Содержание:

Введение

Актуальность темы исследования. Сегодня широкое использование информационных технологий стало объективной необходимостью. Диапазон областей, в которых используются информационные технологии, чрезвычайно широк. Одной из сфер, где их значение традиционно было здорово с самого начала их быстрого развития, является финансовая сфера. Несмотря на то, что около десяти-пятнадцати лет назад в кредитных учреждениях использовались ручные методы обработки информации, компьютеры, электронные терминалы, средства связи и связи, теперь были практически обязательными атрибутами любого банка.

В компьютерной технике понятие безопасности очень широк. Это подразумевает и надежность компьютера, а также сохранение ценных данных и защиту информации от внесения в нее изменений неавторизованными лицами и сохранение секретности корреспонденции в электронных сообщениях. Разумеется, во всех цивилизованных странах законы защищают безопасность граждан, но в области компьютерных технологий правоприменительная практика еще недостаточно развита, а законодательный процесс не идет в ногу с развитием компьютерных систем, в значительной степени зависит от меры самообороны. [6, 69]

Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. В некоторых случаях пользователи или потребители мер безопасности могут рассматриваться как меры по ограничению доступа и эффективности. Однако такие инструменты, как криптография, могут значительно повысить степень защиты, не ограничивая доступ пользователей к данным.

Объектом исследования является информационная безопасность.

Предметом исследования является защита информации

Цель курсовой работы - рассмотреть типы и состав угроз в информационной безопасности.

Исходя из цели исследования, необходимо решить следующие задачи:

1) Изучение защиты информации

2) Проанализировать механизмы обеспечения безопасности в

3) Изучить типы и состав угроз в информационной безопасности.

Источниками исследования были нормативные правовые акты Российской Федерации, комментарии законодательства, учебная и специальная литература, материалы монографий и публикаций различных авторов, статьи юридических журналов, электронные ресурсы.

В исследовании используется коллатерально-правовой метод, элементы метода анализа и формальный исторический метод.

Курсовая работа состоит из введения, двух глав, заключения, списка использованной литературы.

1. Обеспечение защиты информационной безопасности

1.1 Меры защиты информации

В компьютерных сетях сконцентрирована информация, исключительное право на использование, которой принадлежит определенным лицам или группам лиц, действующих по личной инициативе или в соответствии с должностными обязанностями.

Такая информация должна быть защищена от всех видов посторонних помех: чтение лицами, которые не имеют права доступа к информации и намеренно изменяющей информацию. Кроме того, в ВС должен принять меры для защиты вычислительных ресурсов сети от их несанкционированного использования, то есть исключить доступ к сети лиц, которые не имеют права быть исключенными.

Физическая защита системы и данных может выполняться только в отношении рабочих компьютеров и узлов связи и невозможна для широковещательных носителей большой длины. По этой причине Вооруженные Силы должны использовать средства, которые исключают несанкционированный доступ к

данным и обеспечивают их секретность. [10, 152]

Изучение практики работы систем обработки данных и компьютерных систем показало, что существует множество возможных направлений утечки информации и несанкционированных путей доступа в системах и сетях. Среди них:

• Чтение остаточной информации в системной памяти после выполнения разрешенных запросов;

• копирование медиа и информационных файлов с преодолением мер защиты;

• маскировка для зарегистрированного пользователя;

• маскирование системного запроса;

• использование программных ловушек;

• использование дефектов операционной системы;

• Незаконное подключение к оборудованию и линиям связи;

• вредоносное отключение механизмов защиты;

• Введение и использование компьютерных вирусов.

Обеспечение безопасности информации в Вооруженных Силах и автономно работающих компьютерах достигается комплексом организационных, организационных, технических, технических и программных мер.

Организационные меры по защите информации включают:

• ограничение доступа к помещениям, в которых осуществляется подготовка и обработка информации;

• прием на обработку и передачу конфиденциальной информации только проверенных должностных лиц;

• хранение магнитных носителей и регистрационных журналов в закрытых для доступа к несанкционированным лицам сейфах;

• исключение просмотра аутсайдерами содержимого обработанных материалов через дисплей, принтер и т.д.;

• использование криптографических кодов для передачи ценной информации по каналам связи;

• уничтожение красящих лент, бумаги и других материалов, содержащих фрагменты ценной информации.

Организационные и технические меры по защите информации включают:

• силовое оборудование, которое обрабатывает ценную информацию от независимого источника питания или через специальные сетевые фильтры;

• установка кодовых замков на дверях помещений;

• Используйте для отображения информации при входе и выходе ЖК-дисплея или плазменных дисплеев, а также для получения печатных копий - струйных принтеров и термопринтеров, поскольку на дисплее появляется такое высокочастотное электромагнитное излучение, что изображение с его экрана может быть получено на расстоянии нескольких сто километров;

• уничтожение информации, хранящейся в ПЗУ и на жестком диске, при списании или отправке ПК на ремонт;

• установка клавиатуры и принтеров на мягких прокладках, чтобы уменьшить возможность удаления информации акустическим способом;

• Ограничение электромагнитного излучения экранирующими помещениями, где обрабатывается информация, металлические листы или специальный пластик.

Техническими средствами защиты информации являются системы защиты территорий и помещений путем скрининга компьютерных комнат и организации систем контроля доступа. Защита информации в сетях и вычислительных средствах с помощью технических средств осуществляется на основе доступа к памяти с использованием:

• контролировать доступ к различным уровням памяти компьютера;

• Блокировка данных и ввод ключа; [4, 186]

• распределение контрольных бит для записей для целей идентификации и т. Д.

Архитектура программного обеспечения для защиты информации включает:

• контроль безопасности, включая контроль регистрации входа в систему, фиксацию в системном журнале, контроль действий пользователя;

• ответ (включая звук) на нарушение защиты контроля доступа к сетевым ресурсам;

• контроль мандатов доступа;

• формальный контроль над безопасностью операционных систем (базовая общесистемная и сетевая);

• контроль алгоритмов защиты;

• Проверка и подтверждение правильного функционирования технического и программного обеспечения.

Для надежной защиты информации и обнаружения случаев несанкционированных действий осуществляется регистрация работы системы: создаются специальные дневники и протоколы, в которых регистрируются все действия, связанные с защитой информации в системе. Исправлено время получения приложения, его тип, имя пользователя и терминал, с которого инициализировано приложение.

При выборе событий, которые нужно зарегистрировать, следует иметь в виду, что по мере увеличения количества зарегистрированных событий трудно просмотреть дневник и обнаружить попытки преодоления защиты.

В этом случае вы можете применять анализ программного обеспечения и записывать сомнительные события. Специальные программы также используются для тестирования системы защиты.

Периодически или в случайное время они проверяют работоспособность аппаратного и программного обеспечения.

Отдельная группа мер по обеспечению безопасности информации и идентификации несанкционированных запросов включает программы обнаружения нарушений в режиме реального времени.

Программы этой группы образуют специальный сигнал при регистрации действий, которые могут привести к незаконным действиям в отношении защищенной информации.

Сигнал может содержать информацию о характере нарушения, его местоположении и других характеристиках.

Кроме того, программы могут лишить доступ к защищенной информации или имитировать такой режим работы (например, немедленную загрузку устройств ввода / вывода), которая будет идентифицировать правонарушителя и задержать его соответствующей службой.

Одним из наиболее распространенных способов защиты является явное указание секретности вывода.

В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или принтера любой единицы информации (например, файла, записи и таблицы) сопровождается специальным штампом, указывающим уровень секретности. Это требование реализуется с помощью соответствующего программного обеспечения.

Отдельной группе выделяется защита от несанкционированного использования программного обеспечения. Они приобретают особое значение благодаря широко распространенному ПК.

1.2 Виды угроз информационной безопасности

угроза информационной безопасности воспринимается как потенциально возможные действия, явления или процессы, которые могут иметь нежелательные последствия для системы или информации, хранящейся в ней.

Такие угрозы, влияющие на ресурсы, могут привести к повреждению данных, копированию, несанкционированному распространению, ограничению или блокировке доступа к ним. В настоящее время известно достаточно большое количество угроз, которые классифицируются по различным критериям.

По своей природе различаются естественные, искусственные угрозы.

Первая группа включает те, которые вызваны воздействием на компьютерную систему объективных физических процессов или природных явлений. Вторая группа - те угрозы, которые вызваны деятельностью человека.

По степени интенциональности проявления угрозы разделяются на случайные и преднамеренные.

Существует также разделение в зависимости от их непосредственного источника, который может быть природной средой (например, стихийными бедствиями), лицом (раскрытие конфиденциальных данных), программным и аппаратным обеспечением: авторизованным (ошибка операционной системы) и неавторизованным (вирусная инфекция система).

Источник угроз может иметь разные позиции. В зависимости от этого фактора выделяются также три группы:

- Угрозы, источник которых находится за пределами контролируемой группы компьютерной системы (например, перехват данных, передаваемых по каналам связи)

- Угрозы, источник которых - в пределах контролируемой зоны системы (это может быть кража средств массовой информации)

- Угрозы, которые находятся непосредственно в самой системе (например, неправильное использование ресурсов).

Угрозы могут повлиять на компьютерную систему по-разному. Это могут быть пассивные эффекты, реализация которых не влечет за собой изменения в структуре данных (например, копирование). Активными угрозами являются те, которые, напротив, меняют структуру и содержимое компьютерной системы (введение специальных программ).

В соответствии с разделением угроз по этапам доступа пользователей или программ к системным ресурсам существуют такие опасности, которые появляются при доступе к компьютеру и обнаруживаются после доступа к разрешению (несанкционированное использование ресурсов).

Классификация по местоположению в системе подразумевает разделение на три группы: угрозы доступа к информации, хранящейся на внешних устройствах хранения, в ОЗУ и в том, что распространяется по линиям связи.

Угрозы могут использовать прямой стандартный путь к ресурсам через незаконно полученные пароли или путем злоупотребления терминалами законных пользователей или они могут «обходить» существующие средства защиты по-другому.

Такие действия, как кража информации, классифицируются как угрозы, проявляющиеся независимо от деятельности системы. И, например,

распространение вирусов может быть обнаружено исключительно во время обработки данных.

Случайные или непреднамеренные - это те угрозы, которые не связаны с действиями злоумышленников. Механизм их реализации изучен достаточно хорошо, поэтому разработаны методы противодействия.

Несчастные случаи и стихийные бедствия представляют особую опасность для компьютерных систем, поскольку они влекут за собой самые негативные последствия. Из-за физического разрушения систем информация становится недоступной или теряется. Кроме того, невозможно полностью избежать или предотвратить сбои и сбои в сложных системах, в результате чего, как правило, информация, хранящаяся на них, искажается или разрушается, алгоритм работы технических устройств нарушается.

Ошибки, которые могут быть сделаны при разработке компьютерной системы, включая неправильные алгоритмы работы и неправильное программное обеспечение, могут привести к последствиям, которые аналогичны тем, которые происходят в случае сбоя или сбоя в работе технических средств. Более того, такие ошибки могут использоваться злоумышленниками для воздействия на ресурсы системы.

Ошибки пользователей приводят к ослаблению информационной безопасности в 65% случаев. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками предприятий приводит к разрушению, нарушению целостности и конфиденциальности информации.

Существуют также преднамеренные угрозы, связанные с целенаправленными действиями правонарушителя. Изучение этого класса затруднено, поскольку оно носит очень динамичный характер и постоянно пополняется новыми типами угроз.

Для проникновения в компьютерную систему с целью дальнейшего кражи или уничтожения информации используются методы и средства шпионажа, такие как прослушивание, кража программ, атрибуты безопасности, документы и средства массовой информации, визуальное наблюдение и другие.

Когда несанкционированный доступ к данным обычно используется обычным аппаратным и программным обеспечением компьютерных систем, в результате чего нарушаются установленные правила для дифференциации доступа пользователей или процессов к информационным ресурсам. Наиболее

распространенными нарушениями являются перехват паролей (выполняется со специально разработанными программами), выполнение любых действий под именем другого человека, а также использование злоумышленником привилегий законных пользователей.

Специальные вредоносные программы

- «компьютерные вирусы» - это небольшие программы, которые могут самораспространяться после внедрения в компьютер путем создания собственных копий. При определенных условиях вирусы оказывают негативное влияние на систему;

- «черви» - утилиты, которые активируются каждый раз при загрузке компьютера. Они могут перемещаться внутри системы или сети и умножаться аналогично вирусам. Лавинообразное воспроизведение программ приводит к перегрузке каналов связи, памяти, а затем к блокировке работы;

- «Троянские кони» - такие программы «спрятаны» под видом полезного приложения, но на самом деле повреждают компьютер: уничтожают программное обеспечение, копируют и отправляют файлы злоумышленника с конфиденциальной информацией.

Случайные виды уязвимостей

Эти факторы зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности:

1. Сбои и отказы работы систем:

- вследствие неисправности технических средств на разных уровнях обработки и хранения информации (в том числе и тех, что отвечают за работоспособность системы и за контроль доступа к ней);
- неисправности и устаревания отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы);

- сбои разного программного обеспечения, которое поддерживает все звенья в цепи хранения и обработки информации (антивирусы, прикладные и сервисные программы);
- перебои в работе вспомогательного оборудования информационных систем (неполадки на уровне электропередачи).

2. Ослабляющие информационную безопасность факторы:

- повреждение коммуникаций вроде водоснабжения или электроснабжения, а также вентиляции, канализации;
- неисправности в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация).

Объективные разновидности уязвимостей

Этот вид напрямую зависит от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов, следующими способами:

1. Связанные с техническими средствами излучения:

- электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);
- звуковые варианты (акустические или с добавлением вибросигналов);
- электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

2. Активизируемые:

- вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;
- закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

3. Те, что создаются особенностями объекта, находящегося под защитой:

- расположение объекта (видимость и отсутствие контролируемой зоны вокруг объекта информации, наличие вибро- или звукоотражающих элементов вокруг объекта, наличие удаленных элементов объекта);

- организация каналов обмена информацией (применение радиоканалов, аренда частот или использование всеобщих сетей).

4. Те, что зависят от особенностей элементов-носителей:

- детали, обладающие электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности);
- вещи, подпадающие под влияние электромагнитного поля (носители, микросхемы и другие элементы).

Субъективные уязвимости

Этот подвид в большинстве случаев представляет собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и ПО:

1. Неточности и грубые ошибки, нарушающие информационную безопасность:

- на этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в момент его использования (возможно во время ежедневной эксплуатации, во время ввода данных);
- на этапе управления программами и информационными системами (сложности в процессе обучения работе с системой, настройки сервисов в индивидуальном порядке, во время манипуляций с потоками информации);
- во время пользования технической аппаратурой (на этапе включения или выключения, эксплуатации устройств для передачи или получения информации).

2. Нарушения работы систем в информационном пространстве:

- режима защиты личных данных (проблему создают уволенные работники или действующие сотрудники в нерабочее время, они получают несанкционированный доступ к системе);
- режима сохранности и защищенности (во время получения доступа на объект или к техническим устройствам);
- во время работы с техустройствами (возможны нарушения в энергосбережении или обеспечении техники);

- во время работы с данными (преобразование информации, ее сохранение, поиск и уничтожение данных, устранение брака и неточностей).

Ранжирование уязвимостей

Каждая уязвимость должна быть учтена и оценена специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования. Среди всех критериев выделяют три основных:

- Доступность – это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность. В показатель входят технические данные носителя информации (вроде габаритов аппаратуры, ее сложности и стоимости, а также возможности использования для взлома информационных систем неспециализированных систем и устройств).
- Фатальность – характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем. Если оценивать только объективные уязвимости, то определяется их информативность – способность передать в другое место полезный сигнал с конфиденциальными данными без его деформации.
- Количество – характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.

Каждый показатель обозначается символом (Коп)f, и его можно рассчитать с помощью формулы. Максимальная оценка совокупности уязвимостей – 125, это число и находится в знаменателе. А в числителе фигурирует произведение из K1, K2 и K3.

Чтобы узнать информацию о степени защиты системы точно, нужно привлечь к работе аналитический отдел с экспертами. Они произведут оценку всех уязвимостей и составят информационную карту по пятибалльной системе. Единица соответствует минимальной возможности влияния на защиту информации и ее обход, а пятерка отвечает максимальному уровню влияния и, соответственно, опасности. Результаты всех анализов сводятся в одну таблицу, степень влияния разбивается по классам для удобства подсчета коэффициента уязвимости системы.

Если описывать классификацию угроз, которые обходят защиту информационной безопасности, то можно выделить несколько классов. Понятие классов обязательно, ведь оно упрощает и систематизирует все факторы без исключения. В основу входят такие параметры, как:

1. Ранг преднамеренности совершения вмешательства в информационную систему защиты:

- угроза, которую вызывает небрежность персонала в информационном измерении;
- угроза, инициатором которой являются мошенники, и делают они это с целью личной выгоды.

2. Характеристики появления:

- угроза информационной безопасности, которая провоцируется руками человека и является искусственной;
- природные угрожающие факторы, неподконтрольные информационным системам защиты и вызывающиеся стихийными бедствиями.

3. Классификация непосредственной причины угрозы. Виновником может быть:

- человек, который разглашает конфиденциальную информацию, орудуя с помощью подкупа сотрудников компании;
- природный фактор, приходящий в виде катастрофы или локального бедствия;
- программное обеспечение с применением специализированных аппаратов или внедрение вредоносного кода в техсредства, что нарушает функционирование системы;
- случайное удаление данных, санкционированные программно-аппаратные фонды, отказ в работе операционной системы.

4. Степень активности действия угроз на информационные ресурсы:

- в момент обрабатывания данных в информационном пространстве (действие рассылок от вирусных утилит);
- в момент получения новой информации;
- независимо от активности работы системы хранения информации (в случае вскрытия шифров или криптозащиты информационных данных).

Существует еще одна классификация источников угроз информационной безопасности. Она основана на других параметрах и также учитывается во время

анализа неисправности системы или ее взлома. Во внимание берется следующее:

Состояние источника угрозы:

- в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС;
- в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных;
- мошенничество вне зоны действия АС. Случаи, когда информация захватывается во время прохождения по путям связи, побочный захват с акустических или электромагнитных излучений устройств.

Степень влияния:

- активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов;
- пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.

Возможность доступа сотрудников к системе программ или ресурсов:

- вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного);
- вред наносится после согласия доступа к ресурсам системы.

Способ доступа к основным ресурсам системы. Выделяют следующие угрозы:

- применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы;
- использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя.

Размещение информации, которая хранится в системе:

- вид угроз доступа к информации, которая располагается на внешних устройствах памяти, вроде несанкционированного копирования информации с жесткого диска;

- получение доступа к информации, которая показывается терминалу, например, запись с видеокамер терминалов;
- незаконное проникание в каналы связи и подсоединение к ним с целью получения конфиденциальной информации или для подмены реально существующих фактов под видом зарегистрированного сотрудника. Возможно распространение дезинформации;
- проход к системной области со стороны прикладных программ и считывание всей информации.

При этом не стоит забывать о таких угрозах, как случайные и преднамеренные. Исследования доказали, что в системах данные регулярно подвергаются разным реакциям на всех стадиях цикла обработки и хранения информации, а также во время функционирования системы.

В качестве источника случайных реакций выступают такие факторы, как:

- сбои в работе аппаратуры;
- периодические шумы и фоны в каналах связи из-за воздействия внешних факторов (учитывается пропускная способность канала, полоса пропуска);
- неточности в программном обеспечении;
- ошибки в работе сотрудников или других служащих в системе;
- специфика функционирования среды Ethernet;
- форс-мажоры во время стихийных бедствий или частых отключений электропитания.

Погрешности в функционировании программного обеспечения встречаются чаще всего, а в результате появляется угроза. Все программы разрабатываются людьми, поэтому нельзя устранить человеческий фактор и ошибки. Рабочие станции, маршрутизаторы, серверы построены на работе людей. Чем выше сложность программы, тем больше возможность раскрытия в ней ошибок и обнаружения уязвимостей, которые приводят к угрозам информационной безопасности.

Часть этих ошибок не приводит к нежелательным результатам, например, к отключению работы сервера, несанкционированному использованию ресурсов, неработоспособности системы. Такие платформы, на которых была похищена информация, могут стать площадкой для дальнейших атак и представляют угрозу информационной безопасности.

Чтобы обеспечить безопасность информации в таком случае, требуется воспользоваться обновлениями. Установить их можно с помощью паков,

выпускаемых разработчиками. Установление несанкционированных или нелицензионных программ может только ухудшить ситуацию. Также вероятны проблемы не только на уровне ПО, но и в целом связанные с защитой безопасности информации в сети.

Преднамеренная угроза безопасности информации ассоциируется с неправомерными действиями преступника. В качестве информационного преступника может выступать сотрудник компании, посетитель информационного ресурса, конкуренты или наемные лица. Причин для совершения преступления может быть несколько: денежные мотивы, недовольство работой системы и ее безопасностью, желание самоутвердиться.

Есть возможность смоделировать действия злоумышленника заранее, особенно если знать его цель и мотивы поступков:

- Человек владеет информацией о функционировании системы, ее данных и параметрах.
- Мастерство и знания мошенника позволяют ему действовать на уровне разработчика.
- Преступник способен выбрать самое уязвимое место в системе и свободно проникнуть к информации, стать угрозой для нее.
- Заинтересованным лицом может быть любой человек, как свой сотрудник, так и посторонний злоумышленник.

Например, для работников банков можно выделить такие намеренные угрозы, которые можно реализовать во время деятельности в учреждении:

- Ознакомление сотрудников предприятия с информацией, недоступной для них.
- Личные данные людей, которые не трудятся в данном банке.
- Программные закладки с угрозами в информационную систему.
- Копирование программного обеспечения и данных без предварительного разрешения в личных целях.
- Кража распечатанной информации.
- Воровство электронных носителей информации.
- Умышленное удаление информации с целью скрытия фактов.
- Совершение локальной атаки на информационную систему.
- Отказы от возможного контроля удаленного доступа или отрицание факта получения данных.

- Удаление банковских данных самовольно из архива.
- Несанкционированная коррекция банковских отчетов лицом, не составляющим отчет.
- Изменение сообщений, которые проходят по путям связей.
- Самовольное уничтожение данных, которые повредились вследствие вирусной атаки.

Конкретные примеры нарушения защиты информации и доступа к данным

Несанкционированный доступ – один из самых «популярных» методов компьютерных правонарушений. То есть личность, совершающая несанкционированный доступ к информации человека, нарушает правила, которые зафиксированы политикой безопасности. При таком доступе открыто пользуются погрешностями в системе защиты и проникают к ядру информации. Некорректные настройки и установки методов защиты также увеличивают возможность несанкционированного доступа. Доступ и угроза информационной безопасности совершаются как локальными методами, так и специальными аппаратными установками.

С помощью доступа мошенник может не только проникнуть к информации и скопировать ее, но и внести изменения, удалить данные. Делается это с помощью:

- перехвата косвенных электромагнитных излечений от аппаратуры или ее элементов, от каналов связи, электропитания или сеток заземления;
- технологических панелей регулировки;
- локальных линий доступа к данным (терминалы администраторов системы или сотрудников);
- межсетевых экранов;
- методов обнаружения ошибок.

Из всего разнообразия методов доступа и угроз информации можно условно выделить основные преступления:

- Незаконное пользование привилегиями.
- «Маскарад».
- Перехват паролей.

Перехват паролей – распространенная методика доступа, с которой сталкивалось большинство сотрудников и тех, кто занимается обеспечением информационной безопасности. Это мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы. Затем возможно повторное всплывание окошка авторизации, после чего данные снова попадают в руки перехватчика информации, и так обеспечивается полноценный доступ к системе, возможно внесение собственных изменений. Есть и другие методики перехвата пароля, поэтому стоит пользоваться шифрованием паролей во время передачи, а сделать это можно с помощью специальных программ или RSA.

Способ угрозы информации «Маскарад» во многом является продолжением предыдущей методики. Суть заключается в действиях в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе:

- Передача ложных данных в системе от имени другого человека.
- Попадание в информационную систему под данными другого сотрудника и дальнейшее совершение действий (с предварительным перехватом пароля).

Особенно опасен «Маскарад» в банковских системах, где манипуляции с платежами приводят компанию в убыток, а вина и ответственность накладываются на другого человека. Кроме того, страдают клиенты банка.

Незаконное использование привилегий – название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя. Именно администраторы наделены максимальным списком действий, эти люди и становятся жертвами злоумышленников. При использовании этой тактики происходит продолжение «маскарада», когда сотрудник или третье лицо получает доступ к системе от имени администратора и совершает незаконные манипуляции в обход системы защиты информации.

Но есть нюанс: в этом варианте преступления нужно перехватить список привилегий из системы предварительно. Это может случиться и по вине самого администратора. Для этого требуется найти погрешность в системе защиты и проникнуть в нее несанкционированно.

Угроза информационной безопасности может осуществляться на умышленном уровне во время транспортировки данных. Это актуально для систем

телекоммуникаций и информационных сеток. Умышленное нарушение не стоит путать с санкционированными модификациями информации. Последний вариант выполняется лицами, у которых есть полномочия и обоснованные задачи, требующие внесения изменений. Нарушения приводят к разрыву системы или полному удалению данных.

Существует также угроза информационной безопасности, которая нарушает конфиденциальность данных и их секретность. Все сведения получает третье лицо, то есть посторонний человек без права доступа. Нарушение конфиденциальности информации имеет место всегда при получении несанкционированного доступа к системе.

Угроза защите безопасности информации может нарушить работоспособность компании или отдельного сотрудника. Это ситуации, в которых блокируется доступ к информации или ресурсам ее получения. Один сотрудник создает намеренно или случайно блокирующую ситуацию, а второй в это время натыкается на блокировку и получает отказ в обслуживании. Например, сбой возможен во время коммутации каналов или пакетов, а также угроза возникает в момент передачи информации по спутниковым системам. Их относят к первичным или непосредственным вариантам, поскольку создание ведет к прямому воздействию на данные, находящиеся под защитой.

Выделяют такие разновидности основных угроз безопасности информации в локальных размерах:

- Компьютерные вирусы, нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в основном они действуют локально.
- «Черви» – модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи.
- «Троянские кони» – программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию.

Даже защитная система компьютера представляет собой ряд угроз защите безопасности. Поэтому программистам необходимо учитывать угрозу осмотра параметров системы защиты. Иногда угрозой могут стать и безобидные сетевые адаптеры. Важно предварительно установить параметры системы защиты, ее характеристики и предусмотреть возможные пути обхода. После тщательного анализа можно понять, какие системы требуют наибольшей степени защищенности (акцент на уязвимостях).

Раскрытие параметров системы защиты относят к непрямым угрозам безопасности. Дело в том, что раскрытие параметров не даст реализовать мошеннику свой план и скопировать информацию, внести в нее изменения. Злоумышленник только поймет, по какому принципу нужно действовать и как реализовать прямую угрозу защиты безопасности информации.

2. Требования к современным средствам защиты информации

2.1 Обеспечение безопасности средств защиты информации

В соответствии с требованиями Государственного комитета Российской Федерации средства защиты информации от несанкционированного доступа (SIS NID), отвечающие высоким уровням защиты, должны обеспечивать:

• дискреционный и обязательный принцип контроля доступа;

• Очистка памяти;

• изоляция модулей;

• маркировка документов;

• Защита ввода и вывода на отчуждаемые физические носители;

• Пользовательский сопоставление с устройством;

• Идентификация и аутентификация;

• гарантий проектирования;

• постановка на учет;

• взаимодействие пользователя с комплексом средств защиты;

• надежное восстановление;

• целостность комплекса защитного оборудования;

• контроль модификации;

• контроль распределения;

• гарантии архитектуры;

Комплексные СДГ НРД должны сопровождаться пакетом следующих документов:

• руководство по ГИС;

• гид пользователя;

• тестовая документация;

• проектная (проектная) документация.

Таким образом, в соответствии с требованиями Государственного комитета Российской Федерации интегрированные СДР должны включать базовый набор подсистем. Специфические возможности этих подсистем в реализации функций защиты информации определяют уровень защиты вычислительного оборудования. Реальная эффективность ГИС NDD определяется функциональностью не только основных, но и дополнительных подсистем, а также качества их реализации. [8, 196]

Компьютерные системы и сети подвержены широкому спектру потенциальных информационных угроз, что требует предоставления большого списка функций и подсистем защиты. В первую очередь рекомендуется защитить наиболее информативные каналы утечки информации, которые являются следующими:

• Возможность копирования данных с компьютерных носителей;

• Каналы передачи данных;

• кража компьютеров или встроенных дисков.

Проблема перекрытия этих каналов осложняется тем, что процедуры защиты данных не должны приводить к значительному снижению производительности

вычислительных систем. Эта задача может быть эффективно решена на основе технологии глобального шифрования информации, рассмотренной в предыдущем разделе.

Современная система массовой защиты должна быть эргономичной и иметь такие свойства, которые благоприятствуют ее широкому применению, например:

• Комплексное - возможность устанавливать различные способы безопасной обработки данных с учетом конкретных требований различных пользователей и предоставлять широкий спектр возможных действий предполагаемого нарушителя;

• совместимость - система должна быть совместима со всеми программами, написанными для этой операционной системы, и должна обеспечивать защищенный режим работы компьютера в компьютерной сети;

• переносимость - возможность установки системы на различные типы компьютерных систем, в том числе переносных;

• простота использования - система должна быть проста в использовании и не должна изменять привычную технологию пользователей;

• работа в режиме реального времени - процессы преобразования информации, включая шифрование, должны выполняться с высокой скоростью;

• высокий уровень защиты информации;

• Минимальная стоимость системы.

2.2 Проблемы защиты информации в компьютерных системах

Широкое использование компьютерных технологий в автоматизированных системах обработки и управления информацией усугубило проблему защиты информации, распространяющейся в компьютерных системах от несанкционированного доступа. Защита информации в компьютерных системах имеет ряд специфических особенностей, связанных с тем, что информация не жестко связана со средой, ее можно легко и быстро копировать и передавать по каналам связи. Известно очень много угроз информации, которые могут быть реализованы как наружу нарушителями, так и внутренними нарушителями.

Радикальное решение проблем защиты электронной информации может быть получено только на основе использования криптографических методов, позволяющих решать наиболее важные проблемы безопасной автоматизированной обработки и передачи данных. В то же время современные высокоскоростные методы криптографических преобразований позволяют сохранить начальную производительность автоматизированных систем. Криптографические преобразования данных являются наиболее эффективным средством обеспечения конфиденциальности данных, целостности и аутентичности. Только их использование в сочетании с необходимыми техническими и организационными мерами может обеспечить защиту от широкого спектра потенциальных угроз.

Проблемы, связанные с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

• перехват информации - целостность информации сохраняется, но ее конфиденциальность нарушается;

• изменение информации - исходное сообщение изменяется или полностью заменяется другим и отправляется адресату;

• замещение авторства информации. Эта проблема может иметь серьезные последствия. Например, кто-то может отправить письмо от вашего имени (этот тип обмана называется спуфинг), или веб-сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не отправлять какие-либо товары. [3, 46]

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронной информации, одним из которых является аутентификация электронной информации в условиях, когда стороны, обменивающиеся информацией, не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи. Теоретической основой для решения этой проблемы было открытие в середине 1970-х годов двухкритериальной криптографии американских исследователей Диффи и Хемимана, что стало блестящим достижением многовекового эволюционного развития криптографии. Революционные идеи двузначной криптографии привели к резкому увеличению числа открытых исследований в области криптографии и показали новые способы разработки криптографии, ее новых возможностей и уникального значения ее методов в современных условиях массового использования электронные информационные технологии.

Технической основой для перехода к информационному обществу являются современные микроэлектронные технологии, которые обеспечивают непрерывный рост качества вычислительной техники и служат основой для сохранения основных тенденций его развития - миниатюризации, снижения энергопотребления, увеличения объема ОЗУ (память) и емкость встроенных и съемных приводов, а также надежность, расширение сфер и масштабов применения. Эти тенденции в развитии компьютерных технологий привели к тому, что на современном этапе защита компьютерных систем от несанкционированного доступа характеризуется увеличением роли программного обеспечения и механизмов криптографической защиты по сравнению с аппаратными.

Возрастающая роль программных и криптографических инструментов зашита в том, что возникающие новые проблемы в области защиты компьютерных систем от несанкционированного доступа требуют использования механизмов и протоколов с относительно высокой вычислительной сложностью и могут быть эффективно решены с использованием компьютерных ресурсов.

Одной из важных социальных и этических проблем, вызванных все более широким использованием методов защиты криптографической информации, является противоречие между желанием пользователей защищать свою информацию и передачу сообщений и желанием специальных государственных служб иметь доступ к информации от некоторых других организаций и отдельных лиц в целях пресечения незаконной деятельности. В развитых странах существует широкий круг мнений относительно подходов к проблеме регулирования использования алгоритмов шифрования.

Предложения высказываются против полного запрета широкого применения криптографических методов на полную свободу их использования. Некоторые предложения касаются использования только ослабленных алгоритмов или установления порядка обязательной регистрации ключей шифрования. Крайне сложно найти наилучшее решение этой проблемы. Как оценить соотношение потерь законопослушных граждан и организаций от незаконного использования их информации и государственных потерь из-за невозможности получить доступ к зашифрованной информации определенных групп, скрывающих их незаконную деятельность? Как можно гарантировать предотвращение незаконного использования криптоалгоритмов лицами, нарушающими другие законы? Кроме того, всегда есть способы скрытого хранения и передачи информации. Эти проблемы еще предстоит решить социологам, психологам, юристам и политикам.

Появление глобальных информационных сетей, таких как ИНТЕРНЕТ, является важным достижением компьютерных технологий, однако с Интернетом связано много компьютерных преступлений.

Результатом опыта использования сети INTERNET является выявленная слабость традиционных механизмов защиты информации и отставание в применении современных методов. Криптография обеспечивает возможность обеспечения безопасности информации в INTERNET и в настоящее время активно работает над внедрением необходимых криптографических механизмов в этой сети. Не отказ от прогресса в информатизации, но использование современных достижений в криптографии является стратегически правильным решением. Широкое использование глобальных информационных сетей и криптография - это достижение и признак демократического общества. [1, 37]

Владение основами криптографии в информационном обществе не может объективно быть привилегией определенных государственных служб, но является насущной необходимостью для широких слоев научно-технических работников, которые применяют компьютерную обработку данных или разрабатывают информационные системы, службы безопасности и менеджеров организаций и предприятий. Только это может послужить основой для эффективной реализации и использования средств информационной безопасности.

Одна конкретная организация не может обеспечить достаточно полный и эффективный контроль над информационными потоками во всем государстве и обеспечить надлежащую защиту национального информационного ресурса. Однако некоторые государственные органы могут создавать условия для формирования рынка для оборудования защиты качества, обучать достаточное количество специалистов и осваивать основы криптографии и защищать информацию от массовых пользователей.

В России и других странах СНГ в начале 1990-х годов явно наблюдалась тенденция опережать расширение масштабов и объема информационных технологий в развитии систем защиты данных. Эта ситуация в определенной степени была и характерна для развитых капиталистических стран. Это естественно: сначала должна возникнуть практическая проблема, а затем решения будут найдены. Начало перестройки в ситуации сильного отставания в странах СНГ в области информатизации в конце 1980-х годов создало благодатную почву для резкого преодоления существующего разрыва.

Примером развитых стран, возможностью приобретения системного программного обеспечения и компьютерной техники являются внутренние пользователи. Включение массового потребителя, заинтересованного в быстрой обработке данных и других преимуществах современных информационно-вычислительных систем в решении проблемы компьютеризации, привело к очень высоким темпам развития этой области в России и других странах СНГ. Однако естественная совместная разработка средств автоматизации для обработки информации и защиты информации в значительной степени была нарушена, что привело к массовым компьютерным преступлениям. Не секрет, что компьютерные преступления в настоящее время являются одной из самых насущных проблем.

Использование систем защиты иностранного производства не может устранить эту предвзятость, поскольку продукция такого типа, поступающая на российский рынок, не соответствует требованиям из-за существующих экспортных ограничений, принятых в США, основным производителем средств защиты информации. Еще одним аспектом первостепенной важности является то, что продукты такого типа должны пройти установленную процедуру сертификации в уполномоченных организациях для такой работы.

Сертификаты иностранных фирм и организаций не могут заменить отечественные. Сам факт использования зарубежной системы и прикладного программного обеспечения создает потенциальную угрозу для информационных ресурсов. Использование иностранных средств защиты без надлежащего анализа соблюдения выполняемых функций и уровня предоставляемой защиты может значительно усложнить ситуацию.

Форсирование процесса информатизации требует адекватного предоставления потребителям средств защиты. Отсутствие достаточных средств защиты информации, циркулирующей в компьютерных системах на внутреннем рынке, в течение значительного времени препятствовало осуществлению мер защиты данных в необходимом масштабе. Ситуация усугублялась отсутствием достаточного числа специалистов в области защиты информации, поскольку последние, как правило, были подготовлены только для специальных организаций. Реструктуризация последнего, связанная с изменениями, происходящими в России, привела к созданию независимых организаций, специализирующихся в области защиты информации, которые поглотили освобожденный персонал, и, как результат, возникновение духа конкуренции, который привел к появление достаточно большого количества сертифицированных средств защиты для отечественных разработчиков.

Одной из важных особенностей массового использования информационных технологий является то, что для эффективного решения проблемы защиты государственного информационного ресурса необходимо распространять меры защиты данных среди массовых пользователей. Информация должна быть защищена в первую очередь там, где она создается, собирается и обрабатывается теми организациями, на которые непосредственно влияет несанкционированный доступ к данным. Этот принцип является рациональным и эффективным: защита интересов отдельных организаций является составной частью реализации защиты интересов государства в целом.

Заключение

После массового использования современных информационных технологий криптография вторгается в жизнь современного человека. Использование электронных платежей основано на криптографических методах, возможности передачи конфиденциальной информации по открытым сетям связи, а также решении большого числа других проблем защиты информации в компьютерных системах и информационных сетях. Требования к практике привели к необходимости массового применения криптографических методов и, следовательно, необходимости расширения открытых исследований и разработок в этой области. Владение основами криптографии становится важным для ученых и инженеров, специализирующихся на разработке современных средств защиты информации, а также в сферах эксплуатации и проектирования информационных и телекоммуникационных систем.

Одной из актуальных проблем современной прикладной криптографии является разработка высокоскоростных программных шифров блочного типа, а также высокоскоростных устройств шифрования.

В настоящее время предлагается ряд методов шифрования, защищенных патентами Российской Федерации и основанных на идеях использования:

• Гибкий график выборки соединений;

• Создание алгоритма шифрования для секретного ключа;

• замены, которые зависят от преобразованных данных.

Список литературы

1. Абросимов А.Г., Бородинова М.А, Учебный методический комплекс по курсу «теория экономических информационных систем».2015.-140с.
2. Арский Ю.М., Гиляревский Р.С., Егоров В.С. Информационный рынок в России/.–М.: 2016 -293 с.
3. Багриновский К.А., Хрусталев Е.Ю. Новые информационные технологии. – 2015.- 314 с.
4. Баранов А. П., Борисенко Н. П., Зегжда П. Д., Корт С. С., Ростовцев А. Г. Математические основы информационной безопасности. Орел, 1997).
5. Бармен С. Разработка правил информационной безопасности: пер. с англ. М.: Издательский дом «Вильямс», 2016.-208 с.
6. Бугаенко Д. Рынок финансовой информатизации: состояние и перспективы – 2015. - 263 с.
7. В.А. Галатенко. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
8. Волков Е.А. Экономическая эффективность автоматизированного управления. – М: 2016. – 147 с.
9. Гайкович В., Першин А. Безопасность электронных банковских систем. М., 2017 -. 370 с.
10. Емяков А.Д. К понятию информация/социол.исслед.-2016.-№4.-с.144-146
11. Корт С. С., Боковенко И. Н. Язык описания политик безопасности. Проблемы информационной безопасности // Компьютерные системы. 2014. № 1. С. 17—25
12. Костюк В.Н. Информация как социальный и экономический ресурс. -М: 2015.-348с.
13. Левин, В. К. Защита информации в информационно-вычислительных системах и сетях /В. К. Левин// Программирование. - 2014. - N5. - С. 5-16.
14. Пещанская А. Проблемы развития информационного общества. 2016. – 126 с.
15. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. — М.: ДМК Пресс, 2016 —227 с.
16. Теория и практика информационной безопасности / под ред. П. Д. Зегжды. М.: Яхтсмен, 2017. - 192 с.