Содержание:

Введение

Вопросы информационной безопасности играют сегодня огромную роль в сфере высоких технологий.

Информация - это одна из самых важных ценностей в современной жизни. С массовым внедрением компьютерных технологий во все сферы деятельности человека объем информации, хранимой в цифровом виде, вырос в десятки тысяч раз. А с появлением компьютерных сетей и Интернета даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Информационная безопасность - это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

Актуальность данной темы состоит в том, что защита информации становится все более востребованной в связи с высоким уровнем технологического прогресса: постоянно появляются новые и совершенствуются уже существующие носители информации, виды, методы и средства их защиты, а это естественным образом влечет за собой усовершенствование и усложнение средств противодействия защите.

Цель курсовой работы рассмотреть виды и состав угроз информационной безопасности.

Задачи курсовой работы:

- Рассмотреть теоретические основы обеспечения информационной безопасности
- Рассмотреть виды и структуру угроз информационной безопасности
- Рассмотреть методы защиты информации

Объектом исследования является информационная безопасность.

Предметом исследования виды и состав угроз информационной безопасности.

Глава 1. Теоретические основы обеспечения информационной безопасности

1.1 Понятие информации и информационной безопасности

Термин «информация» происходит от латинского слова «information», что означает сведения, разъяснения, изложение. Обычно под информацией понимаются знания, сведения, данные, сообщения и сигналы, с которыми мы имеем дело в повседневной жизни и проявление которых мы наблюдаем в природе и обществе.

Такое понятие информации приведено в ФЗ РФ от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации»: информация - сведения (сообщения, данные) независимо от формы их представления.

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства. [1]

Информационная безопасность - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие информационной безопасности положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации (дословно - «Информационная безопасность - это состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз»).[2]

Основные принципы информационной безопасности:

- **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;
- **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;
- **Доступность информации** - это свойство характеризует способность обеспечивать своевременный и беспрепятственный доступ полноправных пользователей к требуемой информации;
- **Достоверность** - данный принцип выражается в строгой принадлежности информации субъекту, который является ее источником или от которого она принята.

Безопасность связана с защитой активов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека, злонамеренными или иными.

За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельца.

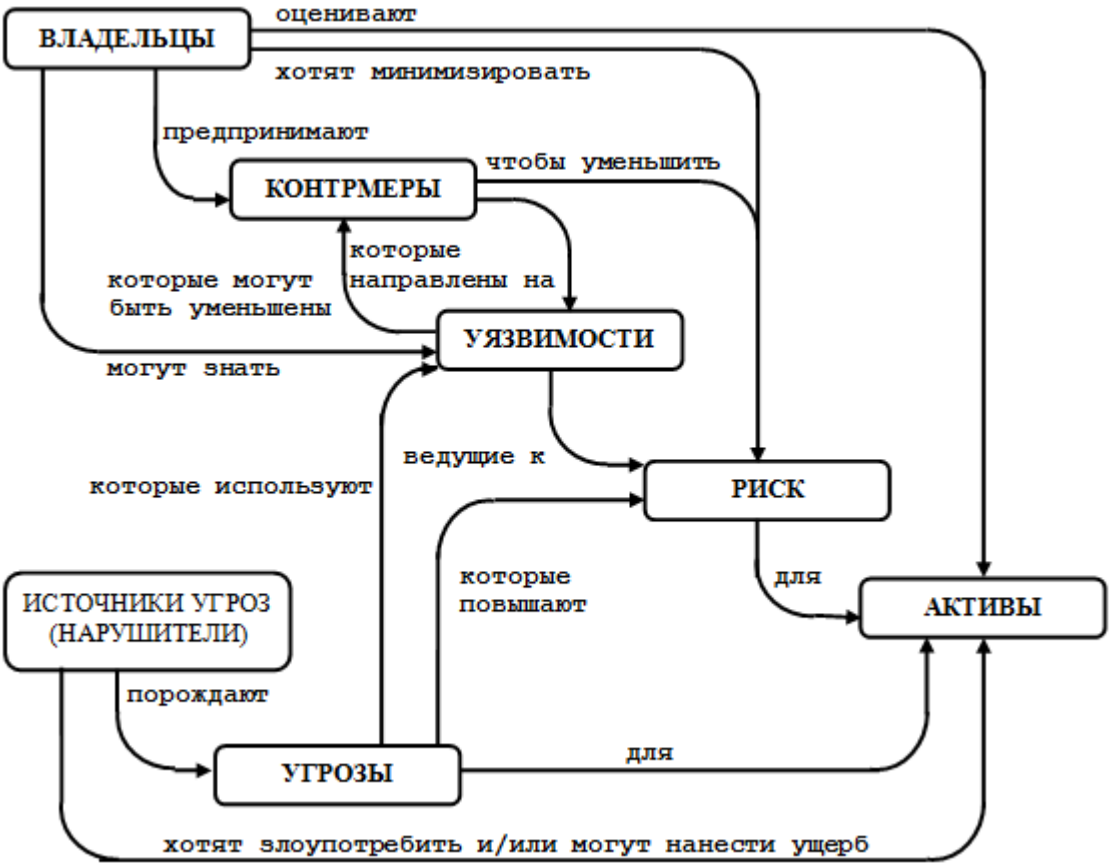

Рисунок 1. Понятия безопасности и их взаимосвязь

К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности владельцев активов (прямо или косвенно распределяя между этими составляющими). Такие уязвимости могут использоваться нарушителями, представляя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск, задавая дополнительные ограничения. [3]

1.2 Анализ и оценка рисков информационной безопасности

В соответствии с ГОСТ Р 51897–2002 «Менеджмент риска. Термины и определения», BS 7799-3:2006 «Система управления ИБ. Руководство по управлению рисками ИБ» процесс управления рисками представляет собой скоординированные действия по управлению и контролю организации в отношении риска. Управление рисками включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске.

Цель процесса оценивания рисков состоит в определении характеристик рисков по отношению к информационной системе и ее ресурсам (активам). На основе полученных данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность ресурсов, оценки значимости угроз, уязвимостей, эффективность существующих и планируемых средств защиты и многое другое.

Угроза (Threat) – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость (Vulnerability) – слабость в системе защиты, которая делает возможным реализацию угрозы.

Анализ рисков (Risk Analysis) – процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Базовый уровень безопасности (Baseline Security) – обязательный минимальный уровень защищенности для информационных систем. В ряде стран существуют критерии для определения этого уровня.

Базовый (Baseline) анализ рисков – анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области ИБ.

Полный (Full) анализ рисков – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

Риск нарушения ИБ (Security Risk) – возможность реализации угрозы.

Оценка рисков (Risk Assessment) – идентификация рисков, выбор параметров для их описания и получение оценок по этим параметрам.

Управление рисками (Risk Management) – процесс определения контрмер в соответствии с оценкой рисков.

Система управления ИБ (Information Security Management System) – комплекс мер, направленных на обеспечение режима ИБ на всех стадиях жизненного цикла ИС.

Ресурсы (активы) – объекты, имеющие ценность для организации и оказывающие влияние на непрерывность осуществления деятельности. Все ресурсы должны быть идентифицированы и учтены, также должны быть определены владельцы ресурсов.

В BS ISO/IEC 17799-2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» выделяются следующие типы ресурсов:

- информация: базы данных и файлы данных, договоры и соглашения, системная документация, руководства пользователей, планы обеспечения непрерывности бизнеса, процедуры восстановления, журналы аудита и архивная информация;
- программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, средства разработки и утилиты;
- физические ресурсы: компьютерное оборудование, коммуникационное оборудование, переносные носители и другое оборудование;
- сервисы: вычислительные и телекоммуникационные сервисы, основные коммунальные услуги, например, отопление, освещение, электроэнергия и кондиционирование;
- организации.

Схема управления рисками информационной безопасности приведена на рис. 1.3.

Рисунок 2. Управление рисками ИБ

При анализе рисков, ожидаемый ущерб, в случае реализации угроз, сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении оцениваемого риска, который может быть:

- снижен, например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности;
- устранен, за счет отказа от использования подверженного угрозе ресурса;
- перенесен, например, застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания;
- принят.[4]

Глава 2. Виды и структура угроз информационной безопасности

2.1 Понятие и структура угроз защищаемой информации

Существует три различных подхода в определении угроз, которые включают в себя следующее:

1. Угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения безопасности информации, при этом безопасность информации означает, что информация находится в таком защищённом виде, который способен противостоять любым дестабилизирующим воздействиям;

2. Угроза трактуется как явление (событие, случай или возможность их возникновения), следствием которых могут быть нежелательные воздействия на информацию;

3. Угроза определяется как реальные или потенциально возможные действия, или условия, приводящие к той или другой форме проявления уязвимости информации.

Любая угроза не сводится к чему-то однозначному, она состоит из определённых взаимосвязанных компонентов, каждый из которых сам по себе не составляет угрозу, но является её частью. Сама угроза возникает лишь при совокупном их взаимодействии.

Угрозы защищаемой информации связаны с её уязвимостью, то есть неспособностью информации самостоятельно противостоять дестабилизирующим воздействиям, нарушающим её статус. А нарушение статуса защищаемой информации состоит в нарушении её физической сохранности, логической структуры и содержания, доступности для правомочных пользователей, конфиденциальности (закрытости для посторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации.

Прежде всего угроза должна иметь какие-то сущностные проявления, а любое проявление принято называть явлением, следовательно, одним из признаков и вместе с тем одной из составляющих угроз должно быть явление.

В основе любого явления лежат составляющие причины, которые являются его движущей силой и которые в свою очередь обусловлены определёнными обстоятельствами или предпосылками. Эти причины и обстоятельства относятся к

факторам, создающим возможность дестабилизирующего воздействия на информацию. Таким образом, факторы являются её одним признаком и составляющей угрозы.

Ещё одним определённым признаком угрозы является её направленность, то есть результат, к которому может привести дестабилизирующее воздействие на информацию.

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Для раскрытия структуры угроз необходимо признаки угроз конкретизировать содержательной частью, которые в свою очередь должны раскрыть характер явлений и факторов, определить из состава и состав условий.

К сущностным проявлениям угрозы относятся:

- источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
- виды дестабилизирующего воздействия на информацию (каким образом);
- способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам помимо причин и обстоятельств следует отнести наличие каналов и методов несанкционированного доступа к конфиденциальной информации для воздействия на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

2.2 Классификация угроз информационной безопасности

Классификация угроз может быть проведена по множеству признаков. Наиболее распространённые из них.

По природе возникновения принято выделять естественные и искусственные угрозы. Естественными принято называть угрозы, возникшие в результате воздействия на автоматизированные системы объективных физических процессов или стихийных природных явлений, не зависящих от человека. В свою очередь,

искусственные угрозы вызваны действием человеческого фактора.

Примерами естественных угроз могут служить пожары, наводнения, цунами, землетрясения и т.д. Неприятная особенность таких угроз -чрезвычайная трудность или даже невозможность их прогнозирования. По степени преднамеренности выделяют случайные и преднамеренные угрозы. Случайные угрозы бывают обусловлены халатностью или непреднамеренными ошибками персонала. Преднамеренные угрозы обычно возникают в результате направленной деятельности злоумышленника.

В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных, неумышленную порчу оборудования. Пример преднамеренной угрозы проникновение

злоумышленника на охраняемую территорию с нарушением установленных правил физического доступа.

В зависимости от источника угрозы принято выделять:

- Угрозы, источником которых является природная среда. Примеры таких угроз - пожары, наводнения и другие стихийные бедствия;
- Угрозы, источником которых является человек. Примером такой угрозы может служить внедрение агентов в ряды персонала автоматизированных систем со стороны конкурирующей организации;
- Угрозы, источником которых являются санкционированные программно-аппаратные средства. Пример такой угрозы некомпетентное использование системных утилит;
- Угрозы, источником которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение систему кейлоггеров.

По положению источника угрозы выделяют:

- Угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз - перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи; дистанционная фото и видеосъёмка; перехват акустической информации с использованием направленных микрофонов;
- Угрозы, источник которых расположен в пределах контролируемой зоны. Примерами подобных угроз могут служить применение

подслушивающих устройств или хищение носителей, содержащих конфиденциальную информацию.

По степени воздействия на автоматизированные системы выделяют пассивные и активные угрозы. Пассивные угрозы при реализации не осуществляют никаких изменений в составе и структуре автоматизированных систем.

Реализация активных угроз, напротив, нарушает структуру автоматизированной системы. Примером пассивной угрозы может служить несанкционированное копирование файлов с данными.

По способу доступа к ресурсам автоматизированных систем выделяют:

- Угрозы, использующие стандартный доступ. Пример такой угрозы - несанкционированное получение пароля путём подкупа, шантажа, угроз или физического насилия по отношению к законному обладателю;
- Угрозы, использующие нестандартный путь доступа. Пример такой угрозы использование не декларированных возможностей средств защиты.

Критерии классификации угроз можно продолжать, однако на практике чаще всего используется следующая основная классификация угроз, основывающаяся на трёх введённых ранее базовых свойствах защищаемой информации:

1. Угрозы нарушения конфиденциальности информации, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.
2. Угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием автоматизированных систем.
3. Угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу автоматизированной системе для легальных пользователей блокируется.

Отметим, что реальные угрозы информационной безопасности далеко не всегда можно строго отнести к какой-то одной из перечисленных категорий. Так, например, угроза хищения носителей информации может быть при определённых условиях отнесена ко всем трём категориям. Заметим, что перечисление угроз, характерных для той или иной автоматизированной системы, является важным этапом анализа уязвимостей автоматизированных систем, проводимого, например, в рамках аудита информационной безопасности, и создаёт базу для последующего

проведения анализа рисков.

Выделяют два основных метода перечисления угроз:

1. Построение произвольных списков угроз. Возможные угрозы выявляются экспертным путём и фиксируются случайным и неструктурированным образом. Для данного подхода характерны неполнота и противоречивость получаемых результатов.
2. Построение деревьев угроз. Угрозы описываются в виде одного или нескольких деревьев. Детализация угроз осуществляется сверху вниз, и в конечном итоге каждый лист дерева даёт описание конкретной угрозы. Между поддеревьями в случае необходимости могут быть организованы логические связи. Рассмотрим в качестве примера дерево угрозы блокирования доступа к сетевому приложению (рис. 3).

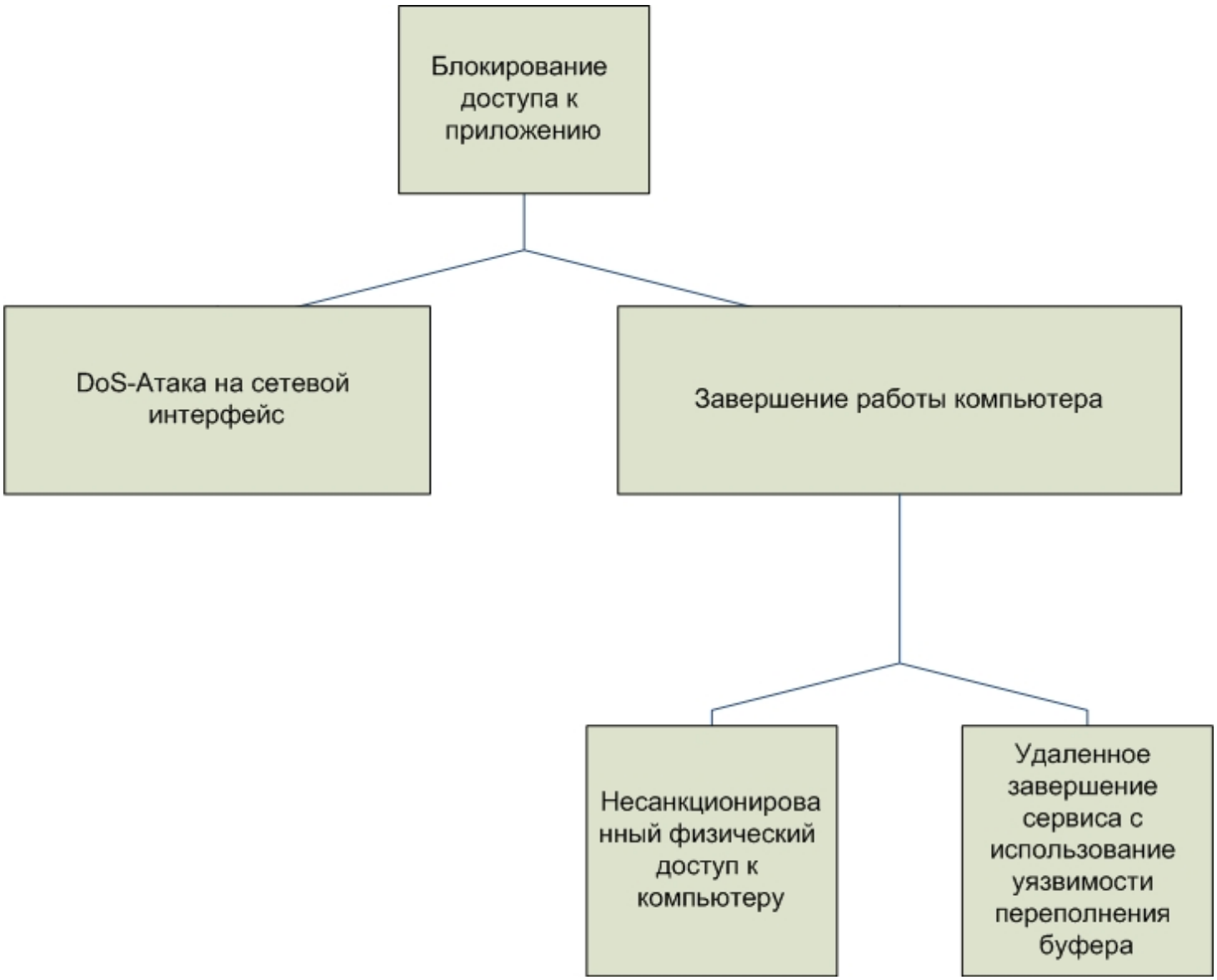

Рисунок 3. Дерево угрозы блокирования доступа к сетевому приложению

2.3 Виды угроз информационной безопасности

Определение, анализ и классификация возможных угроз безопасности АИС является одним из важнейших аспектов проблемы обеспечения ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Классификацию угроз ИБ можно выполнить по нескольким критериям:

1. По аспекту ИБ: угрозы конфиденциальности, угрозы целостности, угрозы доступности. Дополнительно можно выделить угрозы аутентичности и апеллируемости.

2. По компонентам АИС, на которые нацелена угроза: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура).

3. По расположению источника угроз: внутри или вне рассматриваемой АИС. Угрозы со стороны инсайдеров являются наиболее опасными.

4. По природе возникновения: естественные (объективные) и искусственные (субъективные). Естественные угрозы — это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека. Искусственные угрозы — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и преднамеренные (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Рассмотрим перечень конкретных угроз:

Основные непреднамеренные искусственные угрозы АС (действия, совершаемые

людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

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

3) неумышленная порча носителей информации;

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

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием

ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

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

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

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

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

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы с внешних носителей и т.п.);

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

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

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

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

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

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

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

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

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

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

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

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации

пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации;

10) несанкционированное копирование носителей информации;

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

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

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

14) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический

адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

16) вскрытие шифров криптозащиты информации;

17) внедрение аппаратных спецвложений, программных «закладок» и вирусов (троянских коней), то есть таких участков программ, которые не нужны для осуществления

заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

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

сообщений;

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

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

2.4 Каналы утечки информации

При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

- акустическое излучение информативного речевого сигнала;

- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы КЗ (контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);

- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;

- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;

- побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;

- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии

паразитной генерации в узлах (элементах) технических средств;

- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;

- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

- прослушивание ведущихся телефонных и радиопереговоров;

- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

- хищение технических средств с хранящейся в них информацией или отдельных носителей информации.

Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;

- из смежных помещений, принадлежащих другим учреждениям (предприятиям) и расположенным в том же здании, что и объект защиты;

- при посещении учреждения (предприятия) посторонними лицами;

- за счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через информационные сети общего пользования.

Глава 3. Защита информации

3.1 Методы защиты информации

Защита информации в компьютерных системах обеспечивается созданием комплексной системы защиты. Комплексная система защиты включает:

- правовые методы защиты;
- организационные методы защиты;
- методы защиты от случайных угроз;
- методы защиты от традиционного шпионажа и диверсий;
    - ▪ ▪ методы защиты от электромагнитных излучений и наводок;
- методы защиты от несанкционированного доступа;
- криптографические методы защиты;
- методы защиты от компьютерных вирусов.

Среди методов защиты имеются и универсальные, которые являются базовыми при создании любой системы защиты. Это, прежде всего, правовые методы защиты информации, которые служат основой легитимного построения и использования системы защиты любого назначения. К числу универсальных методов можно отнести и организационные методы, которые используются в любой системе защиты без исключений и, как правило, обеспечивают защиту от нескольких угроз.

Методы защиты от случайных угроз разрабатываются и внедряются на этапах проектирования, создания, внедрения и эксплуатации компьютерных систем. К их числу относятся:

- создание высокой надёжности компьютерных систем;
- создание отказоустойчивых компьютерных систем;
- блокировка ошибочных операций;
- оптимизация взаимодействия пользователей и обслуживающего персонала с компьютерной системой;
- минимизация ущерба от аварий и стихийных бедствий;

- дублирование информации.

При защите информации в компьютерных системах от традиционного шпионажа и диверсий используются те же средства и методы защиты, что и для защиты других объектов, на которых не используются компьютерные системы. К их числу относятся:

- создание системы охраны объекта;
- организация работ с конфиденциальными информационными ресурсами;
- противодействие наблюдению и подслушиванию;
- защита от злоумышленных действий персонала.

Все методы защиты от электромагнитных излучений и наводок можно разделить на пассивные и активные. Пассивные методы обеспечивают уменьшение уровня опасного сигнала или снижение информативности сигналов. Активные методы защиты направлены на создание помех в каналах побочных электромагнитных излучений и наводок, затрудняющих приём и выделение полезной информации из перехваченных злоумышленником сигналов. На электронные блоки и магнитные запоминающие устройства могут воздействовать мощные внешние электромагнитные импульсы и высокочастотные излучения. Эти воздействия могут приводить к неисправности электронных блоков и стирать информацию с магнитных носителей информации. Для блокирования угрозы такого воздействия используется экранирование защищаемых средств.

Для защиты информации от несанкционированного доступа создаются:

- система разграничения доступа к информации;
- система защиты от исследования и копирования программных средств.

Исходной информацией для создания системы разграничения доступа является решение администратора компьютерной системы о допуске пользователей к определённым информационным ресурсам. Так как информация в компьютерных системах хранится, обрабатывается и передаётся файлами (частями файлов), то доступ к информации регламентируется на уровне файлов. В базах данных доступ может регламентироваться к отдельным её частям по определённым правилам. При определении полномочий доступа администратор устанавливает операции, которые разрешено выполнять пользователю. Различают следующие операции с файлами:

- чтение (R);

- запись;
- выполнение программ (E).

Операции записи имеют две модификации:

- субъекту доступа может быть дано право осуществлять запись с изменением содержимого файла (W);
- разрешение дописывания в файл без изменения старого содержимого (A).

Система защиты от исследования и копирования программных средств включает следующие методы:

- методы, затрудняющие считывание скопированной информации;
- методы, препятствующие использованию информации.

Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий. По виду воздействия на исходную информацию методы криптографического преобразования информации разделяются на следующие группы:

- шифрование;
- стенография;
- кодирование;
- сжатие.

Вредительские программы и, прежде всего, вирусы представляют очень серьёзную опасность для информации в компьютерных системах. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

Компьютерные вирусы - это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в компьютерных системах. Вирусы могут выполнять изменение или уничтожение программного обеспечения или данных, хранящихся в компьютерных системах. В процессе распространения вирусы могут себя модифицировать.

Все компьютерные вирусы классифицируются по следующим признакам:

- по среде обитания;

- по способу заражения;
- по степени опасности вредительских воздействий;
- по алгоритму функционирования.

По среде обитания компьютерные вирусы подразделяются на:

- сетевые;
- файловые;
- загрузочные;
- комбинированные.

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах внешних запоминающих устройств. Комбинированные вирусы размещаются в нескольких средах обитания. Например, загрузочно-файловые вирусы.

По способу заражения среды обитания компьютерные вирусы делятся на:

- резидентные;
- нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания в оперативную память компьютера. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешённые только операционной системе, заражают среду обитания и при выполнении определённых условий реализуют вредительскую функцию.

Нерезидентные вирусы попадают в оперативную память компьютера только на время их активности, в течение которого выполняют вредительскую функцию и функцию заражения. Затем они полностью покидают оперативную память, оставаясь в среде обитания.

По степени опасности для информационных ресурсов пользователя вирусы разделяются на:

- безвредные;
- опасные;
- очень опасные.

Безвредные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам компьютерной системы. Однако такие вирусы всё-таки наносят определённый ущерб:

- расходуют ресурсы компьютерной системы;
- могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов;
- вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы при модернизации операционной системы или аппаратных средств.

Опасные вирусы вызывают существенное снижение эффективности компьютерной системы, но не приводят к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах.

Очень опасные вирусы имеют следующие вредительские воздействия:

- вызывают нарушение конфиденциальности информации;
- уничтожают информацию;
- вызывают необратимую модификацию (в том числе и шифрование) информации;
- блокируют доступ к информации;
- приводят к отказу аппаратных средств;
- наносят ущерб здоровью пользователям.

По алгоритму функционирования вирусы подразделяются на:

- не изменяющие среду обитания при их распространении;
- изменяющие среду обитания при их распространении.

Для борьбы с компьютерными вирусами используются специальные антивирусные средства и методы их применения. Антивирусные средства выполняют следующие задачи:

- обнаружение вирусов в компьютерных системах;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Обнаружение вирусов и блокирование работы программ-вирусов осуществляется следующими методами:

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита.

Устранение последствий воздействия вирусов реализуется следующими методами:

- восстановление системы после воздействия известных вирусов;
- восстановление системы после воздействия неизвестных вирусов.

3.2 Профилактика заражения вирусами компьютерных систем

Главным условием безопасной работы в КС является соблюдение ряда правил, которые апробированы на практике и показали свою высокую эффективность:

Правило первое – использование программных продуктов, полученных законным официальным путем. Вероятность наличия вируса в пиратской копии во много раз выше, чем в официально полученном программном обеспечении;

Правило второе – дублирование информации. Прежде всего, необходимо сохранять дистрибутивные носители ПО. При этом запись на носители, допускающие выполнение этой операции, должна быть, по возможности, заблокирована. Следует особо позаботиться о сохранении рабочей информации. Предпочтение в создании копий – съемным машинным носителям информации с защитой от записи;

Правило третье – регулярно использовать антивирусные средства (перед началом работы целесообразно выполнять программы-сканеры и программы-ревизоры. Антивирусные средства должны регулярно обновляться;

Правило четвертое – особую осторожность следует проявлять при использовании новых съемных носителей информации и новых файлов (новые дискеты обязательно должны быть проверены на отсутствие загрузочных и файловых вирусов, а полученные файлы – на наличие файловых вирусов (программами-сканерами и программами, осуществляющими эвристический анализ). При первом выполнении исполняемого файла используются резидентные сторожа. При работе

с полученными документами и таблицами целесообразно запретить выполнение макрокоманд средствами, встроенными в текстовые и табличные редакторы, до завершения полной проверки этих файлов;

Правило пятое – при работе в распределенных системах или в системах коллективного пользования целесообразно новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели ЭВМ (АРМ администратора системы или лица, отвечающего за безопасность информации) и только после всесторонней проверки они могут передаваться пользователям;

Правило шестое – если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции.

О наличии вируса в КС пользователь может судить по следующим событиям:

- появление сообщений антивирусных средств о заражении или о предполагаемом заражении;

- явные проявления присутствия вируса, такие как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в КС;

- неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств КС.

Заключение

Люди являются самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию. Причины, обстоятельства и условия этого воздействия относительно людей следует рассматривать, исходя из классификации преднамеренного и непреднамеренного воздействия. Подводя итог, следует отметить, что для предотвращения преднамеренного воздействия особое внимание следует уделять морально-нравственному портрету человека и организации комплексной системы защиты информации. В случае же непреднамеренного воздействия ключевыми пунктами являются уровень квалификации сотрудников и наличие хорошо разработанных правил работы с защищаемой информацией. Это еще раз подтверждает, что в

процессе защиты информации должны быть задействованы все лица, работающие с защищаемой информацией.

Также и для остальных источников угроз (кроме природных явлений) были рассмотрены причины, обстоятельства и условия дестабилизирующего воздействия на информацию. В конечном счете, основное внимание следует уделить качеству как самих средств обеспечения функционирования информационных процессов, так и к их обслуживанию, профилактическим проверкам.

Что касается такого источника угроз, как природные явления, то в данном случае возможно лишь минимизировать потери от урона (например, посредством технических средств), но никак не устранить или нейтрализовать данный источник.

В конечном счете, классификация и характеристика источников угроз защищаемой информации является неотъемлемой частью процесса защиты информации.

Список использованной литературы и источников

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие.

– М.: Изд. Центр ЕАОИ, 2012. – 311 с.
2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
3. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
4. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
5. Конотопов, М.В. Информационная безопасность. Лабораторный практикум / М.В. Конотопов. - М.: КноРус, 2013. - 136 с.
6. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов. / А.А. Малюк. - М.: Горячая линия -Телеком , 2004. - 280 с.
7. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.
8. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

9. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.
10. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.
11. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2011. - 277 с.
12. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2010. - 336 с.
13. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
14. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

1. Гафнер В. В. Информационная безопасность: учеб. пособие / В.В. Гафнер — Ростов н/Д: Феникс, 2010. — 324 с. ↑

2. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия-Телеком, 2004. - 280 с. ↑

3. ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий". ↑

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие.

   – М.: Изд. Центр ЕАОИ, 2012. – 311 с. ↑