Содержание:

Введение

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик ИС. Существует довольно обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль (например, банковские информационные системы).

Под безопасностью ИС понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на ИС.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

егодня можно утверждать, что рождается новая современная технология — технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

Таким образом, обеспечение информационной безопасности является комплексной задачей. Это обусловлено тем, что информационная среда является сложным многоплановым механизмом, в котором действуют такие компоненты, как электронное оборудование, программное обеспечение, персонал.

Цель исследования – описание видов и состав угроз информационной безопасности.

Для достижения данной цели необходимо решение следующих **задач:**

- Привести основные термины и их определение;
- Описать основные принципы информационной безопасности;
- Выявить источники угроз информационной безопасности;
- Описать источники угроз информационной безопасности Российской Федерации;
- Описать основные виды угроз информационной безопасности;
- Описать классы угроз информационной безопасности в международных стандартах.

Объектом исследования является виды и состав угроз информационной безопасности. **Предметом** исследования являются информационная безопасность.

Работа состоит из введения, трех глав, заключения и списка использованной литературы.

Глава 1. Основные понятия и определения

1.1. Основные термины и их определение

При смене способа хранения информации с бумажного вида на цифровой, появился главный вопрос - как эту информацию защитить, ведь очень большое количество факторов влияет на сохранность конфиденциальных данных.

Безопасность информационных систем является частью более широкой проблемы: безопасность компьютерных систем или еще более общей проблемы - информационной безопасности.

Важнейшей стороной обеспечения информационной безопасности является определение и классификация угроз. Угрозы безопасности информации — это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации.

В разных источниках понятия «угроза информационной безопасности» раскрывается по разному.

В интернете предложено следующее определения понятия угроза информационной безопасности – это совокупность условий и факторов, создающих опасность нарушения информационной безопасности[1].

Аналогичное определение термина угроза безопасности информации представлено в «Доктрине информационной безопасности Российской Федерации» – «совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации»[2]. В доктрине представлено широкое определение данного понятия.

Угрозы информационной безопасности — это различные обстоятельства (условия, факторы состояния), т.е. опасные воздействия на информацию, информационную инфраструктуру, реализацию правового статуса человека и гражданина в области информационной деятельности, а также опасные действия, связанные с причинением вреда реализации национальных интересов, связанных с этими объектами. Названные воздействия (условия и факторы) способны нарушить нормальное функционирование таких объектов (или их динамичное равновесие)[3].

Угрозу отождествляют обычно либо с характером (видом, способом) дестабилизирующего воздействия на информацию, либо с последствиями (результатами) такого воздействия. Однако такого рода термины могут иметь много трактовок. Возможен и иной подход к определению угрозы безопасности информации, базирующийся на понятии «угроза». Угроза - это намерение нанести физический, материальный или иной вред общественным или личным интересам, возможная опасность[4].

Для того чтобы определить угрозы, от которых необходимо обезопасить информацию, нужно определить объекты защиты. Ведь информация — это некоторые данные, носителями которых могут быть как материальные, так и нематериальные объекты. К примеру, носителями конфиденциальной информации могут быть документы, технические средства обработки и хранения информации и даже люди.

Носители конфиденциальной информации

Документационными носителями информации могут быть проекты, бизнес-планы, техническая документация, контракты и договора, а также картотеки отдела кадров (персональные данные) и отдела по работе с клиентами. Отличительной их особенностью является зафиксированность данных на материальном объекте — бумаге.

Техническими средствами обработки и хранения информации являются персональные компьютеры, ноутбуки, серверы, сканеры, принтеры, а также съемные носители (переносные жесткие диски, флеш-карты, CD-диски, дискеты) и т.п. Информация в технических средствах хранится и обрабатывается в цифровом виде. Зачастую конфиденциальные данные отправляются через Интернет, например, по электронной почте. В сети они могут быть перехвачены злоумышленниками. Кроме того при работе компьютеров из-за их технических особенностей обрабатываемые данные преобразуются в электромагнитные излучения, распространяющиеся далеко за пределы помещения, которые также могут быть перехвачены и использованы в недобросовестных целях.

Многие ошибочно относят документы и технические носители к одной категории источников конфиденциальной информации, но это не так: документ как источник ведь может быть представлен и на бумажном, и на электронном носителе, а вот далеко не всякий технический носитель может быть признан документом[5].

Опасность технических носителей определяется высоким темпом роста парка технических средств, компьютерных сетей и ПЭВМ, находящихся в эксплуатации, их широким применением в самых различных сферах человеческой деятельности, высокой степенью концентрации информации на технических носителях и масштабностью участия людей в использовании этих носителей в практической деятельности[6].

Люди также могут быть «носителями» информации. Например, сотрудники компании, которые имеют или могут иметь доступ к конфиденциальной информации. Таких людей называют инсайдерами. Инсайдер необязательно является злоумышленником, но в любой момент может им стать. Кроме того несанкционированный доступ к конфиденциальной информации могут получить посетители, клиенты или партнеры, а также обслуживающий персонал.

Подытожим, все выше изложенное: угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

Если говорить об угрозах информационно-технического характера, можно выделить такие элементы как кража информации, вредоносное ПО, хакерские атаки, СПАМ, халатность сотрудников, аппаратные и программные сбои, финансовое мошенничество, кража оборудования.

Согласно статистике применительно к этим угрозам, можно привести следующие данные (по результатам исследований, проведённых в России компанией InfoWath):

- Кража информации – 64%
- Вредоносное ПО – 60%
- Хакерские атаки – 48%
- Спам – 45%
- Халатность сотрудников – 43%
- Аппаратные и программные сбои – 21%
- Кража оборудования – 6%
- Финансовое мошенничество – 5%

1.2. Основные принципы информационной безопасности

Информационная безопасность базируется на соблюдении следующих принципов:

1. Целостность данных - такое свойство, в соответствии с которым информация сохраняет свое содержание и структуру в процессе ее передачи и хранения. Создавать, уничтожать или изменять данные может только пользователь, имеющий право доступа.

2. Конфиденциальность — свойство, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц. Таким образом, конфиденциальность дает гарантию того, что в процессе передачи данных, они могут быть известны только авторизованным пользователям

3. Доступность информации - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации.

4. Достоверность – данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Задача обеспечения информационной безопасности подразумевает реализацию многоплановых и комплексных мер по предотвращению и отслеживанию несанкционированного доступа неавторизованных лиц, а также действий,

предупреждающих неправомерное использование, повреждение, искажение, копирование, блокирование информации.

Вопросы информационной безопасности становятся первоочередными в тех случаях, когда выход из строя или возникновение ошибки в конкретной компьютерной системе могут привести к тяжелым последствиям[7].

Глава 2. Источники угроз информационной безопасности

2.1 Источники угроз информационной безопасности

По состоянию источника угроз информационная безопасность делится на:

непосредственно в АС, к примеру неточная реализация ресурсов АС;

в пределах зоны АС, к примеру, применение подслушивающих приборов, записей, хищение распечаток, носителей данных и т.п.;

вне зоны АС, например захват информации, которая передается по путям связи, захват побочных акустических, электромагнитных и других излучений устройств.

По степени воздействия на АС делится на:

активные угрозы, которые при реакции вносят сдвиг в структуру и сущность АС, к примеру ввод вирусов и троянских коней;

пассивные угрозы, которые при исполнении ничего не изменяют в типе и сущности АС, к примеру угроза копирования секретной информации.

По способу пути к ресурсам АС:

угрозы, выполняемые с применением маскированного нестандартного каналу пути к ресурсам АС, на пример несанкционированный путь к ресурсам АС путем применения каких либо возможностей ОС;

угрозы, выполняемые с применением стандартного каналу доступа к ресурсам АС, к примеру незаконное получение паролей и других параметров разграничения доступа с последующей маскировкой под зарегистрированного работника фирмы.

По шагам доступа работников или программ к ресурсам:

угрозы, которые реализуются после согласия доступа к ресурсам АС, к примеру угрозы некорректного или несанкционированного применение ресурсов АС;

угрозы, которые реализуются на шаге доступа к ресурсам АС, к примеру угрозы несанкционированного доступа в АС.

По нынешнему месту размещению информации, хранимой и обрабатываемой в АС:

угрозы проходу к информации, которая находится в ОЗУ;

угрозы проходу к информации, которая находится на внешних запоминающих носителях, например несанкционированное копирование конфиденциальной информации с жесткого носителя;

угрозы проходу к информации, видимой на терминале, например запись отображаемых данных на видеокамеру;

угрозы проходу к информации, которая проходит в каналах связи, например незаконное подсоединение к каналам связи с задачей прямой подмены законного работника со следующим вводом дезинформации и навязыванием ложных данных, незаконное подсоединение к каналам связи с следующим вводом ложных данных или изменением транслируемой информации.

Как описано выше, опасные влияния на АС классифицируются на случайные и преднамеренные. Изучение опыта проектирования, производство и эксплуатации АС доказывает, что данные подвергается разным случайным реакциям на всех ступенях цикла и функционирования АС.

Источником случайных реакций в процессе выполнения АС могут быть:

сбои аппаратурных устройств;

ошибки в работе обслуживающих работников и других сотрудников;

критичные ситуации, в результате стихийных бедствий и отключений электричества;

шумы и фон в каналах связи из-за влияния внешних факторов канала;

огрехи в программном обеспечении.

спецификация физической среды.

Погрешности в ПО это один из видом компьютерных повреждений. ПО рабочих станций, серверов, маршрутизаторов и т д. создано людьми, поэтому оно может содержать ошибки. Если сложность подобного ПО выше, то и больше риск раскрытие в нем ошибок и уязвимых узлов. Некоторые из них могут не представляют никакой угрозы, а некоторые же могут привести к вещественным результатам, таким как неработоспособность серверной платформы, получение похитителем контроля над серверной платформой, несанкционированное эксплуатация ресурсов. Как правило, аналогичные погрешности ликвидируются с помощью паков обновлений, которые регулярно выпускают создатели ПО. Поэтому, для устранения таких ошибок необходимо во время обновлять ПО. Кроме того, ошибки в работе могут возникнуть из-за проблем защиты информации в сети.

Преднамеренные угрозы сплоченны с целенаправленными методами преступника. Преступником может быть сотрудник, обычный посетитель, наемники, конкурентные особи и т.д. Методы преступника могут быть объяснены следующими факторами: конкурентной борьбой, любопытством, недовольством сотрудника своей карьерой, материальным интересом (взятка), стремлением самоутвердиться любыми методами и т.п.

Рассмотрим на примере банковской АС намеренные угрозы:

ознакомление банковских работников с информацией, к которой у них нету доступа;

НСД личностей, которые не относятся к ряду банковских работников;

программные закладки;

несанкционированное создание резервных копий программ и данных;

хищение распечатанных банковских файлов;

хищение цифровых носителей, которые содержат конфиденциальные данные;

умышленное устранение информации;

локальные атаки;

измена сообщений, которые транслируются по каналам связи;

несанкционированное модификация банковскими работниками финансовых отчетов;

отказ от авторства сообщения, которое отправлено по канал связи;

уничтожение архивной банковских данных, которые были ранее сохранены на внешних носителях;

уничтожение данных, вызванное вирусной реакцией;

отказ от факта получение данных;

отказ при контроле удаленного доступа.

Можно заключить, что несанкционированный доступ является самым распространенным и многовариативным вид компьютерных правопреступлений.

Рассмотрим основные приемы и способы НСД:

незаконное применение привилегий;

«маскарад»;

перехват паролей.

Перехват паролей можно сделать в результате применения специально разработанных приложений. При заходе законного работника в систему организации, программа-перехватчик имитирует на экране работника ввод имени и пароля этого работника, которые после ввода отправляются владельцу приложения-перехватчика, затем сотруднику на экран выводится сообщение об ошибке системы и управление возвращается ОС.

Как правило, работник, полагает, что ввел неправильный пароль. И при повторном вводе работник вводит в систему организации. А перехватчик имеет логин и пароль этого работника, и затем использует в собственных целях. На данный момент применяются и другие методы захвата вводных данных работников системы. Для шифрование паролей при передачи, рекомендуется употреблять RSA.

«Маскарад» — это исполнение любых действий одним работником от имени другого работника, который имеет соответствующими правами доступа. Основная задача «маскарада» это пользование чужими данными, для получения конфиденциальной информации в личных целях. Распространены следующие методы выполнения «маскарада»:

передача данных в сеть от имени другого работника.

вход в систему под вводными данными в систему другого работника (этому «маскараду» способствует перехват пароля).

В банковских системах «Маскарад» очень опасен, особенно в электронных платежах, где неправильная идентификация клиента из-за «маскарада» вора может привести к убыткам законного клиента банка[8].

Незаконная эксплуатация привилегий. Множество систем защиты создают определенные списки привилегий для совершение заданных целей. Каждый сотрудник получает свой список привилегий: администраторы — максимальный список действий, обычные пользователи — минимальный список действий. Несанкционированный перехват привилегий, например с помощью «маскарада», приводит к вероятному совершении правонарушителем определенных действий в обход системы защиты. Нужно отметить, что незаконный перехват списка привилегий вероятен либо при наличии погрешностей в системе защиты, либо из-за недочета администратора при регулированием системой и назначении списка привилегий.

Угрозы которые нарушают целостность информации, сохраненной в информационной системе или передаваемой по линиям связи, которые созданы на ее модификацию или искажение, в итоге приводят к разрыву ее качества или полному удалению. Целостность данных может быть нарушена умышленно, в результате объективных воздействий со стороны окружающих факторов. Эта угроза частично актуальна для систем транспортировки данных — систем телекоммуникаций и информационные сети. Умышленные действия которые нарушают целостность данных не надо путать с ее санкционированными модификациями, которые выполняется полномочными личностями с обоснованной задачей.

Угрозы которые нарушают конфиденциальность, созданы на разглашение конфиденциальной или секретной информации. При действии этих угроз данных становится известной личностям, которые не должны иметь к ней доступ. В

источниках информационной безопасности угроза преступления конфиденциальности имеет каждый раз, когда получен НСД к закрытой информации, сохраняющейся в информационной системе или передаваемой от между системами.

Угрозы которые нарушают работоспособность сотрудников или системы в целом. Они направлены на создание таких вариантов ситуаций, когда определенные действия либо понижают работоспособность АС, либо блокируют доступ к ресурсным фондам. К примеру, если один сотрудник системы хочет получить доступ к определенной службе, а другой создает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть временным или постоянным. Примером может быть сбой при коммутации каналов и пакетов. А также угрозы на средства передачи информации, к примеру спутниковые системы.

Эти угрозы можно числить непосредственными или первичными, тогда как создание этих угроз ведет к прямому воздействию на защищаемую информацию.

Сегодня для современных ИТ систем, защита является необходимым компонентом АС обработки информации. Атакующая сторона сначала должна преодолеть подсистему защиты, и только потом нарушать допустим целостность АС. Но нужно понимать, что практически не существует абсолютной системы защиты, вопрос стоит лишь во средствах и времени, требующихся на ее обход.

Защитная система также представляет угрозу, поэтому для нормальных защищенных информационных систем нужно учитывать четвертый вид угроз — угроза осмотра параметров системы под защиты. На практике мероприятие проверяется шагом разведки, в ходе которого узнаются основные параметры системы защиты, ее характеристики и т. п. В результате этого шага является корректировка поставленной задачи, а также выбор самого оптимального технических методов обхода системы защиты. Даже сетевые адаптеры представляют угрозу.

Угрозу раскрытия параметров системы защиты можно называть непрямой угрозой. реализация угрозы не даст какой-либо ущерб обрабатываемой информации в информационной системе, но даст возможность реализовать прямые или первичные угрозы, описаны выше.

Трудно предсказуемыми источниками угроз информации являются стихийные бедствия и аварии, которые могут возникнуть на объекте размещения

компьютерной системы. Пожар, наводнение, землетрясение, удар молнии, выход из строя электропитания и т.д. чреваты для компьютерной системы наиболее разрушительными последствиями[9].

2.2 Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

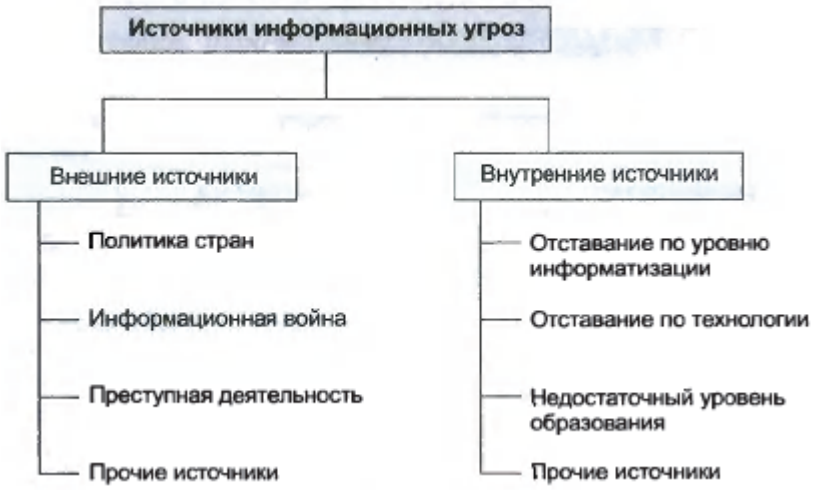

Рисунок 1 - Источники основных информационных угроз для России

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним[10].

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

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

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

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

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

недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

недостаточная экономическая мощь государства;

снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

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

отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан[11].

Глава 3. Виды угроз информационной безопасности

3.1 Виды угроз информационной безопасности

Угрозы информационной безопасности – это возможные действия или события, которые могут вести к нарушениям ИБ. Виды угроз информационной безопасности очень разнообразны и имеют множество классификаций, которые представлена на рисунке 1 (См. Приложение 1).

Угрозы ИБ являются целями/конечными результатами деятельности нарушителей информационной безопасности.

Рисунок 1 - Шесть основных видов угроз информационной безопасности (классифицированных по характеру нарушения)

Анализ актуальных угроз конфиденциальной информации, на основе которого строится система информационной безопасности предприятия и осуществляется организация защиты информации, начинается с понимания и классификации этих угроз. В настоящий момент теория информационной безопасности рассматривает несколько классификаций информационных рисков и угроз защиты информации. Мы остановимся на генерализированном разделении угроз информационной безопасности интеллектуальной собственности организации на две категории –внешние и внутренние угрозы. Данная

классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать как удалённо, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, либо же действовать посредством доступа к внутренним ресурсам IT-инфраструктуры объекта.

В случае внешних атак, преступник ищет уязвимости в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д. Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации. Рассмотрим эти категории рисков информационной безопасности подробнее.

Внешние угрозы информационной безопасности

Доклад Всемирного экономического форума «Глобальные риски 2012» (“GlobalRisks 2012”) рассматривает кибератаки как одну из основных угроз мировой экономике. По вероятности наступления, кибератаки входят в пятёрку наиболее вероятных глобальных угроз на 2012 год. Такое заключение Всемирного экономического форума свидетельствует о высокой актуальности и значительной опасности электронной преступности. В документе приводится также график роста официально признанных инцидентов киберпреступности с указанием значительного увеличения потерь от таких преступлений на примере США (См. Рисунок 2):

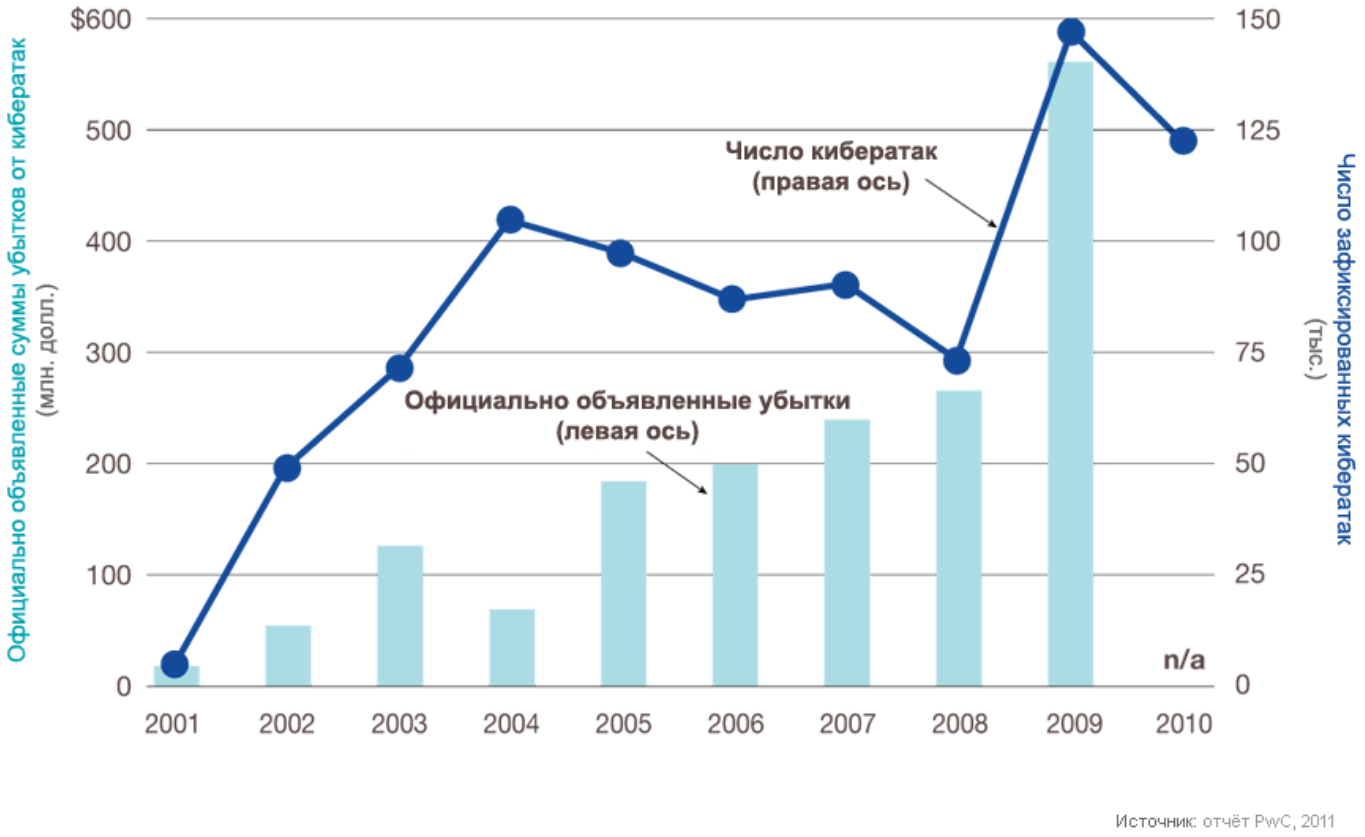

Рисунок 2 - График роста официально признанных инцидентов киберпреступности

Следует отметить, что доклад PricewaterhouseCoopers за 2011 год, в соответствии с данными которого был построен этот график, оперирует только официально признанными фактами электронных преступлений, равно как и официально объявленными цифрами убытков – реальная картина выглядит ещё более удручающей. Причём не только в США, эта тенденция является общемировой.

Итак, кибератаки сегодня – давно не голливудский миф, это реальная и серьёзная опасность информационной инфраструктуре, интеллектуальной и физической собственности государственных и коммерческих объектов. Наиболее распространённой и разнообразной по методам исполнения формой киберпреступности является использование вредоносного ПО. Такие угрозы представляют прямую опасность конфиденциальности и целостности информационных ресурсов организации. В атаках с использованием вредоносных кодов и приложений используются уязвимости информационных систем для осуществления несанкционированного доступа к базам данных, файловой системе локальной корпоративной сети, информации на рабочих компьютерах сотрудников. Спектр угроз информационной безопасности, вызванных использованием

вредоносного программного обеспечения чрезвычайно широк. Вот некоторые примеры таких *угроз защиты информации*:

- Внедрение вирусов и других разрушающих программных воздействий;
- Анализ и модификация/уничтожение установленного программного обеспечения;
- Внедрение программ-шпионов для анализа сетевого трафика и получения данных о системе и состоянии сетевых соединений;
- Использование уязвимостей ПОдля взлома программной защиты с целью получения несанкционированных прав чтения, копирования, модификации или уничтожения информационных ресурсов, а также нарушения их доступности;
- Раскрытие, перехват и хищение секретных кодов и паролей;
- Чтение остаточной информации в памяти компьютеров и на внешних носителях;
- Блокирование работы пользователей системы программными средствами и т.д.

Внутренние угрозы информационной безопасности

Большинство инцидентов информационной безопасности связано с воздействием внутренних угроз – утечки и кражи информации, утечки коммерческой тайны и персональных данных клиентов организации, ущерб информационной системе связаны, как правило, с действиями сотрудников этой организации. В классификации внутренних угроз в первую очередь можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений, и совершаемые без злого умысла, по неосторожности или технической некомпетентности.

Итак, преступления сотрудников, способных причинить вред сохранности интеллектуальной и коммерческой собственности организации (их принято называть «инсайдерами») можно разделить на категории злонамеренного инсайда и непредумышленного инсайда. Злоумышленным инсайдером могут стать:

- Сотрудники, затаившие злобу на компанию-работодателя («обиженные»). Такие инсайдеры действуют исходя из мотивов личной мести, причин для которой может быть масса – от увольнения/понижения в должности до отказа компании предоставить статусные атрибуты, например, ноутбук или расширенный соцпакет.

- Нечистые на руку сотрудники, стремящиеся подзаработать за счёт компании-работодателя. Такими инсайдерами становятся сотрудники, использующие секретные информационные ресурсы компании для собственной выгоды. Базы данных клиентов, интеллектуальная собственность компании, состав коммерческой тайны – такая информация может использоваться инсайдером в личных интересах, либо продаваться конкурентам.
- Внедрённые и завербованные инсайдеры. Самый опасный и самый трудно-идентифицируемый тип внутренних злоумышленников. Как правило, являются звеном преступной цепочки или членом организованной преступной группы. Такие сотрудники имеют достаточно высокий уровень доступа к конфиденциальной информации, ущерб от их действий может стать фатальным для компании.

Злонамеренные инсайдеры представляют определённую опасность для информационной системы и конфиденциальных данных, однако вероятность злоумышленных инцидентов ничтожно мала по сравнению с утечками информации, совершаемыми по неосторожности или вследствие технической безграмотности сотрудников. Да, увы, это так – львиная доля всех инцидентов информационной безопасности на объекте любой сложности является следствием непредумышленных действий сотрудников. Возможностей для таких утечек информации множество: от ошибок ввода данных при работе с локальными сетями или интернетом до утери носителя информации (ноутбук, USB-накопитель, оптический диск); от пересылки данных по незащищённым каналам связи до непредумышленной загрузки вирусов с развлекательных веб-сайтов.

Информационная безопасность и защита информации на предприятии: комплексный подход

Традиционные средства защиты (антивирусы, фаерволы и т.д.) на сегодняшний день не способны эффективно противостоять современным киберпреступникам. Для защиты информационной системы организации требуется комплексный подход, сочетающий несколько рубежей защиты с применением разных технологий безопасности.

Для *защиты от внешних интернет угроз* информационной безопасности отлично зарекомендовали себя системы предотвращения вторжений на уровне хоста (HIPS). Правильно настроенная система даёт беспрецедентный уровень защищённости, близкий к 100%. Грамотно выработанная политика безопасности, применение совместно с HIPS других программных средств защиты информации (например,

антивирусного пакета) предоставляют очень высокий уровень безопасности. Организация получает защиту практически от всех типов вредоносного ПО, значительно затрудняет работу хакера, решившего попробовать пробить информационную защиту предприятия, сохраняет интеллектуальную собственность и важные данные организации.

Защита от внутренних угроз также требует комплексного подхода. Он выражается в выработке должных политик информационной безопасности, введением чёткой организационной структуры ответственных за информационную безопасность сотрудников, контроле документооборота, контроле и мониторинге пользователей, введении продвинутых механизмов аутентификации для доступа к информации разной степени важности. Степень такой защиты зависит от объективных потребностей организации в защите информации. Далеко не всем объектам требуется дорогостоящая DLP-система, дающая неплохие результаты по защите данных предприятия от утечек, но требующая сложнейшей процедуры внедрения и пересмотра текущих механизмов документооборота. Оптимальным выбором для большинства компаний станет введение функционала защиты от утечек данных, контроле документооборота и мониторинг действий пользователей локальной сети организации. Такое решение является недорогим, простым в развёртывании и эксплуатации, но весьма эффективным инструментом информационной безопасности.

3.2 Классы угроз информационной безопасности в международных стандартах

Разграничение классов информационной безопасности позволяет отличать друг от друга системы, обеспечивающие разную степень защищенности информации и информационной инфраструктуры, лучше знать возможности классифицируемых систем и выполняемые ими требования. Это гарантирует более обоснованный выбор и более качественное управление системой информационной безопасности.

Классы информационной безопасности определены в нескольких общеизвестных стандартах. Наиболее известна классификация, данная в стандарте министерства обороны США «Критерии оценки доверенных компьютерных систем» (TrustedComputerSystemEvaluationCriteria, TCSEC). Стандарт TCSEC также именуется «Оранжевой книгой». В «Оранжевой книге» определены четыре уровня безопасности – D, C, B и A. Уровень D признан неудовлетворительным. Уровни C и B

подразделяются на классы (C1, C2, B1, B2 и B3). Таким образом, всего в стандарте определено шесть классов информационной безопасности – C1, C2, B1, B2, B3 и A1.

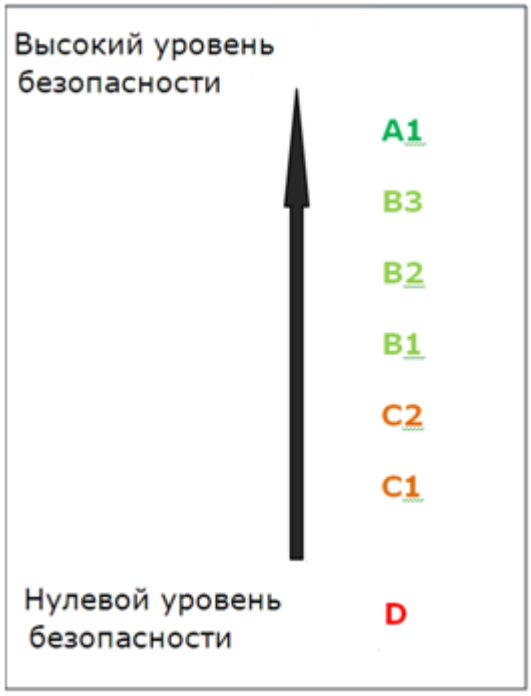

Рисунок 4 – Требования «Оранжевой книги»

По мере перехода от D к A растет уровень информационной безопасности, а к информационной системе предъявляются все более жесткие требования.

В таблице Б.1, приведенной ниже, отражены основные требования «Оранжевой книги», предъявляемые к уровням и классам информационной безопасности.

Еще один стандарт, описывающий классы информационной безопасности, – «Европейские критерии» (InformationTechnologySecurityEvaluationCriteria, ITSEC), выдвинутые рядом западноевропейских государств. Данный стандарт, вышедший в 1991 году, содержит согласованные критерии оценки безопасности информационных технологий, выработанные в ходе общеевропейской интеграции. «Европейские критерии» описывают классы функциональности систем информационной безопасности, характерных для правительственных и коммерческих структур. Некоторые из этих классов соответствуют классам информационной безопасности «Оранжевой книги».

По аналогии с «Оранжевой книгой» были построены вышедшие чуть позже «Руководящие документы» Гостехкомиссии при президенте России. «Документы» устанавливают семь классов защищенности средств вычислительной техники от

несанкционированного доступа к информации. В некоторых вопросах «Руководящие документы» отклоняются от американского стандарта – например, они отдельно определяют классы межсетевых экранов.

Заключение

Конфиденциальная информация представляет огромный интерес для конкурирующих фирм. Именно она становится причиной посягательств со стороны злоумышленников.

Многие проблемы связаны с недооценкой важности угрозы, в результате чего для предприятия это может обернуться крахом и банкротством. Даже единичный случай халатности рабочего персонала может принести компании многомиллионные убытки и потерю доверия клиентов.

Угрозам подвергаются данные о составе, статусе и деятельности компании. Источниками таких угроз являются её конкуренты, коррупционеры и преступники. Особую ценность для них представляет ознакомление с охраняемой информацией, а также ее модификация в целях причинения финансового ущерба.

К такому исходу может привести утечка информации даже на 20%. Иногда потеря секретов компании может произойти случайно, по неопытности персонала или из-за отсутствия систем защиты.

Для информации, являющейся собственностью предприятия, могут существовать угрозы следующих видов.

Угрозы конфиденциальности информации и программ. Могут иметь место после нелегального доступа к данным, каналам связи или программам. Содержащие или отправленные данные с компьютера могут быть перехвачены по каналам утечки.

Для этого используется специальное оборудование, производящее анализ электромагнитных излучений, получаемых во время работы на компьютере.

Опасность повреждения. Незаконные действия хакеров могут повлечь за собой искажение маршрутизации или потерю передаваемой информации.

Угроза доступности. Такие ситуации не позволяют законному пользователю использовать службы и ресурсы. Это происходит после их захвата, получения по

ним данных или блокировки линий злоумышленниками. Подобный инцидент может искажать достоверность и своевременность передаваемой информации.

Риск отказа от исполнения транзакций. Отказ пользователя от передаваемой им же информации с тем, чтобы избежать ответственности.

Внутренние угрозы. Такие угрозы несут для предприятия большую опасность. Они исходят от неопытных руководителей, некомпетентного или неквалифицированного персонала.

Иногда сотрудники предприятия могут провоцировать специально внутреннюю утечку информации, показывая этим своё недовольство зарплатой, работой или коллегами. Они запросто могут преподнести всю ценную информацию предприятия его конкурентам, попытаться уничтожить её, или умышленно внести в компьютеры вирус.

Библиография

Угрозы информационной безопасности [электронный ресурс] – URL: https://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D1%80%D0%BE%D0%B7%D1%8B_%D0%B8% (дата обращения 05.03.2016)

Доктрина информационной безопасности Российской Федерации от 09.09.2000

Геращенко, М. М.Информационные технологии в юридической деятельности : учеб.пособ

Батаршина Р.Р., Дьяченко В.А., Кодолова И.А., Степанова Ю.В., Тартаковская Н.З., Фатых

Гладкий, А.А. Обман, подставы и провокации в малом и среднем бизнесе: руководство. -

Макаров В.Е. Социальные основы информационной безопасности деловой организации. М

Научное и прикладное использование современных информационных систем и технологи

Лямин Л.В. Применение технологий электронного банкинга: риск-ориентированный подх

Семененко В.Л. Информационная безопасность: Учебное пособие. 4-е изд.. стереотип. -М

Понятие национальной безопасности [электронный ресурс] - URL: php?dn=html&way=bW

Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учебное п

Приложение 1

По характеру нарушения	• нарушение конфиденциальности данных • нарушение работоспособности ЭВМ • незаконное вмешательство в функционирование ЭВМ и т.д.
По тяжести нарушения	• незначительные ошибки • мелкое хулиганство • серьезные преступления/природные и техногенные катастрофы
По предвидению последствий нарушителем	• намеренные нарушения • ненамеренные нарушения
По мотивации	• злонамеренные нарушения • незлонамеренные нарушения
По месту возникновения	• внешние угрозы • внутренние угрозы (угрозы со стороны инсайдеров)
По законченности	• реализованные • нереализованные
По объекту воздействия	• угрозы, нацеленные на всю информационную систему • угрозы, нацеленные на отдельные компоненты ИС
По причине возникновения	• угрозы, возникшие из-за недостаточности средств технической защиты • угрозы, возникшие из-за недостаточности организационных мер
По каналу проникновения	• угрозы, проникающие через уязвимости ПО, бесконтрольные съёмные носители • угрозы, проникающие через бреши в системах авторизации, недостатки систем хранения документов и т.д.
По виду реализации угрозы	• вредоносные программы, спам-письма, программные закладки, хакерские атаки • уязвимые процедуры авторизации и другие регламенты ИБ • стихийные бедствия
По происхождению	• антропогенные • техногенные • природные
По размеру ущерба	• незначительные • значительные • критичные

Рисунок 1 - Различные виды угроз информационной безопасности

Приложение 2

Таблица 1- Классы информационной безопасности, определённые в «Оранжевой книге»

Уровень C - Произвольное управление доступом

Класс C1 обеспечивает базовый уровень безопасности, разделяя пользователей и данные. Информационные системы, принадлежащие к данному классу, должны отвечать следующим основным требованиям:

доверенная база управляет доступом именованных пользователей к именованным объектам;

пользователи четко идентифицируют себя;

аутентификационная информация пользователей защищена от несанкционированного доступа;

доверенная вычислительная база имеет изолированную область для собственного выполнения, защищенную от внешних воздействий;

есть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;

защитные механизмы протестированы на отсутствие способов обхода или разрушения средств защиты доверенной вычислительной базы;

описаны подход к безопасности и его применение при реализации доверенной вычислительной базы.

Класс C2 (в дополнение к требованиям к C1) гарантирует ответственность пользователей за свои действия:

права доступа гранулируются с точностью до пользователя, а доступ к любому объекту контролируется;

при выделении объекта из пула ресурсов доверенной вычислительной базы, устраняются следы его использования;

каждый пользователь системы уникальным образом идентифицируется, а каждое регистрируемое действие ассоциируется с конкретным пользователем;

доверенная вычислительная база позволяет создавать, поддерживать и защищать журнал регистрационной информации, касающейся доступа к объектам, которые контролируются базой;

тестирование подтверждает отсутствие видимых недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Уровень B - Принудительное управление доступом

Класс B1 (в дополнение к требованиям к C2):

доверенная вычислительная база управляет метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;

доверенная вычислительная база обеспечивает реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;

доверенная вычислительная база обеспечивает взаимную изоляцию процессов путем разделения их адресных пространств;

специалисты тщательно анализируют и тестируют архитектуру и исходный код системы;

существует неформальная или формальная модель политики безопасности, поддерживаемая доверенной вычислительной базой.

Класс B2 (в дополнение к требованиям к B1):

все ресурсы системы, прямо или косвенно доступные субъектам, снабжаются метками секретности;

в доверенной вычислительной базе поддерживается доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации;

предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;

доверенная вычислительная база внутренне структурирована на хорошо определенные, относительно независимые модули;

системный архитектор тщательно анализирует возможность организации тайных каналов обмена с памятью и оценивает максимальную пропускную способность каждого выявленного канала;

продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;

модель политики безопасности является формальной; для доверенной вычислительной базы существуют описательные спецификации верхнего уровня, точно и полно определяющие её интерфейс;

в процессе разработки и сопровождения доверенной вычислительной базы

Уровень А - Верифицируемая безопасность

Класс А1 (в дополнение к требованиям к В3):

тестирование продемонстрировало то, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;

представлены формальные спецификации верхнего уровня; используются современные методы формальной спецификации и верификации систем;

механизм управления конфигурациями распространяется на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;

описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

1. Угрозы информационной безопасности [электронный ресурс] – URL: https://ru.wikipedia.org/wiki/%D0%A3%D0%B3%D1%80%D0%BE%D0%B7%D1%8B_%D0% (дата обращения 05.03.2016) ↑

2. Доктрина информационной безопасности Российской Федерации от 09.09.2000 ↑

3. Геращенко, М. М.Информационные технологии в юридической деятельности : учеб.пособие : в 2 ч. / М. М. Геращенко, Е. А. Печенкина, В. Н. Храпов ; СибАГС. —Новосибирск : Изд-во СибАГС, 2012. —Ч. 2.— 191с. ↑

4. Батаршина Р.Р., Дьяченко В.А., Кодолова И.А., Степанова Ю.В., Тартаковская Н.З., Фатыхова Л.Г. Теоретические разделы курса “Инфоматика” / Под ред. И.А. Кодоловой: Учебное пособие для экономических специальностей вузов.– Казань: КГФЭИ, 2010. ↑

5. Гладкий, А.А. Обман, подставы и провокации в малом и среднем бизнесе: руководство. - С-Пб.: БХВ-Петербург. - 2013. ↑

6. Макаров В.Е. Социальные основы информационной безопасности деловой организации. Монография. Таганрог: Изд-ль С.А. Ступин,2015.-233с. ↑

7. Научное и прикладное использование современных информационных систем и технологий в подготовке ГГ-специалистов: коллективная монография под общей редакцией Я В Ворохобнной. ОХ Казначссвой - Невпнномысск: НГГТИ,2011.-230с. ↑

8. Лямин Л.В. Применение технологий электронного банкинга: риск-ориентированный подход /Л.В. Лямин. - М. : КНОРУС ; ЦИПСиР. 2011. - 336 с. ↑

9. Семененко В.Л. Информационная безопасность: Учебное пособие. 4-е изд.. стереотип. -М.:МГИУ. 2010.-277 с. ↑

10. Понятие национальной безопасности [электронный ресурс] - URL: php?dn=html&way=bW9kL2h0bWwvY29udGVudC84c2VtLzA2Mi8xLTEuaHRt (дата доступа 04.02.2016) ↑

11. Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. — СПб.: Питер, 2008. — 272 с: ил. ↑