Содержание:

ВВЕДЕНИЕ

Защита информационных ресурсов обеспечивается различными методами и средствами, обеспечивающими безопасность и целостность данных. Средства защиты переделяются степенью подготовленности нарушителя. Кроме этого различают виды нарушений с позиции нарушителя: умышленное и неумышленное нарушение.

В процессе обеспечения защиты информации используются разнообразные методы. Среди них можно отметить следующие: законодательный, организационный, технический, математический, программный, а так же стоит отметить морально-этический. Широко распространены разнообразные программные методы, значительно расширяющие возможности в обеспечении безопасности хранящейся информации.

С целью получить объективные качественные и количественные оценки о состоянии вопроса обеспечения информационной безопасности в Российской Федерации, угроз безопасности информационных ресурсов в соответствии с некоторыми критериями оценки и показателями безопасности производится настоящая работа.

Тема данной курсовой работы — «Виды и состав угроз информационной безопасности».

Данная тематика является актуальной, так как на данный момент наблюдается рост различных информационных рисков, связанный с появлением разнообразных технических средств, увеличением компьютерной грамотности населения, ростом числа ЭВМ, распространению доступа к информационным ресурсам разнообразного характера и так далее.

Анализ и изучение данной тематики дает возможность определить наиболее эффективные мероприятия для предотвращения угроз безопасности информационным ресурсам. Опираясь на анализ эффективности системы защиты информации, легко производить корректировки понимания угроз безопасности информации, оценки угроз и соответствующих действий. Кроме того, результаты

анализа безопасности дают возможность увидеть минимизацию параметров уязвимости, что усиливает режим IT-безопасности в целом.

Цель исследования данной курсовой работы – исследование угроз информационной безопасности, их вида и состава.

Объект исследования – угрозы информационной безопасности, методы обеспечения информационной безопасности.

При написании курсовой работы были применены такие методы научного исследования, как изучение научной литературы по теме исследования, нормативно-правовой базы, аналитический и сравнительный методы. Среди теоретических методов, используемых при разработке курсовой работы, отмечу анализ, а так же метод классификации. Практические методы, используемые в работе – наблюдение, сравнение, которые использовались, в частности, при оценке эффективности систем защиты информации.

Современное законодательство РФ и других стран предусматривает ряд мер ответственности за нарушения в сфере защиты персональных данных, поэтому нарушения законодательства в данной области могут в значительной степени навредить деятельности как отдельных компаний, так и государству в целом.

1 Теоретические аспекты анализа угроз информационной безопасности

1.1 Нормативно-правовая база в области информационной безопасности

С целью понимания законодательной базы исследуемой тематики, рассмотрим наиболее важные законодательные акты, касающиеся этой сферы.

В первые в российской практике закон «О правовой охране программ...» определил понятия, правовые конструкции и термины, которые касаются основных объектов охраняемой сферы. Так, к примеру, в главе 1 данного закона дано определение терминов: «программа для ЭВМ», «база данных», «модификация программы», а так же некоторых других. Программы для компьютеров, а так же базы данных

отнесены к непосредственным объектам авторского права [15].

Закон Российской Федерации «Об авторском праве и смежных правах» произвел регуляцию отношений, возникающих в процессе создания и использования произведений науки, искусства и литературы (авторское право), фонограмм, передач эфирного вещания, исполнением постановок (смежные права). Данный закон - один из основных в системе информационного законодательства РФ. Он уточняет и определяет ряд формулировок, которые касаются авторских, а так же смежных прав на программы для персональных компьютеров.

Закон Российской Федерации «О государственной тайне» определил отношения в сфере защиты информации, когда последняя относится к государственной тайне. Так как главная цель принятия этого закона — гарантии безопасности РФ в информационной сфере, в нем определяются базовые понятия, которые касаются специальных информационных взаимоотношений. Данный закон закрепляет определение «носителей сведений, которые составляют государственную тайну». К данным сведениям отнесены совокупность материальных объектов, в том числе и физических полей, в которых сведения, относящиеся к государственной тайне, определяют свое отражение в качестве символов, сигналов, технических решений. Важный момент - это приведенная в данном законе классификация средств информационной защиты, а именно: технические, программные, а так же другие средства контроля эффективности информационной защиты. Определены в указанном законе и порядки доступа к сведениям, которые составляют государственную тайну.

Федеральный закон Российской федерации «Об обязательном экземпляре документов» впервые ввел понятие «документ». Согласно данному определению (ст. 1), документом является «материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, который предназначен для передачи во времени и пространстве с целью общественного использования и хранения». Из данного определения следует, что документом является сам носитель при условии фиксации на нем в установленном законодателем виде конкретных сведений [18].

Федеральный закон РФ «О связи» определяет правовые основы деятельности в сфере связи, а так же полномочия органов власти, права и обязанности должностных лиц, которые участвуют в деятельности в данной области или пользуют услуги связи.

Данный закон определяет, что различные виды связи функционируют на территории РФ и на территориях, которые находятся под юрисдикцией РФ, как взаимосвязанный производственно-хозяйственный комплекс, который предназначен для оказания услуг связи любому пользователю, а так же обеспечения деятельности организаций, управления процессами производства, для нужд государственного аппарата, обороны государства, безопасности страны. Федеральную связь формирует вся совокупность организаций, а так же государственные органы, которые осуществляют и обеспечивают связь на территории РФ. Материальная и техническая основа федеральной связи формируется единой сетью электросвязи РФ, состоящей из сети связи общей доступности, выделенных сетей связи, сетей связи специальных назначений, а так же других сетей связи, функционирующих для передачи данных с помощью электромагнитных систем. Та к же в формировании материальной и технической основы федеральной связи учувствует сеть почтовой связи РФ.

Конституция РФ гарантирует тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и других сообщений (п. 2 ст. 23). Детальное развитие данные положения нашли в ФЗ «О связи». В статье 63 данного закона указывается, что «на территории РФ гарантируется тайна переписки, телефонных переговоров, телеграфных и иных сообщений, которые передаются по сетям связи. Введение ограничения на право тайны переписки, телефонных переговоров, почтовых отправлений, которые передаются по сетям связи, допускается исключительно в случаях, которые предусмотрены федеральными законами». Необходимость обеспечить соблюдение тайны связи возложена на непосредственных операторов связи. Помимо этого, операторы связи должны соблюдать сохранность личной информации абонентов, а так же оказываемых им услугах связи, которые стали известными операторам в процессе выполнения профессиональных обязательств (ст. 53).

С целью обеспечить надежность функционирования и безопасность сети связи, а, следовательно, и информационную безопасность, данный закон определяет совокупность положений об обязательном лицензировании деятельности в сфере услуг связи (ст. 29) и о утверждении соответствия средств связи, а так же услуг связи в форме сертификатов и деклараций соответствия (ст. 41).

Вышеуказанный закон разграничивает ответственность при нарушении законодательства России в сфере связи: «лица, которые нарушили законодательство РФ в сфере связи, несут уголовную, административную и гражданско-правовую ответственность» (ст. 68 Федерального закона «О связи»).

ФЗ РФ «Об информации, информационных технологиях и о защите информации», который заменил собой ФЗ от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», регулирует отношения, возникающие в процессе:

- осуществления прав на получение, передачу, производство, а так же распространение данных;

- применения информационных ресурсов;

- обеспечения защиты конфиденциальной информации и данных.

Указанный закон не затрагивает отношений, которые регулируются законодательством, касающимся интеллектуальной собственности (ч. 2 ст. 1).

Данный закон регламентирует отношения в сфере информации, устанавливая права и обязанности субъектов информации, определяя ответственность при правонарушениях в области информации.

Помимо законов на начальных этапах деятельности по созданию и модернизации законодательства в области защиты информации изданы соответствующие указы Президента РФ.

Президент утвердил Доктрину информационной безопасности РФ.

Указанная доктрина является совокупностью официальных взглядов на цели, принципы, основные направления и задачи в сфере обеспечения информационной безопасности РФ. Доктрина развивает Концепцию национальной безопасности РФ относительно информационной сферы.

Большую значимость имеют следующие положения указанной Доктрины.

Информационная безопасность РФ определяется в Доктрине, как состояние защищенности интересов РФ в сфере информации и информационных технологий, которые определяются совокупностью сбалансированных интересов личности, а так же общества и государства в целом.

Доктрина определяет в числе угроз информационной безопасности РФ угрозы конституционным правам человека и гражданина в сфере духовной и личной жизни, а так же информационной деятельности.

Значимое место в Доктрине имеют особенности обеспечения информационной безопасности в области экономики, которая играет огромную роль в формировании национальной безопасности РФ (п. 6 разд. II) [19].

В данный момент законодательная база, касающаяся обеспечения защиты информации в РФ находится в состоянии формирования. Однако процесс ее развитие и совершенствования происходит значительными темпами.

1.2 Угрозы и нарушители безопасности информации

Угрозы информационной безопасности возникают на различных этапах их функционирования информационных систем. Под данными этапами понимается использование информационных ресурсов, хранение, обработка информации в ИС и так далее.

Объекты атак на данных этапах – это совокупность технических, программных и информационных средств ИС.

Угрозы безопасности информационным ресурсам и программно-аппаратному обеспечению возникают как в процессе их рабочей эксплуатации, так и при разработке ПО. Этот аспект особенно характерен для разработки программно-аппаратного обеспечения, разработки баз данных, а так же других компонентов компьютерных систем (КС).

Цели атак:

- получение сведений об информационных средствах;
- внесение различных уязвимостей в средства информационной системы ИС;
- внесение несанкционированных изменений в электронную документацию;
- хищение информации;
- нарушение конфигурации средств информационной системы баз данных.

Потенциальных нарушителей, которые могут нанести вышеуказанный вред информационным ресурсам ИС, классифицируют на нарушителей:

- внешних, которые не имеют санкционированных возможностей для объекта доступа в контролируемую зону ИС;

- внутренних, которые имеют постоянный или разовый доступ в контролируемую зону.

Классификация нарушителей относительно возможностей доступа к компонентам узлов информационной системы приведена на рисунке в приложении 1.

Нарушители - это отдельные лица, которые ведут злоумышленную деятельность относительно информационных ресурсов защищаемых объектов.

Нарушители включают [15]:

- посетителей;
- некоторые категории обсуживающего персонала и представители ремонтных организаций объектов защиты, которые не имеют доступ к компонентам БД.

- представителей эксплуатационных и обслуживающих служб, которые находятся в пределах контролируемой зоны на постоянной основе или периодически. Нарушители данного типа не обладают техническими средствами и доступом к программному обеспечению БД.

- сотрудников объекта защиты, которые не являются операторами ИС.

- сотрудников, которые являются операторами рабочих мест информационной системы и имеют непосредственный доступ к информационным ресурсам БД.

- сотрудников, которые осуществляют обслуживание узлов БД постоянно.

Основные атаки на информационные ресурсы БД осуществляются с помощью:

- внешних каналов связи, не защищенных от НСД к информационным ресурсам организационными и техническими мерами;
- штатных средств;
- каналами непосредственного доступа к объектам атак;
- машинных носителей информации;
- носителей информации, выведенных из употребления.

В процессе решения проблем роста уровня защищенности программно-аппаратных средств следует исходить из того, что самыми вероятными объектами воздействия будут выступать программно-аппаратные средства, которые выполняют функции получения, распределения, обработки, а так же хранения информационных ресурсов.

На сегодняшний день одни из самых опасных средств деструктивного воздействия на программно-аппаратные компоненты - это компьютерные вирусы.

Компьютерный вирус - это программа, которая способна наносить определенный вред, размножаться, прикрепляться к другим программным продуктам, распространяться по телекоммуникационным каналам.

Основные средства деструктивного воздействия на программно-аппаратные компоненты, наряду с вирусными программами, - это так называемые алгоритмические и программные закладки.

Алгоритмическая закладка - это преднамеренное искажение некоторой части алгоритма решения задачи, либо выстраивание его таким образом, что в результате финишной программной реализации данного алгоритма в составе программных компонентов или комплексов, последние будут ограничены в выполнении должных функций или не выполнять их вообще.

Программная закладка - это совокупность операторов или операндов, преднамеренно включаемую в состав реализуемого кода программного средства на каком-либо этапе его разработки в завуалированной форме.

Деструктивные воздействия алгоритмических и программных закладок можно классифицировать следующим образом:

- изменение функционирования программно-аппаратных компонентов компьютерных систем;

- несанкционированный доступ к информационным ресурсам;

- несанкционированная модификация данных, вплоть до их полного уничтожения.

В последнем пункте вышеприведенной классификации под информацией необходимо понимать как какие-либо информационные данные, так и коды программных средств. Необходимо отметить, что указанные классы вредоносных воздействий могут пересекаться.

Проанализируем более подробно результаты деструктивных воздействий.

В первом классе воздействий необходимо выделить:

- снижение скорости работы программно-аппаратных средств;
- частичная либо полная блокировка работы программно-аппаратных средств;

- имитация физических либо аппаратурных сбоев работы программно-аппаратных средств;
- переадресация информационных сообщений;
- получение доступа в систему для непредусмотренных устройств.

Несанкционированный доступ к информационным ресурсам, осуществляемый в автоматизированных системах, направлен на:

- получение паролей конкретных пользователей;
- получение доступа к конфиденциальной информации;
- идентификацию данных, запрашиваемых пользователями;
- осуществление подмены паролей с целью доступа к данным.

Несанкционированная модификация информационных ресурсов - это наиболее опасная разновидность воздействий программных закладок, так как приводит к значительным последствиям. В данном классе воздействий следует отметить:

- разрушение информационных ресурсов и кодов программ;
- внесение трудно обнаруживаемых изменений в информационные массивы данных;
- внедрение программных закладок в рабочие программы и подпрограммы;
- модификация пакетов данных.

Из всего вышесказанного следует, что алгоритмические и программные закладки обладают широким спектром воздействий на информационные ресурсы, обрабатываемые вычислительными средствами, а так же на программно-аппаратные средства. При осуществлении контроля технологической безопасности программно-аппаратных средств следует учитывать их назначение, состав аппаратных средств, а так же общесистемного программного обеспечения.

Для пресечения незаконных действий с программно-аппаратными средствами имеют место нижеприведенные сценарии поведения:

- получение новых версий программных продуктов;

- возможность получения оперативных консультаций;

- проведение образовательных мероприятий по использованию программно-аппаратного обеспечения.

Рассмотренные деструктивные программные средства по своей природе носят разрушительный и вредоносный характер. Последствия их применения могут приводить к значительному и даже непоправимому ущербу в различных областях человеческой деятельности, где использование компьютерных систем и программно-аппаратных средств является необходимостью.

2 Анализ современных угроз информационной безопасности и борьба с ними

2.1 Современные угрозы информационной безопасности

Произведем исследование наиболее вероятных угроз информационной безопасности в нашей стране.

При обработке информации локальных ИС, имеющих подключения к сетям связи общего пользования, возможна реализация следующих угроз безопасности:

- угрозы утечки информации по техническим каналам;

- угрозы НСД к конфиденциальной информации.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки акустической (речевой) информации;

- угрозы утечки видовой информации;

- угрозы утечки информации по каналу ПЭМИН.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИС, возможно при наличии функций голосового ввода в ИС или функций воспроизведения информации акустическими средствами ИС.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники,

информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС.

Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

Угрозы НСД в локальных ИС связаны с действиями нарушителей, имеющих доступ к ИС, включая пользователей ИС, реализующих угрозы непосредственно в ИС.

Угрозы НСД в ИС, связанные с действиями нарушителей, имеющих доступ к ИС, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Кроме этого, источниками угроз НСД к информации в АРМ могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИС на базе распределенных АРМ возможны:

- угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

- угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);

- угрозы внедрения вредоносных программ.

Кроме того, в такой ИС могут иметь место:

- угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

- угрозы выявления паролей;

- угрозы удаленного запуска приложений;

- угрозы внедрения по сети вредоносных программ.

Список самых опасных угроз ИБ составляют такие угрозы как кража информации (64%), вредоносные программы (49%), хакерские атаки (48%), спам (45%) и халатность сотрудников (43%).

Сегодня вирусы и хакеры больше напоминают неизбежное зло, которое все знают и уже не воспринимают как нечто из ряда вон выходящее.

Минимизировать риск искажения или уничтожения информации можно при помощи резервных копий. Сбои информационной системы, как и кража оборудования тоже явления некритичные и легко восполнимые. Утечка же всего одного документа может стоить миллионов. А то и полного банкротства.

Совокупность угроз ИБ в общем случае можно классифицировать на угрозы внешнего и внутреннего характера.

Источником внешней угрозы может выступать любой человек, у которого нет санкционированного доступа к защищаемой системе. Источником внутренней угрозы могут быть люди, у которых есть санкционированный доступ к защищаемой системе (администраторы, конечные пользователи, разработчики приложений).

К внешним воздействующим факторам, которые создают угрозы можно отнести следующие:

- целенаправленные, деструктивные действия лиц, целью которых является искажение, уничтожение или хищение программ, данных и документов системы;

- целенаправленное воздействие на каналы передачи информации, поступающей от внешних источников, с целью вызвать отказ в обслуживании;

- неправильная работа или вообще остановка аппаратуры вычислительных средств.

Среди внутренних угроз можно выделить следующие атаки:

- атаки со стороны авторизованных пользователей;

- непреднамеренные ошибки сотрудников, нарушающих по разным причинам установленную политику безопасности, или некорректно построенная политика безопасности;

- умышленное изменение или искажение хранимых данных.

Атаки на ОС, в которых функционирует информационная система, - наиболее частый вид атак. Возможность практической реализации той или иной атаки на ОС в значительной мере определяется архитектурой и конфигурацией ОС.

Тем не менее, существуют атаки, которые могут быть направлены практически на любые ОС. Рассмотрим их.

1. Воровство ключевой информации. Эта атака может реализовываться с использованием следующих методов:

- получение пароля визуальным способом при его вводе пользователем;

- кража пароля из командного файла;

- перехват пароля программной закладкой.

2. Подбирание пароля. В данном случае применяются следующие способы:

- неоптимизированный перебор. При этом происходит последовательное перебирание всех возможных вариантов пароля. Очевидно, что для паролей длиннее шести символов этот способ занимает много времени и является малоэффективным;

- перебор, опирающийся на статистику появления символов и биграмм. Разные символы встречаются в паролях пользователей с разной вероятностью. По имеющимся результатам исследований, символы встречаются в алфавите паролей с частотой, сходной с частотой их встречаемости в обычном естественном языке. Поэтому, практически этот метод выглядит как подбор вначале паролей, в которых встречаются символы с наибольшей частотой появления, при этом время перебора заметно снижается. В некоторых случаях при подборе паролей применяется не только частота появления символов, но и статистика появления биграмм и триграмм, которые являются комбинаций двух и трех последовательных символов. Для реализации этого способа существует огромное количество программ, основной целью которых является взлом операционной системы. При этом выделяются две ключевые технологии взлома: явный подбор пароля путем их подачи на вход системы аутентификации, а также вычисление значения хэш-функции с последующим его сравнением с известным образом пароля;

- перебор, оптимизация которого достигается благодаря использованию словарей вероятных паролей. Используя этот метод подбора паролей, злоумышленник вначале осуществляет пробный ввод в качестве пароля всех слов из содержащего

наиболее вероятные пароли словаря. Если успех не достигнут, возможен подбор из комбинаций слов, содержащихся в словаре, добавления к началу или к концу слов, содержащихся в словаре, одного или нескольких знаков, таких как цифра, знак препинания, буква и т.д.;

- перебор, оптимизация которого организована на основе полученных сведений о пользователе. Для этого случая характерен подбор пароля злоумышленником по принципу наиболее вероятных паролей, которые мог использовать сотрудник (естественно, по мнению злоумышленника). В качестве таких паролей традиционно выступают паспортные данные (имя, фамилия, дата рождения, номер телефона, имя супруги и т.д.);

- перебор, оптимизация которого основана на базе применения знаний о существующей подсистеме аутентификации операционной системы. При допустимости существования эквивалентных паролей (определяется конкретной ключевой системой ОС), для перебора из каждого класса эквивалентности достаточно опробовать только один пароль.

Очевидно, что наиболее вероятно комплексное применение злоумышленником вышеперечисленных методов.

3. Попытка атаки на систему посредством сканирования доступных сетевых ресурсов (случай, когда злоумышленник имеет легальный доступ в систему). Суть данной атаки состоит в операции последовательного считывания файлов, которые хранятся на жестких дисках компьютера. В случае отказа при обращении к конкретному файлу (либо каталогу) злоумышленником выполняется дальнейшее сканирование. При большом количестве пользователей и не очень разумно построенной политике безопасности (например, разрешение самостоятельного создания пользователям доступных сетевых ресурсов), есть вероятность проникновения в систему через доступный ресурс. Следовательно, в процессе такой атаки произойдет считывание злоумышленником содержимого всех файлов, по отношению к которым были допущены ошибки. Такой метод применим не только для сканирования содержимого жестких дисков персонального компьютера, но и для сканирования содержимого разделяемых ресурсов локальной сети.

4. Превышение полномочий. В процессе анализа и использования ошибок, найденных в программном обеспечении или на этапе администрирования операционной системы, злоумышленник наделяет себя правами, намного превышающими полагающимися ему действующей политикой безопасности.

Превышение полномочий достигается следующими путями:

- при запуске программы от имени пользователя, наделенного достаточными полномочиями;

- при запуске программы в роли системной программы (то есть, как сервиса, демона, драйвера), исполняемой от имени операционной системы;

- в результате подмены динамически подгружаемой библиотеки, которую используют системные программы, либо несанкционированного изменения переменных среды, содержащих информацию о пути к такой библиотеке;

- при модификации кода или данных подсистемы защиты операционной системы.

5. Атаки класса «Отказ в обслуживании». Целью таких атак является осуществление полного или хотя бы частичного вывода операционной системы компьютера из строя. Данный класс атак можно подразделить на:

- атаки, связанные с захватом ресурсов – программой осуществляется захват всех ресурсов компьютера, каких возможно. Например, происходит присваивание программой самой себе наивысшего приоритета с последующим уходом в так называемый вечный цикл;

- атаки, связанные с бомбардировкой трудновыполнимыми запросами – происходит отправка программой (которая при этом находится в вечном цикле) операционной системе запросов;

- атаки, связанные с отправкой заведомо бессмысленных запросов – программой, находящейся в вечном цикле, происходит отправка операционной системе заведомо бессмысленных (часто, случайно генерируемых) запросов;

- наиболее очевидный вид атак, связанных с применением известных ошибок в программном обеспечении или недочетов в администрировании операционной системы.

Самыми опасными атаками для информационной системы являются атаки из сетей передачи данных. Это связано со спецификой и разнообразием используемых в сетях протоколов, а также использованием автономных программ небольшого размера, которые могут быть загружены в компьютерные системы пользователей. Эти протоколы и активные элементы способны создать серьезную угрозу для безопасности системы.

Среди внутренних ИТ-угроз абсолютное лидерство занимет угроза «Нарушение конфиденциальности информации». Все без исключения российские организации считают эту проблему самой злободневной. Интересно заметить, что крупные и часть средних компаний рассматривают ее с внутрикорпоративной точки зрения (защита собственных активов), а малые предприятия - с точки зрения ситуации в стране в целом.

Чем крупнее организация, тем более актуальной для нее является проблема сохранности конфиденциальности.

После анализа путей утечки данных, можно утверждать, что наибольшей незащищенностью характеризуются мобильные накопители информации. Этот показатель стремительно вырвался вперед и даже опережает электронную почту.

Объяснение такому положению вещей кроется в современных методах кражи информации. Как известно, российская специфика этой отрасли кибер-преступности заключается в хищении крупных баз данных. Их объемы достигают нескольких сотен гигабайт, которые можно унести только используя только высокоемкие накопители информации, например, съемные жесткие диски, флэш-карты, CD/DVD диски и т.п. Передать такие объемы данных по электронной почте или Интернету не представляется возможным. Тем более что пересылка этими средствами протоколируется, может быть заблокирована и использована в качестве доказательства вины злоумышленника. Наконец, далеко не во всех организациях разрешен свободный доступ к почте и существует прямое подключение к другим сетевым сервисам.

Подход к обеспечению конфиденциальности информации должен быть комплексным. Необходимо контролировать все каналы утечки без исключения. В обратном случае данные «утекут» через малейшую неучтенную брешь и все усилия по их безопасности окажутся напрасны.

В целом изменения в стране за последние 5-7 лет с точки зрения защиты конфиденциальной информации и устранения угроз можно признать положительными, хотя общей ситуации далеко до идеала.

2.2 Предлагаемые стратегии обеспечения информационной безопасности для различных

угроз ИБ

Рассмотрим три методики обеспечения информационной безопасности.

Анализируемые методики приведены в таблице 2.

Выбор оборонительной методики означает, что если исключить вмешательство в процесс функционирования информационной системы, то можно нейтрализовать лишь наиболее опасные угрозы. Обычно это достигается построением «защитной оболочки», включающей разработку дополнительных организационных мер, создание программных средств допуска к ресурсам информационной системы в целом, использованию технических средств контроля помещений, в которых расположено терминальное и серверное оборудование.

Таблица 2 - Анализируемые методики обеспечения информационной безопасности

Учитываемые угрозы	**Влияние на информационные системы**		
	отсутствует	**частичное**	**существенное**
Наиболее опасные	Оборонительная стратегия		
Все идентифицированные угрозы		Наступательная стратегия	
Все потенциально возможные			Упреждающая стратегия

Наступательная методики предусматривает активное противодействие известным угрозам, влияющим на информационную безопасность системы. Наступательная методики может включать установку дополнительных программно-аппаратных средств аутентификации пользователей, внедрение более совершенных

технологий разгрузки и восстановления данных, повышение доступности системы с использованием резервирования.

Упреждающая методики предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы. Важной частью упреждающей методики является оперативный анализ информации центров изучения проблем информационной безопасности, изучение отечественного и мирового передового опыта, проведение независимого аудита уровня обеспечения безопасности информационных ресурсов организации.

Отмечу, что наиболее эффективной методикой обеспечения информационной безопасности является упреждающая методика, которая позволяет исключить и пресечь абсолютное большинство угроз безопасности информационных ресурсов.

Для наступательной методики алгоритм включает следующие операции:

1. Постановка задачи, уточнение границ работ.

2. Сбор и анализ информации.

3. Проведение анализа рисков.

4. Разработка рекомендаций по улучшению информационной безопасности.

Рассмотрим более подробно описание каждого этапа упреждающей стратегии.

1. Постановка задачи, уточнение границ работ.

Данный этап включает сбор необходимых исходных данных, проведение их предварительного анализа, проведение организационных мер, касающихся подготовки анализа информационной безопасности, а именно:

• Уточнение целей и задач анализа ИБ.

• Формирование рабочей группы для проведения анализа ИБ.

2. Анализ информационных ресурсов исследуемого объекта.

На данном этапе происходит сбор информационных ресурсов, оцениваются следующие меры и средства информационной безопасности объекта исследования:

• организационные меры в сфере ИБ;

• программно-технические средства информационной безопасности;

• обеспечение физического уровня безопасности.

Проводится анализ характеристик выстраивания и функционирования корпоративных информационных систем, а именно:

• Организационных характеристик;

• Организационно-технических характеристик;

• Технических характеристик, которые связаны с архитектурой информационной системы;

• Технических характеристик, которые связаны непосредственно с конфигурацией устройств сети и серверов информационной системы;

• Технических характеристик, которые связаны с функционированием механизмов информационной безопасности.

Когда все исходные данные получены, формируется отчет об обследовании. Данный отчет является базой для следующих этапов анализа ИБ — анализ рисков и разработка рекомендаций по улучшению ИБ.

3. Процедура проведения анализа информационных рисков.

Процедура анализа рисков производится с целью оценить реальные угрозы нарушения режима защиты информации и формирования предложений, выполнение которых даст возможность минимизировать данные угрозы безопасности информации. Исходная информация для анализа информационных рисков — это согласованный с компанией-заказчиком отчет о произведенном обследовании.

Процедура анализа рисков позволяет:

• произвести адекватную оценку существующих угроз информационной безопасности;

• произвести идентификацию критичных ресурсов информационной системы;

• произвести выбор адекватных требований в области обеспечения ЗИ;

• разработать перечень самых опасных уязвимых направлений и угроз.

В процессе анализа рисков информационной безопасности производят:

• классификацию информации;

• анализ уязвимостей;

• составление модели возможного злоумышленника;

• оценку рисков нарушения ИБ.

При проведении анализа рисков должны произвести в том числе и оценку степени критичности уязвимых мест, а также возможности использования этих мест возможными злоумышленниками с целью осуществления противоправных действий.

Наиболее эффективным методом оценки качества СЗИ является тест на проникновение в информационную систему. Данный метод является оптимальным способом, позволяющим оценить защищенность информационной системы в целом, обнаружить отдельные уязвимости и проверить надежность существующих механизмов защиты информационной системы от несанкционированного воздействия, используя различные модели нарушителей.

При проведении анализа информационной безопасности рекомендуется использовать два вида тестов на проникновение, что обеспечит наиболее объективную картину состояния информационной системы.

1. Тест на проникновение из сети Интернет (из внешней сети).

2. Тест на проникновение из внутренней локальной вычислительной сети (из внутренней сети).

Каждый из двух видов возможно проводить следующими методами:

• тестирование методом черного ящика — тестирование без предварительных знаний о тестируемом объекте. При выборе данного метода тестирования организация предоставляет лишь диапазон внутренних IP-адресов серверов, внутреннего сетевого оборудования, рабочих станций пользователей, сетевых принтеров или перечень конкретный внутренних сервисов. Данный подход максимально приближен к действиям злоумышленника не знакомого с целевой системой;

• тестирование методом белого ящика — более детальное исследование, основанное на дополнительной информации о тестируемом объекте. При выборе данного метода тестирования может запрашиваться дополнительная документация, файлы конфигурации, схемы структуры сети, полный доступ к тестируемому объекту. Тест моделирует ситуацию, возможную в случае утечки информации, когда атакующий находится внутри сетевой инфраструктуры организации (злоумышленник либо является сотрудником организации, либо злоумышленник знает способ проникнуть внутрь сетевой инфраструктуры извне) и в какой-то мере знает архитектуру сетевой инфраструктуры, знаком со схемами организации сети, возможно, даже имеет доступ к некоторым паролям.

4. Разработка рекомендаций по улучшению информационной безопасности.

На основе данных, полученных в результате исследования, а также результатов анализа рисков информационных активов, должны быть разработаны некоторые решения и рекомендации относительно совершенствования системы обеспечения информационной безопасности, применение которой даст возможность снизить риски информационной безопасности. По завершению анализа формируется отчет, который содержит оценку исходного уровня безопасности информационных ресурсов, данные об имеющихся проблемах, а также анализ выявленных рисков информационной безопасности, рекомендации по устранению этих рисков.

Вышеописанная методика дает возможность полностью исключить случаи нарушения информационной безопасности ИС.

2.3 Реализация защиты от угроз ИБ с помощью программно-аппаратных средств

Программно-аппаратная защита используется для защиты от несанкционированного (неавторизованного) доступа и нелегального использования. Суть функционирования: средства программно-аппаратной защиты опрашивают специальное устройство, используемое в качестве ключа, и работает только в его присутствии. Таким образом, механизм программно-аппаратной защиты содержит две составляющие [17]: аппаратное устройство (аппаратная часть) и программный модуль (программная часть).

Рассмотрим основные особенности, которые в обязательном порядке должны иметь место при организации системы защиты ИС.

Для организации защищенного порядка работы прежде всего необходимо обеспечить распознавание законного пользователя. Этот процесс часто называют авторизацией пользователя.

Авторизация пользователя включает три этапа:

1. Идентификация пользователя.

2. Аутентификация пользователя.

3. Непосредственно авторизация пользователя.

Идентификация пользователя может быть основана:

- на знании некоторой секретной информации (пароль, код);

- на владении некоторым специальным предметом или устройством (магнитная карточка, электронный ключ);

- на биометрических характеристиках (отпечатки пальцев, сетчатка глаза, спектральный состав голоса и т.п.).

Многие специалисты технологии защиты, основанные на использовании смарт-карт, считают прогрессивными, поэтому уделяют большое внимание их развитию.

Так же для обеспечения надежной информационной безопасности широкое применение нашли электронные ключи.

Электронный ключ может быть выполнен либо на основе специализированного чипа, либо на микросхемах энергонезависимой электрически перепрограммируемой памяти, либо на базе микропроцессоров.

В памяти электронного ключа хранится уникальная информация. Программная часть системы защиты определяет наличие электронного ключа при запуске программы и проверяет правильность содержащейся в ключе информации.

Итак, к основным особенностям организации защиты информации в ИС относятся: обязательное использование систем авторизации пользователей предприятия; использование программных механизмов парольной защиты; применение при работе с информационной системой предприятия электронных ключей.

2.4 Особенности организационно-правовой защиты информации

Рассмотрим обобщенную систему организационно-правовых мер обеспечения защиты ИС.

Организационные меры должны быть закреплены в нормативных и правовых документах.

С целью обеспечения информационной безопасности, в организации-носителе должны быть организованы следующие организационно-правовые меры обеспечения информационной безопасности:

- договоренность об охране помещений;

- введен пропускной режим на территорию организации;

- разработаны режим и правила противопожарной безопасности;

- организован режим видеоконтроля;

- оформлены должностные инструкции сотрудников, разграничивающие их права и обязанности;

- отработана процедура оформления дополнительных соглашений к трудовым договорам сотрудников о неразглашении ими конфиденциальной информации, которые регламентируют ответственность в области защиты информации;

- разработаны инструкция по охране периметра, а так же инструкция по эксплуатации системы охранной сигнализации и видеонаблюдения;

- разработано описание технологических процессов обработки конфиденциальной информации;

- при помощи паролей разграничен доступ к персональным компьютерам.

Правовое обеспечение системы защиты информации объединяет в себе совокупность корпоративных нормативно-организационных документов, в которую входят:

- устав;

- коллективный трудовой договор;

- трудовые договоры с сотрудниками организации;

- правила поведения сотрудников отдела в рабочее время;

- определен список лиц, допущенных к работе с документами, содержащими персональные данные клиентов и конфиденциальную информацию компании;

- функциональные обязанности руководителей и специалистов отдела.

- инструкции пользователей информационно-вычислительных сетей и ИС;

- инструкция сотрудников, которые ответственны за защиту информации;

- памятки сотрудникам о сохранении служебной тайны;

- договорные обязательства.

Если не углубляться в тему содержания перечисленных документов, то можно сказать, что все из них содержат указания, требования или правила необходимые для обеспечения высокого уровня информационной защищенности ИС.

Отмечу, что наличие правового обеспечения регулирует многие спорные вопросы, которые очень часто возникают в ходе обмена информацией на различных уровнях. Стороны, которые не будут выполнять эти условия, должны нести ответственность в пределах, предусмотренных соответствующими пунктами документов и российским законодательством.

ЗАКЛЮЧЕНИЕ

Один из наиболее актуальных на сегодня вопросов, который касается защиты информации в Российской федерации, это вопрос организации защиты данных в рамках действующего российского законодательства, а так же актуальными угрозами безопасности информационных систем. Особо острым является вопрос обеспечения безопасности информации в масштабных распределенных информационных системах.

Информационная безопасность - направление, развивающаяся чрезвычайно быстрыми темпами. Этому способствуют общий прогресс информационных

технологий и постоянное противоборство нападающих и защищающихся.

К сожалению, подобная динамичность объективно затрудняет обеспечение надежной защиты. Это есть конкретные причины:

• повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы (перебором вариантов) эффективнее преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;

• усовершенствование сетей, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют число потенциальных злоумышленников, которые имеют техническую возможность осуществить нападение;

• конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки системы, а это в свою очередь ведет к снижению качества тестирования и выпуску продуктов с дефектами защиты;

• навязываемая потребителям парадигма постоянного наращивания аппаратного и программного обеспечения вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Стремясь к нейтрализации и снижению вероятности проявления каких-либо угроз безопасности информации в процессе функционирования информационной системы, необходимо применение комплекса мер защиты, а именно: организационно-технических, инженерных и программно-аппаратных.

В процессе выполнения курсовой работы проведено исследование нормативно-правовой базы систем обеспечения информационной безопасности в Российской Федерации, угроз и нарушителей безопасности ИС, приведена общесистемная классификация методов обеспечения информационной безопасности ИС, проанализированы современные угрозы ИБ и способы борьба с ними.

Кроме этого произведен анализ стратегий обеспечения информационной безопасности и даны обоснованные рекомендации по выбору конкретной стратегии.

Так же приведены особенности программно-аппаратной и организационно-правовой защиты информации в ИС.

По завершению работы, считаю, что все поставленные цели были достигнуты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Архитектура ЭВМ и вычислительных систем: Учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015 - 512 с.: ил.; 60x90 1/16. - (Профессиональное образование). (п) ISBN 978-5-91134-742-0, 500 экз. Режим доступа: http://znanium.com/catalog.php?bookinfo=492687.
2. Базовые и прикладные информационные технологии: Учебник / Гвоздева В. А. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 384 с.: 60x90 1/16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-8199-0572-2. Режим доступа: http://znanium.com/catalog.php?bookinfo=504788.
3. Информационные технологии в профессиональной деятельности: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0349-0, 300 экз. Режим доступа: http://znanium.com/catalog.php?bookinfo=484751.
4. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с.: 60x88 1/16 + (Доп. мат. znanium.com). - (Высшее образование: Бакалавр.). (о) ISBN 978-5-369-01379-3, 200 экз. Режим доступа: http://znanium.com/catalog.php?bookinfo=476047.
5. Основные положения информационной безопасности: Учебное пособие / В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: 60x90 1/16. - (Профессиональное образование) (Обложка. КБС) ISBN 978-5-00091-079-5, 300 экз. Режим доступа: http://znanium.com/catalog.php?bookinfo=508381.
6. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-004-7, 500 экз. Режим доступа: http://znanium.com/catalog.php?bookinfo=489084.
7. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/catalog.php?bookinfo=503511.
8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ред. от 21.12.2013).

9. Федеральный закон Российской Федерации от 26 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 28.12.2013).
10. Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное приказом ФСТЭК России от 05 февраля 2010 года № 58 (зарегистрировано Минюстом России 19 февраля 2010 года № 16456).
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (от 16 ноября 2009 г).
12. Приказа ФСТЭК России №21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
13. Постановление Правительства РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012г. №1119.

ПРИЛОЖЕНИЕ 1 - Классификация типов нарушителей ИБ