Содержание:

ВВЕДЕНИЕ

Информация играет важную роль в обеспечении всех сторон жизнедеятельности общества и особо важная информация всегда подлежала защите от разглашения.

Анализ состояния ситуации в области защиты информации показывает, что в промышленно развитых странах мира существует вполне сложившаяся система защиты информации (ЗИ) в устройствах обработки данных. И, тем не менее, угрозы средствам и методам защиты информации не только не уменьшаются, но и достаточно интенсивно возрастают.

Развитие новых информационных технологий сопровождается такими негативными явлениями, как промышленный шпионаж, компьютерные преступления и несанкционированный доступ (НСД) к конфиденциальной информации. Возникли новые понятия «кибертерроризм», «информационная война» и т.п. Поэтому защита информации является важнейшей государственной задачей в любом государстве. Острая необходимость в защите информации в России нашла выражение в создании Государственной системы защиты информации (ГСЗИ) и в развитии правовой базы информационной безопасности.

Защита информации должна обеспечивать предотвращение ущерба в результате утери (хищения, утраты, искажения, подделки) информации в любом ее виде. Организация мер защиты информации должна проводиться в полном соответствии с действующими законами и нормативными документами по безопасности информации, интересами пользователей информации. Чтобы гарантировать высокую степень защиты информации, необходимо постоянно решать сложные научно-технические задачи разработки и совершенствования средств ее защиты.

В настоящее время широко используются информационные технологии, с их появлением *актуальной* становится проблема защиты информации.

Цель данной курсовой работы состоит в определении видов угроз информационной безопасности и их состава.

Объектом исследования являются сети и информация, передаваемая по компьютерным сетям.

Предметом исследования является обеспечение информационной безопасности сетей.

Для выполнения поставленной цели, необходимо выполнить ряд задач:

- рассмотреть основные угрозы безопасности сети в теоретических источниках;

- провести обзор возможных мер обеспечения безопасности сети и средств защиты;

- провести оценку эффективности мероприятий по защите информации.

Курсовая работа состоит из введения, двух глав, заключения, списка использованных источников и приложений.

При написании курсовой работы использовались труды таких ученых, как Алферов А.П., Белкин П.Ю., Коженевский С.Р., Коул Э., Кравченко В.А., Партыка Т.Л. и других.

ГЛАВА 1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕРЫ ПРЕДОТВРАЩЕНИЯ

1.1. Понятие и виды угроз информационной безопасности

Под угрозой безопасности информации в компьютерной сети (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.[1]

Уязвимость информации — это возможность возникновения такого состояния, при котором создаются условия для реализации угроз безопасности информации.

Атакой на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.

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.[2] 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 состав и состав условий.

К сущностным проявлениям угрозы относятся:[3]

1. источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
2. виды дестабилизирующего воздействия на информацию (каким образом);
3. 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.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на классы (Приложение).

К источникам дестабилизирующего воздействия на информацию относятся:

1. люди;
2. технические средства отображения, хранения, обработки, воспроизведения, передачи информации, средства связи;
3. системы обеспечения функционирования технических средств;
4. технологические процессы отдельных категорий промышленных объектов;
5. природные явления.

Самым распространенным, многообразным и опасным источником дестабилизирующего воздействия на защищаемую информацию являются люди. Он таков, потому что воздействие на защищаемую информацию могут оказывать различные категории людей, как работающих, так и неработающих на

предприятии.

К этому источнику относятся:

1. сотрудники данного предприятия;
2. лица, не работающие на предприятии, но имеющие доступ к защищаемой информации в силу служебного положения;
3. сотрудники государственных органов разведки других стран и конкурирующих предприятий;
4. лица из криминальных структур.

Технические средства являются вторыми по значению источником дестабилизирующего воздействия на защищаемую информацию в силу их многообразия.

К этому источнику относятся:

1. электронно-вычислительная техника;
2. электрические и автоматические машинки и копировально-множительная техника;
3. средства видео и звукозаписывающей и воспроизводящей техники;
4. средства телефонной, телеграфной, факсимильной, громкоговорящей;
5. средства радиовещания и телевидения;
6. средства кабельной и радиосвязи.

Третий источник дестабилизирующего воздействия на информацию включает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования. К этому источнику примыкают вспомогательные электрические и радиоэлектронные системы и средства.[4]

К четвертому источнику относятся технологические процессы обработки различных объектов ядерной энергетики, химической промышленности, радиоэлектроники, а также объекты по изготовлению некоторых видов вооружения и военной техники, которые изменяют естественную структуру окружающей среды.

Пятый источник – это природные явления, которые включают в себя две составляющие:

1. стихийные бедствия;
2. атмосферные явления.

Со стороны людей возможно следующие виды дестабилизирующих воздействий:

- 1. непосредственное воздействие на носители защищаемой информации;
  2. несанкционированное распространение конфиденциальной информации;
  3. нарушение режима работы технических средств отображение хранения, обработки, воспроизведения, передачи информации, средств связи и технологий обработки информации;
  4. вывод из строя технических средств и средств связи;
  5. вывод из строя и нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия на носители защищаемой информации могут быть:

1. физическое разрушение носителя информации;
2. создание аварийных ситуации для носителей;
3. удаление информации с носителей;
4. создание искусственных магнитных полей для размагничивания носителей;
5. внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

1. словесная передача информации (разбалтывание);
2. передача копий носителя информации;
3. показ носителей информации;
4. ввод информации в вычислительные сети и системы;
5. опубликование информации в открытой печати;
6. использование информации в открытых публичных выступлениях;
7. к несанкционированному распространению информации может так же принести и потеря носителей информации.

Способами нарушение работы технических средств и обработки информации могут быть:[5]

1. повреждения отдельных элементов средств
2. нарушение правил эксплуатации средств
3. внесение изменений в порядок обработки информации
4. заражение программ обработки информации вредоносными программами
5. выдача неправильных программных команд

6. превышение расчетного числа запросов
7. создание помех в радио-эфире с помощью дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации
8. передача ложных сигналов
9. подключение подавляющих фильтров в информационные цепи, цепи питание и заземления
10. нарушение режима работы систем обеспечения функционирования средств

К четвертому виду можно отнести следующие способы:

- 1. неправильный монтаж технических средств;
  2. разрушение (поломка) средств, в том числе, повреждения (разрыв) кабельных линий связи;
  3. создание аварийных ситуаций для технических средств;
  4. отключение средств от сетей питания;
  5. вывод из строя или нарушения режима работы систем обеспечения функционирования средств;
  6. монтирование в электронно-вычислительную технику разрушающих радио и программных закладок.

Способом вывода из строя и нарушения режима работы систем обеспечения функционирования технических средств можно отнести:

1. не правильный монтаж систем;
2. разрушение или поломка систем или их отдельных элементов;
3. создание аварийных ситуаций для систем;
4. отключение систем от источников питания;
5. нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

1. выход средств из строя;
2. сбои в работе средств;
3. создание электромагнитных излучений;

Основными способами дестабилизирующего воздействия второго источника являются:

1. технические поломки и аварии;
2. возгорание технических средств;

3. выход из строя систем обеспечения функционирования средств;
4. негативные воздействия природных явлений;
5. воздействия измененной структуры окружающего магнитного поля;
6. воздействия вредоносных программных продуктов;
7. разрушение или повреждение носителя информации;
8. возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

1. выход систем из строя;
2. сбои в работе системы.

К способам этого вида относятся:

1. поломки и аварии;
2. возгорания;
3. выход из строя источников питания;
4. воздействия природных явлений;
5. появление технических неисправностей элементов системы;
6. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
7. изменения химического состава окружающей среды (на объектах химической промышленности);
8. изменения локальной структуры магнитного поля происходящего вследствие деятельности объектов радиоэлектроники и при изготовлении некоторых видов вооружения и военной технике.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясения, наводнения, ураган (смерч), оползни, лавины, извержения вулканов.

К атмосферным явлениям (видам воздействия) относятся: гроза, дождь, снег, град, мороз, жара, изменения влажности воздуха и магнитные бури.

1.2. Меры предотвращения угроз информационной безопасности

По способам осуществления все меры обеспечения безопасности компьютерных сетей подразделяются на: правовые (законодательные), морально-этические, организационные (административные), физические, технические (аппаратно-программные).[6]

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

К морально-этическим мерам противодействия относятся нормы поведения, которые традиционно сложились или складываются по мере распространения компьютерных сетей в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании сетей и других объектов систем обработки данных;

- мероприятия по разработке правил доступа пользователей к ресурсам сетей (разработка политики безопасности);

- мероприятия, осуществляемые при подборе и подготовке персонала;

- организацию охраны и надежного пропускного режима;

- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

- организацию явного и скрытого контроля за работой пользователей;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

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

Технические (аппаратные) меры защиты основаны на использовании различных электронных устройств, входящих в состав КС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

Программные методы защиты предназначаются для непосредственной защиты информации по трем направлениям: а) аппаратуры; б) программного обеспечения; в) данных и управляющих команд.

Для защиты информации при ее передаче обычно используют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.[7]

Все программы защиты, осуществляющие управление доступом к машинной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными.

Доступ может быть определен как:

- общий (безусловно предоставляемый каждому пользователю);

- отказ (безусловный отказ, например разрешение на удаление порции информации);

- зависимый от события (управляемый событием);

- зависимый от содержания данных;

- зависимый от состояния (динамического состояния компьютерной системы);

- частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз);

- по имени или другим признаком пользователя;

- зависимый от полномочий;

- по разрешению (например, по паролю);

- по процедуре.

Также к эффективным мерам противодействия попыткам несанкционированного доступа относятся средства регистрации. Для этих целей наиболее перспективными являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название мониторинга (автоматического наблюдения за возможной компьютерной угрозой).

Мониторинг осуществляется самой операционной системой (ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения машинной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга). В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия “логической бомбы”.

Задачи обеспечения безопасности:[8]

- защита информации в каналах связи и базах данных криптографическими методами;

- подтверждение подлинности объектов данных и пользователей (аутентификация сторон, устанавливающих связь);

- обнаружение нарушений целостности объектов данных;

- обеспечение защиты технических средств и помещений, в которых ведется обработка конфиденциальной информации, от утечки по побочным каналам и от возможно внедренных в них электронных устройств съема информации;

- обеспечение защиты программных продуктов и средств вычислительной техники от внедрения в них программных вирусов и закладок;

- защита от несанкционированных действий по каналу связи от лиц, не допущенных к средствам шифрования, но преследующих цели компрометации секретной информации и дезорганизации работы абонентских пунктов;

- организационно-технические мероприятия, направленные на обеспечение сохранности конфиденциальных данных.

Разобрать подробно все методы и средства защиты информации в рамках ВКР просто невозможно. Охарактеризую только некоторые из них.

К мерам физической защиты информации относятся:

- защита от огня;

- защита от воды и пожаротушащей жидкости

- защита от коррозийных газов;

- защита от электромагнитного излучения;

- защита от вандализма;

- защита от воровства и кражи;

- защита от взрыва;

- защита от падающих обломков;

- защита от пыли;

- защита от несанкционированного доступа в помещение.

Какие же действия нужно предпринять, чтобы обеспечить физическую безопасность?

В первую очередь надо подготовить помещение, где будут стоять серверы. Обязательное правило: сервер должен находиться в отдельной комнате, доступ в которую имеет строго ограниченный круг лиц. В этом помещении следует установить кондиционер и хорошую систему вентиляции. Там же можно поместить мини-АТС и другие жизненно важные технические системы.

Разумным шагом станет отключение неиспользуемых дисководов, параллельных и последовательных портов сервера. Его корпус желательно опечатать. Все это осложнит кражу или подмену информации даже в том случае, если злоумышленник каким-то образом проникнет в серверную комнату. Не стоит пренебрегать и такими тривиальными мерами защиты, как железные решетки и двери, кодовые замки и камеры видеонаблюдения, которые будут постоянно вести запись всего, что происходит в ключевых помещениях офиса.

Другая характерная ошибка связана с резервным копированием. О его необходимости знают все, так же как и о том, что на случай возгорания нужно иметь огнетушитель. А вот о том, что резервные копии нельзя хранить в одном помещении с сервером, почему-то забывают. В результате, защитившись от информационных атак, фирмы оказываются беззащитными даже перед небольшим пожаром, в котором предусмотрительно сделанные копии гибнут вместе с сервером.

Часто, даже защитив серверы, забывают, что в защите нуждаются и всевозможные провода - кабельная система сети. Причем, нередко приходится опасаться не злоумышленников, а самых обыкновенных уборщиц, которые заслуженно считаются самыми страшными врагами локальных сетей. Лучший вариант защиты кабеля - это короба, но, в принципе, подойдет любой другой способ, позволяющий скрыть и надежно закрепить провода. Впрочем, не стоит упускать из вида и возможность подключения к ним извне для перехвата информации или создания помех, например, посредством разряда тока. Хотя, надо признать, что этот вариант мало распространен и замечен лишь при нарушениях работы крупных фирм.

Помимо Интернета, компьютеры включены еще в одну сеть - обычную электрическую. Именно с ней связана другая группа проблем, относящихся к физической безопасности серверов. Ни для кого не секрет, что качество современных силовых сетей далеко от идеального. Даже если нет никаких внешних признаков аномалий, очень часто напряжение в электросети выше или ниже нормы. При этом большинство людей даже не подозревают, что в их доме или офисе существуют какие-то проблемы с электропитанием.[9]

Пониженное напряжение является наиболее распространенной аномалией и составляет около 85% от общего числа различных неполадок с электропитанием. Его обычная причина - дефицит электроэнергии, который особенно характерен для зимних месяцев. Повышенное напряжение почти всегда является следствием какой-либо аварии или повреждения проводки в помещении. Часто в результате отсоединения общего нулевого провода соседние фазы оказываются под напряжением 380 В. Бывает также, что высокое напряжение возникает в сети из-за неправильной коммутации проводов.

Источниками импульсных и высокочастотных помех могут стать разряды молний, включение или отключение мощных потребителей электроэнергии, аварии на подстанциях, а также работа некоторых бытовых электроприборов. Чаще всего такие помехи возникают в крупных городах и в промышленных зонах. Импульсы напряжения при длительности от наносекунд (10~9 с) до микросекунд (10~6 с) могут по амплитуде достигать нескольких тысяч вольт.[10] Наиболее уязвимыми к таким помехам оказываются микропроцессоры и другие электронные компоненты. Нередко непогашенная импульсная помеха может привести к перезагрузке сервера или к ошибке в обработке данных. Встроенный блок питания компьютера, конечно, частично сглаживает броски напряжения, защищая электронные компоненты компьютера от выхода из строя, но остаточные помехи все равно снижают срок службы аппаратуры, а также приводят к росту температуры в блоке питания сервера.

Для защиты компьютеров от высокочастотных импульсных помех служат сетевые фильтры (например, марки Pilot), оберегающие технику от большинства помех и перепадов напряжения. Кроме того, компьютеры с важной информацией следует обязательно оснащать источником бесперебойного питания (UPS). Современные модели UPS не только поддерживают работу компьютера, когда пропадает питание, но и отсоединяют его от электросети, если параметры электросети выходят из допустимого диапазона.

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным аппаратным средствам защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);

- устройства для шифрования информации;

- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

- устройства уничтожения информации на магнитных носителях;

- устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Аппаратные средства привлекают все большее внимание специалистов не только потому, что их легче защитить от повреждений и других случайных или злоумышленных воздействий, но еще и потому, что аппаратная реализация функций выше по быстродействию, чем программная, а стоимость их неуклонно снижается.

На рынке аппаратных средств защиты появляются все новые устройства. Ниже приводится в качестве примера описание электронного замка.

Электронный замок «Соболь».

«Соболь», разработанный и поставляемый ЗАО НИП «Информзащита», обеспечивает выполнение следующих функций защиты:

- идентификация и аутентификация пользователей;

- контроль целостности файлов и физических секторов жесткого диска;

- блокировка загрузки ОС с дискеты и CD-ROM;

- блокировка входа в систему зарегистрированного пользователя при превышении им заданного количества неудачных попыток входа;

регистрация событий, имеющих отношение к безопасности системы.

Идентификация пользователей производится по индивидуальному ключу в виде «таблетки» Touch Memory, имеющей память до 64 Кбайт, а аутентификация — по паролю длиной до 16 символов.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;

- программы разграничения доступа пользователей к ресурсам КС;

- программы шифрования информации;

- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Надо понимать, что под идентификацией, применительно к обеспечению информационной безопасности КС, понимают однозначное распознавание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Также к программным средствам защиты информации относятся:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

- программы тестового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:[11]

- простота тиражирования;

- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);

- простота применения — одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя ни каких новых (по сравнению с другими программами) навыков;

- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

К недостаткам программных средств защиты информации относятся:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирование программ защиты;

- более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);

- пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС), что создает для нарушителя принципиальную возможность их обхода;

- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

ГЛАВА 2. СИСТЕМЫ ПРАВОВОЙ И ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Анализ нормативных документов в области защиты информации

К числу базовых документов по защите информации относится, в первую очередь, Конституция РФ в ст. 23 установлено право на неприкосновенность личной жизни, личной и семейной тайны, тайны телефонных переговоров, почтовых, и иных

сообщений. При этом ограничение этого права допускается только на основании судебного решения. Конституцией РФ не допускается сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

27 июля 2006 года Президент РФ подписал два важнейших для сферы документационного обеспечения управления (делопроизводства) федеральных закона: № 149 - ФЗ «Об информации, информационных технологиях и о защите информации» и № 152-ФЗ «О персональных данных».[12]

10 января 2002 года Президентом был подписан закон «Об электронной цифровой подписи», развивающий и конкретизирующий положения приведенного выше закона № 149.

Основными также являются законы РФ: «О государственной тайне» от 22 июля 2004 г.; «О коммерческой тайне» от 29 июля 2004 (он содержит в себе информацию, составляющую коммерческую тайну, режим коммерческой тайны, разглашение информации, составляющую коммерческую тайну); «Об утверждении Перечня сведений конфиденциального характера»; «Об утверждении Перечня сведений, отнесенных к государственной тайне»; «Об утверждении Перечня сведении, которые не могут составлять коммерческую тайну». Ряд подзаконных правовых нормативных актов, регламентируют организацию защиты государственной тайны, ведение секретного делопроизводства, порядок допуска к государственной тайне должностных лиц и граждан РФ: «Об утверждении положения о лицензировании деятельности по технической защите конфиденциальной информации» и др.

Ряд вопросов, связанных с защитой конфиденциальной информации, регулируется Уголовно-процессуальным кодексом РФ, в нем имеются положения, касающиеся тайны переписки, телефонных и иных переговоров, почтовых отправлений, телефонных и иных сообщений.

Нормы регулирования отношений, возникающих при обращении конфиденциальной информации, содержатся также в Гражданском кодексе РФ. При этом конфиденциальная информация относится в Гражданском кодексе РФ к нематериальным благам.

Критерии, по которым сведения относятся к служебной и коммерческой тайне, содержатся в ст.139 Гражданского кодекса РФ. Она гласит, что информация составляет служебную или коммерческую тайну в случае, когда:

Эта информация имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам.

К этой информации нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Кроме того, определение конфиденциальности коммерческой информации содержится в ст.727 Гражданского кодекса РФ.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс РФ. Он содержит ряд положений, относящихся к защите информации ограниченного доступа и ответственности за ее неправомерное использование.

Особым видом ответственности за нарушение коммерческой тайны является лишение соответствующей аттестации, лицензии уполномоченным органом. Но привлечение к данному виду ответственности в целом не получило к настоящему времени широкое распространение.

Правовые нормы, регулирующие использование конфиденциальной информации в судебных разбирательствах - эти нормы, в частности, установлены в Гражданско-процессуальном кодексе РФ.[13]

Основные требования, предъявляемые к порядку обращения с конфиденциальной информацией в государственных и коммерческих структурах, содержатся также в ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Можно сказать, что законодательные акты РФ не регламентируют в полной мере порядок учета, хранения и использования документов, содержащих конфиденциальную информацию.

Вместе с тем, в некоторых законах содержатся отдельные положения, определяющие общие принципы учета, хранения и использования документов, содержащих конфиденциальные сведения.

2.2. Порядок создания системы технической защиты информации

Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применением (при необходимости) средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

Организация работ по защите информации возлагается на руководителей учреждений и предприятий, руководителей подразделений, осуществляющих разработку проектов объектов информатизации и их эксплуатацию, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации на руководителей подразделений по защите информации (служб безопасности) учреждения (предприятия).

Научно-техническое руководство и непосредственную организацию работ по созданию (модернизации) системы защиты информации (СЗИ) объекта информатизации осуществляет его главный конструктор или другое должностное лицо, обеспечивающее научно-техническое руководство созданием объекта информатизации.

Организация работ по созданию и эксплуатации объектов информатизации и их СЗИ определяется в разрабатываемом на предприятии «Руководстве по защите информации» или в специальном «Положении о порядке организации и проведения работ по защите информации» и должна предусматривать:

- порядок определения защищаемой информации;

- порядок разработки, ввода в действие и эксплуатацию объектов информатизации;

- ответственность должностных лиц за своевременность и качество формирования требований по технической защите информации, за качество и научно-технический уровень разработки СЗИ.

В учреждении (на предприятии) должен быть документально оформлен перечень сведений конфиденциального характера, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа персонала к такого рода сведениям.

Устанавливаются следующие стадии создания системы защиты информации:

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;

- стадия проектирования (разработки проектов) и реализации объекта информатизации, включающая разработку СЗИ в составе объекта информатизации;

- стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

На предпроектной стадии по обследованию объекта информатизации: [14]

- устанавливается необходимость обработки (обсуждения) конфиденциальной информации на данном объекте информатизации;

- определяется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;

- определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;

- определяются условия расположения объектов информатизации относительно границ контролируемой зоны (КЗ);

- определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой автоматизированной системе (АС) и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;

- определяются режимы обработки информации в АС в целом и в отдельных компонентах;

- определяется класс защищенности АС;

- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;

- определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ.

На основе действующих нормативных правовых актов и методических документов по защите конфиденциальной информации, в т.ч. настоящего документа, с учетом установленного класса защищенности АС задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

На стадии проектирования и создания объекта информатизации и СЗИ в его составе на основе предъявляемых требований и заданных заказчиком ограничений на финансовые, материальные, трудовые и временные ресурсы осуществляются:

- разработка раздела технического проекта на объект информатизации в части защиты информации;

- строительно-монтажные работы в соответствии с проектной документацией, размещением и монтажом технических средств и систем;

- разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями;

- закупка сертифицированных образцов и серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации, либо их сертификация;

- закупка сертифицированных технических, программных и программно-технических (в т.ч. криптографических) средств защиты информации и их установка;

- разработка (доработка) или закупка и последующая сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные программные средства;

- организация охраны и физической защиты помещений объекта информатизации, исключающих несанкционированный доступ к техническим средствам обработки, хранения и передачи информации, их хищение и нарушение работоспособности, хищение носителей информации;

- разработка и реализация разрешительной системы доступа пользователей и эксплуатационного персонала к обрабатываемой (обсуждаемой) на объекте информатизации информации;

- определение заказчиком подразделений и лиц, ответственных за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации;

- выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

- разработка эксплуатационной документации на объект информатизации и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

- выполнение других мероприятий, специфичных для конкретных объектов информатизации и направлений защиты информации.

На стадии проектирования и создания объекта информатизации оформляются также технический проект и эксплуатационная документация СЗИ.

На стадии ввода в действие объекта информатизации и СЗИ осуществляются:

- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;

- аттестация объекта информатизации по требованиям безопасности информации.

На этой стадии оформляются:

- акты внедрения средств защиты информации по результатам их испытаний;

- предъявительский акт к проведению аттестационных испытаний;

- заключение по результатам аттестационных испытаний.

С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность технических средств в учреждении (на предприятии), проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

Контроль осуществляется службой безопасности учреждения (предприятия).

При необходимости по решению руководителя предприятия в ЗП и в местах размещения средств обработки информации могут проводиться работы по обнаружению и изъятию «закладок», предназначенных для скрытого перехвата защищаемой информации.

Такие работы могут проводиться организациями, имеющими соответствующие лицензии ФСТЭК России на данный вид деятельности.

ЗАКЛЮЧЕНИЕ

В данной работе были рассмотрены основные аспекты предметной области информационной безопасности, в частности, некоторые виды угроз безопасности и наиболее распространенные методы борьбы с ними.

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

Самым опасным источником дестабилизирующего воздействия на информацию является человек, потому как на защищаемую информацию могут оказывать воздействие различные категории людей.

Разнообразие видов и способов дестабилизирующего воздействия на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

В результате реализации угроз информационной безопасности может быть нанесен серьезный ущерб жизненно важным интересам страны в политической, экономической, оборонной и других сферах деятельности, причинен социально-

экономический ущерб обществу и отдельным гражданам. Исходя из этого, можно сделать вывод, что информационная безопасность – это комплекс мер, среди которых нельзя выделить наиболее важные.

Актуальность вопросов защиты информации возрастает с каждым годом. Многие считают, что данную проблему можно решить чисто техническими мерами – установкой межсетевых экранов и антивирусных программ. Но для построения надежной защиты в первую очередь необходима информация о существующих угрозах и методах противодействия им. Известный принцип “предупрежден, значит вооружен” работает и в сфере компьютерной безопасности: вовремя распознав угрозу можно не допустить неприятного развития событий. Поэтому нужно соблюдать меры защиты во всех точках сети, при любой работе любых субъектов с информацией.

Однако следует понимать, что обеспечить стопроцентную защиту невозможно. С появлением новых технологий будут появляться и новые угрозы.

Современная Доктрина информационной безопасности Российской Федерации наиболее полно раскрывает виды и источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации 12.12.1993г // Российская газета. – 1993.- № 237. – 25 декабря.
2. Гражданский кодекс РФ // Собрание законодательства Российской Федерации. - 2002. - № 46
3. Уголовный кодекс РФ от 13 июня 1996. № 63-ФЗ // СЗ РФ. -1996. -№ 52.
4. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995. № 24-ФЗ // Российская газета. – 1995. - 22 февраля.
5. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. №1-ФЗ // Российская газета. – 2002. - №6. - 12 января.
6. Указ Президента РФ от 3 апреля 1995. №334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» // Российская газета. – 1995. - от 6 апреля. - № 68.

Научная и учебная литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. - М.: Гелиос АРВ, 2011. - 480 с. - ISBN: 5-85438-019-6
2. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2013. - 256 с. - ISBN: 5-279-02606-9
3. Белкин П.Ю., Михальский О.О., Першаков А.С. и др Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 2009. – 248 с. - ISBN: 5-207-13411-1
4. Вишневский А. Сетевые технологии Windows 2000 для профессионалов. - СПб.: Питер, 2010. - 592 с.: ил. ISBN: 5-272-00179-6
5. Камер Д. Сети TCP/IP, том 1. Принципы, протоколы и структура. 4-е издание. - М.: Издательский дом "Вильямс", 2013. - 880 с. - ISBN: 5-8459-0419-6
6. Коженевский С.Р. Технические средства защиты информации. – М.: ДиаСофт, 2013. – 216 с. - ISBN: 9-6679-9220-9
7. Коул Э. Руководство по защите от хакеров. - М.: Издательский дом "Вильямс", 2012. - 640 с. - ISBN: 5-8459-0278-9
8. Кравченко В.А. Защитный комплекс для компьютера. // Журнал Мир ПК. – 2013. – 121 с.
9. Кульгин М. Технологии корпоративных сетей. Энциклопедия. - СПб.: Питер, 2009. - 704 с.: ил. - ISBN: 5-8046-0098-2
10. Никифоров С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей. - М.: Финансы и статистика, 2012. - 224 с. - ISBN: 5-279-02549-6
11. Норткат С., Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях. - М.: Издательский дом "Вильямс", 2011. - 464 с. - ISBN: 5-8459-0225-8
12. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2013. - 248 с.: ил. - ISBN: 5-9556-0002-7
13. Партыка Т.Л., Попов И.И. Информационная безопасность. - М.:"Инфра-М", 2012. - 368 с. - ISBN: 5-16-001155-2
14. Петровский А.И. Хакинг, крэкинг и фрикинг: секреты, описания атак, взлом и защита. - М.: Изд-во "СОЛОН-Пресс", 2011. - 560 с. -ISBN: 5-93455-094-2

ПРИЛОЖЕНИЕ

Угрозы безопасности в КС

Угрозы безопасности информации в КС

Случайные угрозы

Преднамеренные угрозы

Стихийные бедствия и

аварии

Традиционный шпионаж

и диверсии

Сбои и отказы

технических средств

Несанкционированный

доступ к информации

Ошибки при

разработке КС

Электромагнитные

излучения и наводки

Алгоритмические

и программные ошибки

Несанкционированная

модификация структур

Ошибки пользователей и обслуживающего персонала

Вредительские

программы

1. Партыка Т.Л., Попов И.И. Информационная безопасность. - М.:"Инфра-М", 2012. – С. 13 ↑

2. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2013. – С. 98 ↑

3. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2013. – С. 54 ↑

4. Петровский А.И. Хакинг, крэкинг и фрикинг: секреты, описания атак, взлом и защита. - М.: Изд-во "СОЛОН-Пресс", 2011. – С. 65 ↑

5. Петровский А.И. Хакинг, крэкинг и фрикинг: секреты, описания атак, взлом и защита. - М.: Изд-во "СОЛОН-Пресс", 2011. – С. 143 ↑

6. Партыка Т.Л., Попов И.И. Информационная безопасность. - М.:"Инфра-М", 2012. – С. 122 ↑

7. Белкин П.Ю., Михальский О.О., Першаков А.С. и др Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 2009. – С. 45 ↑

8. Камер Д. Сети TCP/IP, том 1. Принципы, протоколы и структура. 4-е издание. - М.: Издательский дом "Вильямс", 2013. – С. 65 ↑

9. Белкин П.Ю., Михальский О.О., Першаков А.С. и др Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 2009. – С. 65 ↑

10. Петровский А.И. Хакинг, крэкинг и фрикинг: секреты, описания атак, взлом и защита. - М.: Изд-во "СОЛОН-Пресс", 2011. – С. 65 ↑

11. Белкин П.Ю., Михальский О.О., Першаков А.С. и др Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 2009. – С. 65 ↑

12. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995. № 24-ФЗ // Российская газета. – 1995. - 22 февраля. ↑

13. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2013. – С. 76 ↑

14. Белкин П.Ю., Михальский О.О., Першаков А.С. и др Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных. - М.: Радио и связь, 2009. – С. 87 ↑