в комплексной системе защиты информации является непрерывным и многоуровневым:

Уровни управления	Решаемые задачи	Органы управления
Стратегический	Стратегия КСЗИ	Руководство предприятия
Оперативный	Концепция	Служба ИБ
Тактический	Политика безопасности	Руководители отделов
Операционный	Регламент по ЗИ	Отдельные сотрудники

Объектом управления может быть как коллектив людей (пользователей системы), так и технические средства.

Критерием эффективности принимаемых решений могут служить:

– на стадии принятия решения – вероятность того, что система перейдет к заданному уровню защищенности информации;

– на стадии контроля – соответствие заданному уровню безопасности.

Построение КСЗИ и ее функционирование должны осуществляться в соответствии со следующими *принципами управления*:

1) *принцип научности,* предполагающий построение КСЗИ на строго научных основах;

2) *принцип системности и комплексности,* делающий необходимым изучение системы защиты и управляющий системы совместно и нераздельно с учетом всех взаимосвязанных элементов, условий и факторов;

3) *принцип единоначалия в управлении и коллегиальности в выработке решений,* предполагающий, что в рамках системы любое коллегиальное решение должно разрабатываться коллегиально. Необходимо добиваться всесторонности разработок, учитывать мнения многих специалистов по различным вопросам. При этом принятое коллегиальное решение проводится в жизнь под персональную ответственность руководителя;

4) *принцип централизованности и децентрализованности.* Централизация и децентрализация должны находиться в единстве и дополнять друг друга;

5) *принцип пропорциональности в управлении,* означающий, что рост и усложнение объекта ведут к росту субъекта управления;

6) *принцип экономии времени,* делающий необходимым постоянное уменьшение трудоемкости операций в производственном процессе;

7) *принцип целевой совместимости и сосредоточения,* состоящий в создании связанной, целенаправленной системы, при которой все ее звенья образуют единый механизм, направленный на решение общей задачи. Работа отдельных служб предприятия строится таким образом, чтобы в конечном итоге в заданное время появилась именно та продукция, в которой нуждается конечный потребитель;

8) *принцип непрерывности и надежности,* предполагающий создание таких условий, при которых достигаются устойчивость и непрерывность заданного режима производственного процесса;

9) *принцип планомерности, пропорциональности и динамизма,* состоящий в том, что производственная система должна быть нацелена на достижение не только текущих, но и долговременных целей своего развития;

10) *принцип эффективности управления,* (актуален, поскольку на практике в производственном процессе существует многовариантность путей достижения одной и той же поставленной цели).

Соблюдение принципов управления позволит существенно повысить эффективность управления КСЗИ.

23. Принципы и методы планирования функционирования КСЗИ

Особое место в управлении КСЗИ занимает планирование.

Планирование – это процесс разработки и последующего контроля за ходом реализации разработанного и принятого к исполнению плана и его корректировки в соответствии с изменяющимися условиями. Кроме того, это процесс обработки информации, направленный на обоснование предстоящих действий, выявление наилучших способов достижения целей.

Функциями планирования являются научное обоснование целей развития, выбор наилучших способов достижения целей.

Различают следующие уровни планирования:

– *стратегическое планирование* – особый вид плановой работы, заключающийся в разработке стратегических решений (в форме прогнозов, проектов, программ и планов). В ходе стратегического планирования разрабатывается политика.

– *тактическое планирование* – планирование отдельных мероприятий, касающихся достижения стратегических целей и определения ресурсов для их реализации.

– *операционное (оперативное) планирование* представляет собой выбор средств решения задач, поставленных, заданных или установленных вышестоящим руководством.

С точки зрения охвата периода времени планирование может быть: краткосрочным, среднесрочным, долгосрочным.

1. *Краткосрочное* (оперативное) планирование – это планирование для управления системой при достижении ближайших целей (планирование в текущей обстановке). Краткосрочное планирование осуществляется на срок до 1 месяца.

2. *Среднесрочное* планирование осуществляется с целью перспективного развития системы в течение небольшого, но значительного промежутка времени (1мес. – 1 год) с целью достижения ближайших перспектив.

3. *Долгосрочное* планирование (свыше 1 года) направлено на обеспечение дальнейшего развития КСЗИ с учетом стратегических планов развития предприятия.

Методика планирования функционирования КСЗИ предусматривает:

– определение порядка действий;

– этапы выполнения;

– критерии оценки эффективности;

– обеспечение каждого мероприятия по защите информации (организационное, материальное и другие виды обеспечения);

– контроль реализации принятых решений.

Контроль реализации принятых решений проводится с целью оценки эффективности реализованных решений, корректировки дальнейших планов, оптимизации хода выполнения решения, методической подготовки персонала.

Особое место в управлении КСЗИ отводится управлению в условиях ЧС.

Принципы планирования (требования) представляют собой основные исходные положения, правила обоснования и организации разработки плановых документов. Они должны постоянно изменяться, совершенствоваться, наполняться новым содержанием по мере развития экономики.

Впервые общие принципы планирования были обозначены А. Файолем. В качестве основных требований к разработке программы действий или планов предприятия им были сформулированы пять принципов:

1) *принцип необходимости планирования* (повсеместное и обязательное применение планов при выполнении любого вида деятельности);

2) *принцип единства планов* (разработка общего или сводного плана социально-экономического развития предприятия);

3) *принцип непрерывности планирования* (на каждом предприятии процессы планирования, организации и управления производством, как и трудовая деятельность, являются взаимосвязанными между собой и должны осуществляться постоянно и без остановки);

4) *принцип гибкости планов* (предполагает возможность корректировки установленных показателей и координации планово-экономической деятельности);

5) *принцип участия* (состоит в том, что никто не может планировать эффективно для кого-то другого).

В зависимости от главных целей или основных подходов, используемой информации, нормативной базы, применяемых путей получения и согласования тех или иных конечных плановых показателей принято различать следующие ***методы планирования:*** экспериментальные, нормативные, балансовые, расчетно-аналитические, программно-целевые, отчетно-статистические, экономико-математические и другие.

Расчетно-аналитический метод основан на расчленении выполняемых работ и группировке используемых ресурсов по элементам и взаимосвязи, анализе условий наиболее эффективного их взаимодействия и разработке на этой основе проектов планов.

Экспериментальный метод – это проектировка норм, нормативов и моделей планов на основе проведения и изучения замеров и опытов, а также учета опыта специалистов.

Отчетно-статистический метод состоит в разработке проектов планов на основе отчетов, статистики и иной информации, характеризующей реальное состояние и изменение характеристики деятельности предприятия.

В процессе планирования ни один из рассматриваемых методов не применяется в чистом виде.

В качестве конечных точек планирования выступают цели. Цели должны быть: реальными и достижимыми; детализированными с точки зрения комплекса и содержания работ подразделений, обеспечивающих их реализацию; измеримыми; однозначными для понимания (четкими).

Цели задаются также с учетом объема работ и сроков их выполнения, с учетом имеющихся ресурсов и возможностей исполнителей.

Основными *этапами* процесса планирования в КСЗИ являются:

– определение и обоснование целей организации системы ЗИ;

– формирование перечня задач, обеспечивающих достижение поставленных целей;

– анализ условий, обеспечивающих достижение целей планирования;

– поиск значимых причин, факторов и тенденций во внутренней и внешней среде защищаемого объекта;

– определение реальных и потенциальных угроз безопасности;

– анализ ресурсов, необходимых для обеспечения решения поставленных задач;

– формирование и выбор стратегических альтернатив организации системы защиты;

– анализ сравнительных преимуществ и недостатков;

– согласование ресурсов, выделяемых для решения задач;

– определение приоритетов и последовательности решения плановых задач и организации их исполнения;

– определение эффективных методов решения задач и использования ресурсов:

– определение видов и способов контроля выполнения плановых задач;

– документальное и организационное оформление плана.

24. Сущность и содержание контроля функционирования КСЗИ

Контроль является одним из важнейших и необходимых направлений работ по ЗИ. *Цель контроля*: выявить слабые места системы, допущенные ошибки, своевременно исправить их и не допустить повторения.

Основные *требования* к контролю: комплексность, своевременность, стандартизация, простота, доступность, гибкость, объективность, экономичность.

Основные *методы контроля*: проверка, изучение, испытания, наблюдения, зачеты, экзамены, тестирование, провокации аварийных ситуаций, атаки и др.

Основными *задачами контроля* являются [2, 11, 31]:

– определение обоснованности и практической целесообразности проводимых мероприятий по ЗИ;

– выявление фактического состояния СЗИ в данный период времени;

– анализ сравнения фактического состояния с заданным режимом, обстановкой и оценка характера допущенных отклонений и недоработок;

– установление причин и обстоятельств отклонений показателей качества, характеризующих СЗИ, от заданных;

– разработка мероприятий по улучшению и корректировке процесса управления и принятия мер по их реализации.

– изучение деловых качеств и уровня профессиональной подготовки лиц, осуществляющих ЗИ.

Меры контроля представляют собой совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по ЗИ. Организационные меры контроля включают проверку:

– выполнения сотрудниками требований по обеспечению сохранности коммерческой тайны;

– выполнения пропускного режима (проверка наличия постоянных пропусков у сотрудников предприятия, проверка работы охранников);

– выполнения сотрудниками правил работы с конфиденциальными документами (правила хранения, размножения и копирования);

– наличия защищаемых носителей конфиденциальной информации.

При проведении технического контроля осуществляется проверка мер технической защиты информации установленным требованиям или предельно допустимым значениям (нормам). В зависимости от объема проверяемых каналов возможной утечки информации технический контроль может быть:

– комплексный, проверка всех каналов;

– целевой, проверка одного из каналов;

– выборочный, проверка наиболее вероятных каналов утечки.

Кроме того, контроль функционирования КСЗИ может быть:

– внешний, проводимый различными государственными органами;

– внутренний, проводимый службой безопасности предприятия.

При классификации видов контроля используются временные рамки, скорость изменения контролируемых процессов, затраты на проведение измерений и обработку результатов и др. (см. приведенную ниже таблицу).

Категория контроля	**Возможные разновидности контроля**
Уровень автоматизации	неавтоматизированный; частично; полностью
Объекты системы	система в целом; подсистемы КСЗИ; отдельные элементы
Полнота охвата	локальный; сквозной; глобальный
Последовательность реализации контрольных операций	последовательный; параллельный; смешанный
Функциональная направленность	организационно-правовой; технический; ресурсный (кадровый, информационный)
Периодичность	систематический; периодический; эпизодический (внезапный)
Вид получаемой информации	первичный; сводный

В последнее время широко применяются следующие виды контроля:

– мониторинг – непрерывное поступление информации;

– контроллинг – оценка экономичности;

– бенчмаркинг – внедрение технологий, стандартов и методов деятельности более успешных организаций-аналогов.

В самом процессе контроля выделяют следующие стадии: предварительная, текущая и заключительная.

Заключительный контроль даёт руководству информацию для: анализа причин нарушений и недостатков в организации и обеспечении ЗИ; выработки рекомендаций по их устранению и планирования проведения аналогичных работ в будущем.

25. Управление КСЗИ в условиях чрезвычайных ситуаций

Чрезвычайная ситуация (ЧС) – это катастрофические изменения состояния некоторого объекта (здания, предприятия, территории), сложившиеся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия и повлекшие за собой большие людские, материальные или финансовые потери.

ЧС классифицируются: по источникам происхождения и по масштабам (количеству пострадавших, размеру материального ущерба, территории распространения).

Выделяют следующие причины возникновения ЧС:

– природные (ураганы, землетрясения, наводнения и т.д.);

– техногенные (поломки, аварии, взрывы);

– антропогенные источники ЧС (неосторожность персонала, злой умысел и т.д.), связанные с деятельностью человека;

– терроризм.

На принятие решений в условиях ЧС существенное влияние оказывают следующие факторы:

– неопределенность, связанная со сложностью сбора и обработки оперативной информации, а также возможным разрушением АС управления;

– недостаток резервов и ресурсов;

– ограниченность времени на принятие решения;

– психофизиологическое состояние лиц, принимающих решения, и тех, кто испытал на себе последствия ЧС (шок, кровопотеря, страх, голод, и т.п.).

Главное в ЧС – это сохранение жизни людей и нормальное функционирование систем жизнеобеспечения, в том числе КСЗИ.

Все ЧС имеют 3 классических периода:

1) угрожаемый;

2) нейтрализации или предотвращения;

3) восстановления функционирования КСЗИ.

В этой связи чрезвычайно важной является подготовка мероприятий на случай возникновения ЧС. Это может быть:

1. Заблаговременная подготовка, включающая:

– прогнозирование потерь при ЧС;

– расчет и формирование резерва, необходимого для сокращения потерь;

– поддержание ресурсов в необходимой степени готовности.

2. Непосредственная подготовка – привлечение (частичное или полное) подготовленного резерва к работам по ликвидации последствий ЧС.

Для КСЗИ в условиях ЧС необходимо разработать:

– меры по защите наиболее важных и ценных носителей информации;

– подробные инструкции, регламентирующие деятельность каждого сотрудника;

– распределение обязанностей и ответственности за сохранность носителей информации;

– материально-техническое обеспечение ЧС (маршруты перевозок, карты, адреса, и. т.п.).

Особое внимание необходимо уделить созданию резервных копий жизненно важной для функционирования комплексной системы информации.

Различают следующие *виды* резервирования:

1) организационное; 2) техническое; 3) информационное.

Среди *методов* резервирования выделяют:

– полное дублирование;

– инкрементальное (наращиваемое) резервирование;

– дифференциальное резервирование.

Полное резервирование обычно затрагивает всю КСЗИ и все защищаемые документы. Еженедельное, ежемесячное и ежеквартальное резервирование подразумевает полное резервирование.

При инкрементальном резервировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее резервиро-

вание добавляет только те файлы, которые были изменены с момента предыдущего инкрементального резервирования. В среднем, этот вид резервирования требует меньше времени. Однако процесс восстановления данных занимает больше времени, так как объем восстанавливаемых данных увеличивается.

При дифференциальном резервировании каждый файл, который был изменен с момента последнего полного резервирования, копируется каждый раз заново. Дифференциальное резервирование ускоряет процесс восстановления.

Управление КСЗИ в ЧС сводится к разработке плана действий в возможных ЧС и к проведению учений, тренировок персонала, и т.п.

Главный показатель системы в ЧС – катастрофоустойчивость – способность вычислительных систем сохранять работоспособность хотя бы в некотором минимальном объеме после возникновения ЧС.

26. Состав методов и моделей оценки эффективности КСЗИ

Эффективность системы – это свойство системы, характеризующее ее способность выполнять свою целевую функцию.

Оценка эффективности – это процедура, направленная на определение качественных и количественных показателей эффективности, выявление критических элементов системы, а также определение интегрального показателя эффективности системы в целом.

Показатель эффективности (ПЭ) – это величина, характеризующая степень достижения системой какой-либо из стоящих перед ней задач.

Примером ПЭ является криптостойкость шифра, которая определяется временем или стоимостью взлома шифра.

ПЭ должен:

– иметь определенный физический смысл;

– быть пригодным для количественного анализа;

– иметь простую и удобную форму;

– отражать одну из значимых сторон функционирования системы;

– обеспечивать необходимую *чувствительность*. Чувствительность – способность объекта реагировать определённым образом на определённое малое воздействие (изменение параметров и характеристик), а также количественная характеристика этой способности.

Все ПЭ можно разделить на 2 группы:

1. Единичные (частные), отражают какую-либо из значимых сторон функционирования системы (вероятность обнаружения нарушителя или вероятность его нейтрализации силами охраны и т.п.);

2. Комплексные (обобщенные), представляют собой комбинацию частных показателей.

Кардинальным обобщающим показателем является показатель экономической эффективности системы, характеризующий целесообразность затрат, произведенных на создание и функционирование системы.

Для того чтобы оценить эффективность системы ЗИ или сравнить системы по их эффективности, необходимо задать некоторое правило предпочтения. Такое правило или соотношение, основанное на использовании показателей эффективности, называют *критерием эффективности*.

Для оценки эффективности КСЗИ и получения критерия эффективности при использовании некоторого множества n показателей используют ряд ***методов***:

1. Выбирается *один главный показатель*, и оптимальной считается система, для которой этот показатель достигает экстремума. При условии, что остальные показатели удовлетворяют системе ограничений, заданных в виде неравенств.

2. Методы, основанные на *ранжировании показателей* по важности. При сравнении систем одноименные показатели эффективности сопоставляются в порядке убывания их важности по определенным алгоритмам.

3. *Мультипликативные и аддитивные* методы получения критериев эффективности основываются на объединении всех или части показателей с помощью операций умножения или сложения в обобщенные показатели. Если в произведение (сумму) включается часть показателей, то остальные частные показатели включаются в ограничения.

4. *Метод Парето*: при использовании n показателей эффективности системе соответствует точка в n-мерном пространстве. В n-мерном пространстве строится область парето-оптимальных решений, содержащая несравнимые решения, для которых улучшение какого-либо показателя невозможно без ухудшения других показателей эффективности. Выбор наилучшего решения из числа парето-оптимальных может осуществляться по различным правилам.

Моделирование оценки эффективности КСЗИ сводится к построению абстрактного образа всей системы с имитацией её основных характеристик в интересах получения требуемых данных – показателей эффективности, как отдельных компонентов, так и всей системы в целом.

Процесс моделирования оценки эффективности разбивается на ряд этапов: выбор критериев; построение модели; реализация процессов оценки эффективности (в интересах поставленной цели).

На практике выделяют следующие группы ***моделей*** оценки эффективности:

аналитические – поведение объекта и КСЗИ моделируется на основании различных функциональных зависимостей и логических условий (используются методы классической математики: интегральное, дифференциальное, вариационное исчисления и др.);

имитационные – моделируют различные реальные ситуации на основе реализуемых алгоритмов в области ЗИ. Имитация – это постижение сути явления, не прибегая к экспериментам на реальном объекте;

экспертные – реализуются на основе эвристического моделирования высококвалифицированными специалистами (экспертами). Эвристические модели не имеют количественного подтверждения, но способствуют более глубокому проникновению в суть дела.

В таблице перечислены возможные области использования моделей при оценке эффективности КСЗИ.

Вид модели		
Аналитическая	**Имитационная**	**Экспертная**
Определение наиболее уязвимых мест в КСЗИ	Исследование объекта ЗИ	Сравнение различных вариантов построения КСЗИ
Вероятностное оценивание и экономический расчёт ущерба от реализации угроз	Оценка влияния различных условий обработки информации и внешней среды на ЗИ	Определение целесообразных затрат на создание КСЗИ
Стоимостной анализ применения мер по ЗИ	Обучение персонала работе с КСЗИ	Анализ последствий воздействия угроз на объект защиты
Научное обоснование количественных показателей эффективности защиты	Оценка влияния реальных событий на КСЗИ	Доведения существующего уровня безопасности КСЗИ до требуемого

В качестве привлекаемых показателей эффективности используются:

– для аналитической модели:

- вероятность обнаружения НСД;
- вероятность реализации угрозы;
- вероятность противодействия НСД;
- надёжность работы объекта защиты в условиях рассматриваемых угроз;

– для экспертной модели:

- весовой коэффициент опасности реализации угрозы;
- величина информационного риска рассматриваемой угрозы;
- степень обеспечения безопасности работы объекта защиты КСЗИ;
- эффективность КСЗИ.

Возможно также построение *экономической* модели, включающей:

1. Определение размеров ущерба с использованием моделей «осведомленность – эффективность»;
2. Определение размеров ущерба с использованием экспертных оценок;
3. Определение упущенной выгоды в результате ограничений на распространение информации;
4. Определение затрат на защиту информации

Сложные модели оценки эффективности КСЗИ могут строиться и на совокупности вышеуказанных моделей.

Заключение

При разработке и проектировании систем реальных защиты информации желательно придерживаться определенных правил:

– создание и эксплуатация СЗИ является сложным и ответственным процессом, поэтому в трудных случаях не стесняйтесь обращаться к специалистам;

– не старайтесь организовать абсолютно надежную защиту – такой защиты просто не существует. Система ЗИ должна быть достаточной, надежной, эффективной и управляемой. Эффективность защиты информации достигается не количеством денег, потраченных на ее организацию, а ее способностью адекватно реагировать на все попытки НСД к информации;

– мероприятия по ЗИ от НСД должны носить комплексный характер, т.е. объединять разнородные меры противодействия угрозам (правовые, организационные, программно-технические);

– уязвимыми могут быть все основные объекты защиты, которые необходимо защищать от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников;

– основная угроза информационной безопасности компьютерных систем исходит непосредственно от сотрудников. С учетом этого необходимо максимально ограничивать как круг сотрудников, допускаемых к конфиденциальной информации, так и круг информации, к которой они допускаются (в том числе и к информации по системе защиты). При этом каждый сотрудник должен иметь минимум полномочий по доступу к конфиденциальной информации.

Тестовые вопросы

1. Основные виды защищаемой информации по содержанию:
1) секретная; 2) признаковая; 3) семантическая; 4) несекретная

2. Информацией, подлежащей защите, является…
1) информация о состоянии операционной системы;
2) сведения об окружающем мире; 3) информация, приносящая выгоду;
4) информация об учреждении профессионального образования

3. Показателями безопасности информации являются:

1) вероятность предотвращения угрозы;
2) время, в течение которого обеспечивается определенный уровень безопасности;
3) время, необходимое на взлом защиты информации;
4) вероятность возникновения угрозы информационной безопасности

4. Результатом реализации угроз ИБ может быть …
1) изменение конфигурации периферийных устройств;
2) уничтожение устройств ввода-вывода информации;
3) несанкционированный доступ к информации;
4) внедрение дезинформации в периферийные устройства

5. Абсолютная защита ПК от сетевых атак возможна при:
1) отсутствии соединения;
2) использовании лицензионного программного обеспечения;
3) установке межсетевого экрана;
4) использовании новейших антивирусных средств

6. В человеко-компьютерных системах необходимо обеспечивать ЗИ от трех угроз:
1) случайной потери или изменения; 2) преднамеренного искажения;
3) санкционированного просмотра; 4) сбоев оборудования;
5) резервного копирования

7. Угрозами информационной войны для РФ являются:

1) ориентированность на отечественные технические средства;
2) несовершенство законодательной базы;
3) значительная протяженность территории;
4) открытость границ

8. Брандмауэр (Firewall) – это…
1) графический редактор; 2) Интернет-браузер;
3) почтовая программа; 4) межсетевой экран

9. Принципиальным отличием межсетевых экранов (МЭ) от систем обнаружения атак или вторжений (СОВ) является то, что:
1) МЭ были разработаны для активной или пассивной защиты, а СОВ - для активного или пассивного обнаружения;
2) МЭ работает только на сетевом уровне, а СОВ ещё и на физическом;
3) МЭ были разработаны для активного или пассивного обнаружения, а СОВ - для активной или пассивной защиты;
4) МЭ работает только на физическом уровне, а СОВ ещё и на сетевом

10. Предотвратить проникновение вредоносных программ на подключенный к сети компьютер помогает…
1) резервное копирование данных; 2) электронная подпись;
3) наличие электронного ключа; 4) антивирусный монитор

11. Защитить личный электронный почтовый ящик от несанкционированного доступа позволяет …
1) скрытие личного пароля; 2) электронная подпись;
3) отключение компьютера; 4) включение режима сохранения логина

12. Наиболее защищёнными от несанкционированного доступа линиями связи на сегодня являются:
1) оптоволоконные; 2) электрические;
3) инфракрасные; 4) радио

ЭЦП

13. Для защиты содержимого письма электронной почты от несанкционированного ознакомления используется…
1) шифрование сообщения; 2) антивирусное средство;

3) электронно-цифровая подпись; 4) межсетевой экран

14. Электронно-цифровая подпись (ЭЦП) документа формируется на основе
1) самого документа; 2) перестановки элементов ключа;
3) сторонних данных; 4**)** специального вспомогательного документа

15. Электронно-цифровая подпись (ЭЦП) документа позволяет получателю
1) только удостовериться в истинности отправителя документа, но не проверить подлинность документа;
2) удостовериться в корректности отправителя документа и удостовериться в том, что документ не изменен во время передачи;
3) только удостовериться в том, что документ не изменен во время передачи;
4) либо удостовериться в корректности отправителя документа, либо удостовериться в том, что документ не изменен во время передачи

16. Электронно-цифровая подпись позволяет:
1) удостовериться в истинности отправителя и целостности сообщения;
2) восстановить повреждённое сообщение;
3) пересылать сообщение по секретному каналу;
4) зашифровать сообщение для сохранения его секретности

17. Электронно-цифровая подпись документа позволяет решить вопрос о:
1) подлинности документа; 2) секретности документа;
3) режиме доступа к документу; 4) ценности документа

18. Сжатый образ исходного текста обычно используется ...
1) для создания электронно-цифровой подписи;
2) в качестве ключа для шифрования текста;
3) как результат шифрования текста, отправляемого по незащищенному каналу;
4) как открытый ключ в симметричных алгоритмах

Вирусы

*19**.** Антивирусные программы, выполняющие после запуска проверку заданной области файловой структуры компьютера, называются …*
1) программы-вакцины; 2) антивирусные сканеры;
3) программы-брандмауэры; 4) антивирусные мониторы

20. Антивирусные программы, имитирующие заражение файлов компьютера вирусами, называют ….

1) программы - доктора; 2) программы – вакцины;

3) программы - брандмауэры; 4) программы – черви

Многие вирусные программы настроены на атаку только незараженных файлов. Программы-вакцины имитируют зараженность файлов и служат действенным средством сохранения важных файлов.

21.Основным путем заражения вирусами по сети является…

1) сообщение с интернет-пейджера; 2) SMS- сообщение;

3) почтовое сообщение; 4) HTML - документ

22. Вирусы могут быть: а) загрузочными; б) мутантами; в) невидимками; г) дефектными; д) логическими

1) а, б, в; 2) б, г, д; 3) в, г, д; 4) а, в, г

23. Основным средством антивирусной защиты является …

1) периодическая проверка компьютера с помощью антивирусного ПО;

2) периодическая проверка списка автоматически загружаемых программ;

3) периодическая проверка списка загруженных программ;

4) использование сетевых экранов при работе в сети Интернет

24. Антивирусной программой является…

1) DRWEB; 2) WIN.COM; 3) PKZIP; 4) ARJ

25. По типу маскировки вирусы делятся на:

1) самоидентифицирующиеся; 2) видимые;

3) условно резидентные; 4) невидимые

26. Чаще всего вирус передается с такой частью электронного письма, как …

1)тема; 2) адрес отправителя;

3)служебные заголовки; 4) вложение

27. Укажите 3 параметра, по которым можно классифицировать компьютерные вирусы

1) среда обитания; 2) степень полезности;
3) объем программы; 4) степень опасности;
5) способ заражения среды обитания

28. Основные действия (фазы), выполняемые компьютерным вирусом:
1) маскировка; 2) проявление; 3) заражение; 4) размножение

29. Укажите 3 группы разделения вирусов в зависимости от среды обитания
1) загрузочные; 2) интерфейсные; 3) сетевые;
4) реестровые; 5) файловые

30. Симптомами заражения являются:
1) уменьшение объема системной памяти и свободного места на диске без видимых причин;
2) периодическое мерцание экрана;
3) изменение длины файлов и даты создания;
4) замедление работы программ, зависание и перегрузка

31. В необходимый минимум средств защиты от вирусов входит:
1) аттестация помещения; 2) выходной контроль;
3) входной контроль; 4) архивирование;
5) профилактика

32. Сетевые черви – это:
1) программы, которые не изменяют файлы на дисках, а распространяются в компьютерной сети, проникают в ОС, находят адреса других компьютеров или пользователей и рассылают по этим адресам свои копии;
2) вредоносные программы, действие которых заключается в создании сбоев при питании компьютера от электрической сети;
3) программы, распространяющиеся только при помощи электронной почты;
4) программы, которые изменяют файлы на дисках

Литература

1. Алферов А.П., Зубов А.Ю. и др. Основы криптографии.: Гелиос АРВ, 2002. – 480 с.
2. Белов Е.Б., Лось В.П. и др. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия - Телеком, 2006. – 544 с.
3. Гатчин Ю.А., Климова Е.В. Ожиганов А.А. Основы информационной безопасности компьютерных систем и защиты государственной тайны: учебное пособие. - СПб: СПбГУ ИТМО, 2001. - 60 с.
4. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.
5. ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
6. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.
7. ГОСТ Р ИСО 7498–2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть1. Архитектура ЗИ.
8. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Академия, 2009. – 416 с.
9. Гришина Н. В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007. – 254 с.
10. Демин С. Л. Конспект лекций в виде презентации по дисциплине Комплексная защита информации (КЗИ).
11. Завгородний В. И. Комплексная защита информации в компьютерных системах: учебное пособие. – М.: Логос, 2001. – 264 с.
12. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации, 2006. – 256 с.
13. Малюк А.А. Введение в информационную безопасность: учебное пособие для студентов. – М.: Горячая линия - Телеком, 2011. – 288 с.
14. Пилиди В.С. Криптография. Вводные главы: Учебное пособие. - Ростов-на-Дону: ЮФУ, 2009. - 110 с.
15. Силаенков А.Н. Проектирование системы информационной безопасности: учебное пособие. – Омск: ОмГТУ, 2009. – 128 с.
16. Федеральный закон № 149-ФЗ Об информации, информационных технологиях и защите информации. – М., 2006.

17. Хорев П. Б. Методы и средства защиты информации в компьютерных системах 2005. – 256 с.

18. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – 2010. – 501 с.

19. Цирлов В.Л. Основы информационной безопасности. Краткий курс. – М.: Феникс, 2008. – 400 с.

20. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М: Форум: ИНФРА-М, 2009. – 415 с.

21. Щеглов А.Ю. Общие вопросы построения систем ЗИ.

22. Щекочихин О.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – Кострома: Изд. КГТУ, 2010. – 64 с.

23. http://www.eos.ru/eos_products/eos_karma/ETSP/

24. http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml – классификация угроз.

25. http://www.lghost.ru/lib/security/kurs5/theme01_chapter04.htm.

26. http://www.eusi.ru/lib/savgorodnij_kompleksnaja_sasita_informacii_v/2.shtml – Завгородний В. И.

27. http://www.hr-portal.ru/article/kak-samomu-napisat-kontseptsiyu-informatsionnoi-bezopasnosti

28. http://www.intuit.ru/department/security/secbasics/9/3.html – Галатенко В.А. Основы ИБ.

29. http://www.topsbi.ru/default.asp?artID=998 (Голов 140611)

30. http://www.cyberpol.ru/cybercrime.shtml#p_01

31. http://kszi.ucoz.ru/ - конспект лекций

32. http://www.kgau.ru/istiki/umk/pis/l24.htm – Основные понятия и методы защиты данных (НСД)

33. http://zashita-informacii.ru/node/119 – причины и виды утечки инф.

34. http://frela-21.narod.ru/kzip/kzip.doc – Попов В.В. (МАИ – конспект).

35. http://zi-kimes.my1.ru/load/0-0-0-84-20 (84_sdA – книга)

Приложение. Основные компьютерные преступления

Компьютерная информация (computer information) – это информация, находящаяся в памяти ЭВМ, зафиксированная на машинных или иных носителях в электронно-цифровой форме, или передающаяся по каналам связи посредством электромагнитных сигналов с реквизитами, позволяющими ее идентифицировать.

Компьютерные преступления (computer crime) – это преступления, совершенные с использованием компьютерной информации, которая является предметом и/или средством совершения преступления.

В соответствии с пунктом 1 ст. 16 Федерального закона "Об информации, информационных технологиях и о защите информации", преступными деяниями в отношении компьютерной информации являются: *уничтожение, модификация, копирование, блокирование, предоставление и распространение*.

Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28-ой УК РФ.

Преступными являются следующие виды деяний:

1. Неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК).

2. Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК).

3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).

Чаще всего компьютерная информация используется для совершения следующих преступлений:

1) нарушение авторских и смежных прав (ст. 146 УК);

2) мошенничество (ст. 159 УК);

3) подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК);

4) изготовление или сбыт поддельных кредитных или расчетных карт, а также иных платежных документов (ст. 187 УК);

5) изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК);

6) причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК) - при незаконном использовании чужого логина и пароля доступа к ресурсам сети "Интернет";

7) уклонение от уплаты налогов с организаций (ст. 199 УК);

8) нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК);

9) незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК);

10) незаконное распространение порнографических материалов (ст. 242 УК);

11) изготовление и оборот материалов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК);

12) незаконное предпринимательство (ст. 171 УК).

Классификация компьютерных преступлений по кодификатору Интерпола

Интерпол в 1991 году разработал кодификатор компьютерных преступлений [30], используемый в 120 странах мира. Все коды, характеризующие компьютерные преступления имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

1. QA – Несанкционированный доступ и перехват:

– *«компьютерный абордаж»* (hacking - "хакинг"): доступ в компьютер или чужую информационную сеть без права на это;

– *перехват* (interception): перехват без права на это с помощью технических средств при использовании линий связи и проводных коммуникаций, а также электромагнитного излучения компьютерного оборудования.

Для характеристики методов НСД и перехвата информации используется следующая специфическая терминология:

- Жучок" (bugging) - установка микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
- "Откачивание данных" (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных в частности о технологии ее прохождения в системе;
- "Уборка мусора" (scavening) - поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и прочих технологических отходов. Электродный вариант требует исследования данных, оставленных в памяти ЭВМ;

- "За дураком" (piggbacking) - состоит в несанкционированном проникновении в пространственные (охраняемые помещения) либо в электронные (программные) закрытые зоны;
- "За хвост" (between the lines entry) - несанкционированное негласное подключение к линии электросвязи законного пользователя в момент его работы в сети ЭВМ. После завершения работы и отключения от сети негласно подключенный компьютер преступника продолжает работу в сети по его идентификаторам (паролю доступа в сеть);
- "Неспешный выбор" (browsing). В этом случае НСД к БД и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем ЭВМ. Однажды обнаружив их, правонарушитель может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;
- "Поиск бреши" (trapdoor entry) - используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
- "Люк" (trapdoor) - является развитием предыдущего алгоритма преступления. В найденной "бреши" программа "разрывается" и туда встраиваются определенное коды управляющих команд. По мере необходимости "люк" открывается, а встроенные команды автоматически обеспечивают НСД к данным;
- "Маскарад" (masquerading). Злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
- "Мистификация" (spoofing) - используется при случайном подключении "чужой" системы. Правонарушитель, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него конфиденциальную информацию, например коды доступа в сеть ЭВМ либо сведения, позволяющие идентифицировать пользователя.

– *кража времени*: неоплата услуг доступа в систему или сеть ЭВМ.

2. QD – Изменение компьютерных данных:

– *логическая бомба* (logic bomb), - тайное встраивание в программу для ЭВМ вредоносной программы (программного модуля), которая должна сработать только при наступлении определенных логических условий;

– *троянский конь* (trojan horse) - тайное введение в чужое ПО вредонос-

ной программы, которая позволяют негласно осуществлять не планировавшиеся разработчиком программы функции. Эти средства используют для негласного добывания конфиденциальных сведений, например, логина и пароля доступа в сеть Интернет;

– *троянская матрешка* - автоматический конструктор для создания вредоносных программ по заданному преступником алгоритму. Она камуфлируется под обычные программы для ЭВМ. При попадании в программную среду компьютера автоматически срабатывает алгоритм создания модулей для циклического построения вредоносной программы. Циклы могут повторяться многократно (количество "реинкарнаций" или перевоплощений определяется преступником), как матрешки, встроенные друг в друга;

– *вирус* (virus) - вредоносная программа, которая заведомо приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, их системы или сети;

– *червь* – саморазмножающийся и самораспространяющийся вирус, специально созданный для функционирования в сети ЭВМ.

В отличие от обычного вируса, распространяемого в виде отдельного файла данных, эта вредоносная программа хранит свои модули на нескольких компьютерах - рабочих станциях сети. При уничтожении одного или нескольких модулей на соответствующем числе рабочих станций, она автоматически воссоздает их после каждого подключения "вылеченного" компьютера к сети - как разрезанный на части дождевой червяк отращивает новые, недостающие участки тела.

Червь, помимо своего оригинального алгоритма, может являться "средством передвижения" (распространения) обычных вирусов, троянских коней и матрешек, а также логических бомб.

3. QF – Компьютерное мошенничество (computer fraud):

– компьютерные мошенничества, связанные с хищением наличных денег из банкоматов;

– компьютерные подделки: мошенничества и хищения из КС путем создания поддельных устройств (пластиковых карт, сотовых "двойников" и пр.);

– мошенничества и хищения, связанные с игровыми автоматами;

– манипуляции с программами ввода-вывода: мошенничества и хищения путем неверного ввода или вывода в компьютерные системы. Сюда же включается метод *подмены данных кода* (data diddling code change). Таким образом,

можно заставить ЭВМ оплачивать несостоявшиеся услуги, переводить платежи и не имевшие место закупки, формировать ложный курс на бирже и т.д.;

– компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с хищением денежных средств, которые составляют около 45% всех преступлений;

– телефонное мошенничество (Phreaking – фрикинг): доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих системы электросвязи.

4. QR – Незаконное копирование («пиратство»):

– незаконное копирование, распространение или опубликование компьютерных игр и другого ПО, защищенного законом об авторском праве и смежных правах (контрафактной продукции);

– незаконное копирование топологии полупроводниковых изделий: копирование защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на это.

5. QS – Компьютерный саботаж

– саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу КС с намерением помешать функционированию компьютерной или телекоммуникационной системы;

– компьютерный саботаж с ПО: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на это.

6. QZ – Прочие компьютерные преступления:

– использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

– хищение информации, составляющей коммерческую тайну (приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на это или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества);

– использование КС или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого были определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА ПРОЕКТИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

1945 - 1966 РЛПУ (кафедра радиолокационных приборов и устройств). Решением Правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения. Приказом по Институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д. т. н., профессор Зилитинкевич СИ. (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. - радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Мишин Б.С., доцент Захаров И.П.. доцент Иванов А Н .

1966 - 1970 КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско-технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер - конструктор - технолог РЭА.

Заведовал кафедрой доцент Иванов А Н .

1970 - 1988 КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям: автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. Новиков В.В. (до 1976 г.), затем проф. Петухов Г.А.

1988 - 1997 МАП (кафедра микроэлектроники и автоматизации проектирования) Кафедра выпускала инженеров - конструкторов - технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям - разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. Арустамов С.А , затем снова проф. Петухов Г.А.

С 1997 ПКС (кафедра). Кафедра выпускает инженеров по специальности Проектирование и технология электронно-вычислительных средств. Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кроме того, кафедра готовит специалистов по специальности 2206 - Организация и технология защиты информации, причем основное внимание уделяется программно-аппаратной защите информации компьютерных систем.

С 1996 г. кафедрой заведует д.т.н., профессор Гатчин Ю.А.

С 2011 г. носит название кафедра Проектирования и безопасности компьютерных систем.

Гатчин Юрий Арменакович
Климова Елена Владимировна

Введение в комплексную защиту объектов информатизации

Учебное пособие

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати 01.11.11
Заказ № 2408
Тираж 100 экз.
Отпечатано на ризографе