Федеральное агентство по образованию

Государственное образовательное учреждение

Высшего профессионального образования

Тульский государственный университет

Кафедра технологии полиграфического производства

и защиты информации

**Контрольно-курсовая работа по дисциплине**

**"История и современная система защиты информации в России"**

***Каналы и методы несанкционированного доступа к информации.***

Выполнил: студент гр.632281

Корнев П.Г.

Приняла: ассистент

Пальчун Е.Н.

Тула 2010

Оглавление

Введение

1. Несанкционированный доступ к информации

2. Электромагнитные излучения и наводки

3. Несанкционированная модификация структур

4. Вредительские программы

5. Классификация злоумышленников

6. Традиционный шпионаж и диверсии

Заключение

Список литературы

## Введение

Информационные технологии во всех сферах общественной жизни бурно развиваются. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника и защиты своих информационных ресурсов.

Значимость обеспечения безопасности государства в информационной сфере подчеркнута в принятой в сентябре 2000 года "Доктрине информационной безопасности Российской Федерации": "Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, в ходе технического прогресса эта зависимость будет возрастать".

Остроту межгосударственного информационного противоборства можно наблюдать в оборонной сфере, высшей формой которой являются информационные войны. Не менее остро стоит вопрос информационного противоборства и на уровне организаций, отдельных граждан. Об этом свидетельствуют многочисленные попытки злоумышленников получить контроль над компьютерными технологиями и информацией для извлечения материальной выгоды.

Противоборство государств в области информационных технологий, стремление злоумышленников противоправно использовать информационные ресурсы, необходимость обеспечения прав граждан в информационной сфере, наличие множества случайных угроз вызывают острую необходимость обеспечения защиты информации в компьютерных системах, являющихся материальной основой информатизации общества.

В данной работе я хотел бы осветить основные каналы несанкционированного доступа и утечки информации, а также совершенствование методов и средств несанкционированного получения информации.

## 1. Несанкционированный доступ к информации

Термин "несанкционированный доступ к информации" (НСДИ) определен как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств вычислительной техники или автоматизированных систем.

Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Право доступа к ресурсам компьютерных систем определяется руководством для каждого сотрудника в соответствии с его функциональными обязанностями. Процессы инициируются в компьютерных системах в интересах определенных лиц, поэтому и на них накладываются ограничения по доступу к ресурсам.

Выполнение установленных правил разграничения доступа в компьютерных системах реализуется за счет создания системы разграничения доступа.

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

отсутствует система разграничения доступа;

сбой или отказ в компьютерных системах;

ошибочные действия пользователей или обслуживающего персонала компьютерных систем;

ошибки в системе разграничения доступа;

фальсификация полномочий.

Если система разграничения доступа отсутствует, то злоумышленник, имеющий навыки работы в компьютерных системах, может получить без ограничений доступ к любой информации. В результате сбоев или отказов средств компьютерных систем, а также ошибочных действий обслуживающего персонала и пользователей возможны состояния системы, при которых упрощается НСДИ. Злоумышленник может выявить ошибки в системе разграничения доступа и использовать их для НСДИ. Фальсификация полномочий является одним из наиболее вероятных путей (каналов) НСДИ.

## 

## 2. Электромагнитные излучения и наводки

Процесс обработки и передачи информации техническими средствами компьютерных систем сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках, Они получили названия побочных электромагнитных излучений и наводок (ПЭМИН). С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Наибольший уровень электромагнитного излучения в компьютерных системах присущ работающим устройствам отображения информации на электронно-лучевых трубках. Содержание экрана такого устройства может просматриваться с помощью обычного телевизионного приемника, дополненного несложной схемой, основной функцией которой является синхронизация сигналов. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 метров. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 метров.

Наведенные в проводниках электрические сигналы могут выделяться и фиксироваться с помощью оборудования, подключаемого к этим проводникам на расстоянии в сотни метров от источника сигналов. Для добывания информации злоумышленник может использовать также "просачивание" информационных сигналов в цепи электропитания технических средств компьютерных систем.

"Просачивание" информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором выпрямительного устройства. "Просачивание" также возможно за счет падения напряжения на внутреннем сопротивлении источника питания при прохождении токов усиливаемых информационных сигналов. Если затухание в фильтре выпрямительного устройства недостаточно, то информационные сигналы могут быть обнаружены в цепи питания. Информационный сигнал может быть выделен в цепи питания за счет зависимости значений потребляемого тока в оконечных каскадах усилителей (информационные сигналы) и значений токов в выпрямителях, а значит и в выходных цепях.

Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения. Электромагнитные импульсы способны уничтожить информацию на магнитных носителях. Мощные электромагнитные и сверхвысокочастотные излучения могут вывести из строя электронные блоки компьютерных систем. Причем для уничтожения информации на магнитных носителях с расстояния нескольких десятков метров может быть использовано устройство, помещающееся в портфель.

## 3. Несанкционированная модификация структур

Большую угрозу безопасности информации в компьютерных системах представляет несанкционированная модификация алгоритмической, программной и технической структур системы. Несанкционированная модификация структур может осуществляться на любом жизненном цикле компьютерных систем. Несанкционированное изменение структуры компьютерных систем на этапах разработки и модернизации получило название "закладка". В процессе разработки компьютерных систем "закладки" внедряются, как правило, в специализированные системы, предназначенные для эксплуатации в какой-либо фирме или государственных учреждениях. В универсальные компьютерные системы "закладки" внедряются реже, в основном для дискредитации таких систем конкурентом или на государственном уровне, если предполагаются поставки компьютерных систем во враждебное государство. "Закладки", внедренные на этапе разработки, сложно выявить ввиду высокой квалификации их авторов и сложности современных компьютерных систем.

Алгоритмические, программные и аппаратные "закладки" используются либо для непосредственного вредительского воздействия на компьютерные системы, либо для обеспечения неконтролируемого входа в систему.

Вредительские воздействия "закладок" на компьютерные системы осуществляются при получении соответствующей команды извне (в основном характерно для аппаратных "закладок") и при наступлении определенных событий в системе.

Такими событиями могут быть: переход на определенный режим работы (например, боевой режим системы управления, оружием или режим устранения аварийной ситуации на атомной электростанции т.п.), наступление установленной даты, достижение определенной наработки и т.д.

Программные и аппаратные "закладки" для осуществления неконтролируемого входа в программы, использование привилегированных режимов работы (например, режимов операционной системы), обхода средств защиты информации получили название "люки".

## 4. Вредительские программы

Одним из основных источников угроз безопасности информации в компьютерных системах является использование специальных программ, получивших общее название "вредительские программы".

В зависимости от механизма действия вредительские программы делятся на четыре класса:

"логические бомбы";

"черви";

"троянские кони";

"компьютерные вирусы".

"Логические бомбы" - это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход компьютерной системы в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

"Червями" называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

"Троянские кони" - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

"Компьютерные вирусы" - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на компьютерные системы.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

## 5. Классификация злоумышленников

Возможности осуществления вредительских воздействий в большой степени зависят от статуса злоумышленника по отношению к компьютерным системам. Злоумышленником может быть:

разработчик компьютерных систем;

сотрудник из числа обслуживающего персонала;

пользователь;

постороннее лицо.

*Разработчик* владеет наиболее полной информацией о программных и аппаратных средствах компьютерных систем и имеет возможность внедрения "закладок" на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты компьютерных систем.

*Пользователь* имеет общее представление о структурах компьютерных систем, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения "закладок" пользователями очень ограничены.

*Постороннее лицо*, не имеющее отношения к компьютерным системам, находится в наименее выгодном положении по отношению к другим злоумышленникам. Если предположить, что он не имеет доступ на объект компьютерных систем, то в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности. Он может осуществлять вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если компьютерная система является распределенной.

Большие возможности оказания вредительских воздействий на информацию компьютерных систем имеют *специалисты, обслуживающие эти системы*. Причем, специалисты разных подразделений обладают различными потенциальными возможностями злоумышленных действий. Наибольший вред могут нанести работники службы безопасности информации. Далее идут системные программисты, прикладные программисты и инженерно-технический персонал.

На практике опасность злоумышленника зависит также от финансовых, материально-технических возможностей и квалификации злоумышленника.

## 6. Традиционный шпионаж и диверсии

В качестве источников нежелательного воздействия на информационные ресурсы по-прежнему актуальны методы и средства шпионажа и диверсий, которые использовались и используются для добывания или уничтожения информации на объектах, не имеющих компьютерных систем. Эти методы также действенны и эффективны в условиях применения компьютерных систем. Чаще всего они используются для получения сведений о системе защиты с целью проникновения в компьютерные системы, а также для хищения и уничтожения информационных ресурсов.

К методам шпионажа и диверсий относятся:

подслушивание;

визуальное наблюдение;

хищение документов и машинных носителей информации;

хищение программ и атрибутов системы защиты;

подкуп и шантаж сотрудников;

сбор и анализ отходов машинных носителей информации;

поджоги;

взрывы.

Для подслушивания злоумышленнику не обязательно проникать на объект. Современные средства позволяют подслушивать разговоры с расстояния нескольких сотен метров. Так прошла испытания система подслушивания, позволяющая с расстояния 1 км фиксировать разговор в помещении с закрытыми окнами. В городских условиях дальность действия устройства сокращается до сотен и десятков метров в зависимости от уровня фонового шума. Принцип действия таких устройств основан на анализе отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн. Колебания оконных стекол от акустических волн в помещении могут сниматься и передаваться на расстояния с помощью специальных устройств, укрепленных на оконном стекле. Такие устройства преобразуют механические колебания стекол в электрический сигнал с последующей передачей его по радиоканалу. Вне помещений подслушивание ведется с помощью сверхчувствительных направленных микрофонов. Реальное расстояние подслушивания с помощью направленных микрофонов составляет 50-100 метров.

Разговоры в соседних помещениях, за стенами зданий могут контролироваться с помощью стетоскопных микрофонов. Стетоскопы преобразуют акустические колебания в электрические. Такие микрофоны позволяют прослушивать разговоры при толщине стен до 50-100 см. Съем информации может осуществляться также и со стекол, металлоконструкций зданий, труб водоснабжения и отопления.

Аудиоинформация может быть получена также путем высокочастотного навязывания. Суть этого метода заключается в воздействии высокочастотным электромагнитным полем или электрическими сигналами на элементы, способные модулировать эти поля, или сигналы электрическими или акустическими сигналами с речевой информацией. В качестве таких элементов могут использоваться различные полости с электропроводной поверхностью, представляющей собой высокочастотный контур с распределенными параметрами, которые меняются под действием акустических волн. При совпадении частоты такого контура с частотой высокочастотного навязывания и при наличии воздействия акустических волн на поверхность полости контур переизлучает и модулирует внешнее поле (высокочастотный электрический сигнал). Чаще всего этот метод прослушивания реализуется с помощью телефонной линии. При этом в качестве модулирующего элемента используется телефонный аппарат, на который по телефонным проводам подается высокочастотный электрический сигнал. Нелинейные элементы телефонного аппарата под воздействием речевого сигнала модулируют высокочастотный сигнал. Модулированный высокочастотный сигнал может быть демодулирован в приемнике злоумышленника. .

Одним из возможных каналов утечки звуковой информации может быть прослушивание переговоров, ведущихся с помощью средств связи. Контролироваться могут как проводные каналы связи, так и радиоканалы. Прослушивание переговоров по проводным и радиоканалам не требует дорогостоящего оборудования и высокой квалификации злоумышленника.

Дистанционная видеоразведка для получения информации в компьютерных системах малопригодна и носит, как правило, вспомогательный характер.

Видеоразведка организуется в основном для выявления режимов работы и расположения механизмов защиты информации. Из компьютерных систем информация реально может быть получена при использовании на объекте экранов, табло, плакатов, если имеются прозрачные окна и перечисленные выше средства размещены без учета необходимости противодействовать такой угрозе.

Видеоразведка может вестись с использованием технических средств, таких как оптические приборы, фото-, кино - и телеаппаратура. Многие из этих средств допускают консервацию (запоминание) видеоинформации, а также передачу ее на определенные расстояния.

В прессе появились сообщения о создании в США мобильного микроробота для ведения дистанционной разведки. Пьезокерамический робот размером около 7 см и массой 60 г способен самостоятельно передвигаться со скоростью 30 см/с в течение 45 мин. За это время "микроразведчик" способен преодолеть расстояние в 810 метров, осуществляя транспортировку 28 г полезного груза (для сравнения - коммерческая микровидеокамера весит 15 г).

Для вербовки сотрудников и физического уничтожения объектов компьютерных систем также не обязательно иметь непосредственный доступ на объект. Злоумышленник, имеющий доступ на объект компьютерных систем, может использовать любой из методов традиционного шпионажа.

Злоумышленниками, имеющими доступ на объект, могут использоваться миниатюрные средства фотографирования, видео - к аудиозаписи. Для аудио - и видеоконтроля помещений и при отсутствии в них злоумышленника могут использоваться закладные устройства или "жучки". Для объектов компьютерных систем наиболее вероятными являются закладные устройства, обеспечивающие прослушивание помещения. Закладные устройства делятся на проводные и излучающие. Проводные закладные устройства требуют значительного времени на установку и имеют существенный демаскирующий признак - провода. Излучающие "закладки" ("радиозакладки") быстро устанавливаются, но также имеют демаскирующий признак - излучение в радио или оптическом диапазоне. "Радиозакладки" могут использовать в качестве источника электрические сигналы или акустические сигналы. Примером использования электрических сигналов в качестве источника является применение сигналов внутренней телефонной, громкоговорящей связи. Наибольшее распространение получили акустические "радиозакладки". Они воспринимают акустический сигнал, преобразуют его в электрический и передают в виде радиосигнала на дальность до 8 км. Из применяемых на практике "радиозакладок" подавляющее большинство (около 90%) рассчитаны на работу в диапазоне расстояний 50 - 800 метров.

## Заключение

Таким образом, информация в современном мире является неотъемлемой частью жизнедеятельности человека, она окружает нас везде и всюду. Порой значимость какой-либо информации достигает национальных масштабов, тем самым остро ставя вопрос её защиты от утечки или уничтожения.

Защита информации должна иметь комплексный характер и не ограничиваться каким-либо одним из видов, то есть необходимо не только защищать саму информацию или её носитель, но и регламентировать круг лиц, способных иметь доступ к информации, а также уровни доступа к защищаемой информации. Тем самым, только после проведения полномасштабного комплекса мер по защите, уже с большей уверенностью можно будет говорить, что информация защищена, и ей ничто не угрожает.

## Список литературы

1. Диева С.А. Организация и современные методы защиты информации/ С.А. Диева - М.: Концерн "Банковский деловой центр", 1998. - 472с.

2. Куприянов А.И. Основы защиты информации: учеб. Пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов - М.: Издательский центр "Академия", 2006. - 256 с.

3. Стрельцов А.А. Обеспечение информационной безопасности России/ Под ред.В.А. Садовничего и В.П. Шерстюка - М.: МЦНМО, 2002. - 296с.

4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа/ А.Ю. Щеглов - М.: Наука и техника, 2004. - 384с.