**ЛЕКЦИЯ: Каналы утечки информации**

1. **Понятие каналов утечки информации.**

Современные информационные технологии разделили судьбу всех про­грессивных технологий XX в. Бесспорно, что широкое внедрение средств компьютерной техники (СКТ) и телекоммуникаций в производственную, хозяйственную, финансовую деятельность предприятий, учреждений, орга­низаций значительно повышает эффективность их работы. Рубеж тысяче­летий знаменуется все большим проникновением СКТ в повседневную жизнь людей, вовлечением их в глобальную сеть Internet . Так, например, по оценкам зарубежных специалистов, темп роста пользователей Internet составляет порядка 15 % в месяц. Обратной стороной глобальной информатизации явилось появление компьютерной преступности.

На локальном уровне угроз компьютерной безопасности (например, для помещений, занимаемых учреждением, организацией, предприятием, и раз­мещенных в них СКТ) выделяют каналы утечки информации, под которы­ми понимают совокупность источников информации, материальных носи­телей или среды распространения несущих эту информацию сигналов и средств выделения информации из сигналов или носителей.

Факторы информационных угроз следует рассматривать как потенци­альную возможность использования каналов утечки информации. Объек­тивное существование данных каналов утечки предполагает их возможное использование злоумышленниками для несанкционированного доступа к информации, ее модификации, блокированию и иных неправомерных мани­пуляций, т. е. наличие каналов утечки информации влияет на избрание спо­соба совершения преступления.

В рамках данного учебного пособия каналы утечки информации целесо­образно условно классифицировать на традиционные каналы утечки ин­формации (каналы утечки информации в широком смысле) и каналы утечки информации непосредственно из СКТ (каналы утечки в узком смысле). Наличие первых предопределяет широкое использование их с применением специальных технических средств для проведения различных разведывательных мероприятий. Они известны задолго до появления современных средств вычислительной техники (см. рис.1).

Рис.1

|  |
| --- |
| *Локальные факторы угроз информационной безопасности* |

*Каналы утечки информации и технические устройства несанкционированного доступа*

*Каналы утечки информации в широком смысле*

*Каналы утечки информации в узком смысле*

Каналы утечки информации непосредственного из СКТ и технические устройства съема такой информации стали использоваться злоумышленниками сравнительно недавно.

Для получения информации из обозначенных выше традиционных каналов утечки применяются специализированные технические средства ведения разведки (ТСВР), среди которых выделяют следующие основные группы:

1. радиомикрофоны и микрофоны;
2. оптические системы;

■устройства перехвата телефонных сообщений;

1. видеосистемы записи и наблюдения;
2. системы определения местоположения контролируемого объекта;
3. системы контроля и воздействия на компьютеры и их сети.
4. устройства приема, записи, управления.

**Традиционные каналы утечки информации.**

Традиционные каналы утечки информации приведены на рисунке 2.

Рис. 2

|  |  |
| --- | --- |
|   Традиционные каналы утечки аудио- и видеоинформации | Контактное или бесконтактное подключение к электронным устройствам. Встроенные микрофоны, видео- и радиозакладки в стенах, мебели предметах. |
| Съем акустической информации при помощи лазерных устройств с отражающих поверхностей. |
| Оптический дистанционный съем видеоинформации. |
| Применение узконаправленных микрофонов и диктофонов. |
| Утечки информации по цепям заземления, сетям громкоговорящей связи, охранно-пожарной сигнализации, линиям коммуникаций и сетям электропитания. |
| Высокочастотные каналы утечки информации бытовой и иной технике. |
| Утечка за счет плохой звукоизоляции стен и перекрытий. |
| Исследование злоумышленником производственных и технологических отходов. |
| Утечка информации через телефонные и факсимильные аппараты. |
| Оборудование виброканалов утечки информации на сетях отопления газо -и водоснабжения. |
| Утечка информации через персонал. |

Утечка информации с носителей (либо с носителями)

Утечка электромагнитных сигналов (в т.ч. оптического диапазона)

Утечка акустических сигналов (речевая информация)

Контактное подключение к электронным устройствам является простейшим способом съема информации. Чаще всего реализуется непосредственным подключением к линии связи.

Бесконтактное подключение может осуществляться за счет электромагнитных наводок или с помощью сосредоточенной индуктивности.

Встроенные микрофоны, видео- и радиозакладки в стенах, мебели, предметах. Могут быть установлены в элементы интерьера, строительные конструкции, СКТ, теле- и радиоприемники, розетки, телефонные аппараты, калькуляторы, замаскированы под канцелярские принадлежности, элементы одежды и т. д. Обладают дальностью действия от 50 до 1000 м при сравни­тельно небольшой стоимости. Ниже приведены примеры таких устройств.

Съем акустической информации при помощи лазерных устройств с от­ражающих поверхностей. Принцип действия основан на моделировании по амплитуде и фазе отраженного лазерного луча от окон, зеркал и т. д. Отра­женный сигнал принимается специальным приемником. Дальность дейст­вия — до нескольких сотен метров. На эффективность применения подобных устройств сильное влияние оказывают условия внешней среды (погодные условия).

Оптический дистанционный съем видеоинформации. Может осуществ­ляться через окна помещений с использованием длиннофокусного оптиче­ского оборудования в автоматическом или в ручном режиме работы.

Применение узконаправленных микрофонов и диктофонов. Применяются высокочувствительные микрофоны с очень узкой диаграммой направленно­сти. Узкая диаграмма направленности позволяет указанным устройствам избежать влияния посторонних шумов. Узконаправленные микрофоны мо­гут быть использованы совместно с магнитофонами и диктофонами.

Утечки информации по цепям заземления, сетям громкоговорящей свя­зи, охранно-пожарной сигнализации, линиям коммуникаций и сетям элек­тропитания. Утечка информации по цепям заземления возможна за счет существования гальванической связи проводников электрического тока с землей.

При организации каналов утечки информации через сигнализации раз­личного назначения злоумышленники используют «микрофонный эффект» датчиков. Подобные каналы утечки получили название параметрических каналов. Они формируются путем «высокочастотной накачки» (ВЧ - облучения, ВЧ -навязывания) электронных устройств с последующим пере­излучением электромагнитного поля, промодулированного информацион­ным сигналом. Промодулированные ВЧ-колебания могут быть перехвачены и демодулированы соответствующими техническими средствами.

Аналогичным образом могут быть созданы высокочастотные каналы утечки информации в бытовой и иной технике.

Утечка за счет плохой звукоизоляции стен и перекрытий. Съем инфор­мации может происходить с применением как простейших приспособлений (фонендоскоп), так и достаточно сложных технических устройств, например специализированных микрофонов.

Оборудование виброканалов утечки информации на сетях отопления, газо- и водоснабжения. Средой распространения акустических волн явля­ются трубы газо- и водоснабжения, конструкции зданий. Акустическая ин­формация может, например, восприниматься при помощи пьезоэлектриче­ских датчиков, затем усиливаться и фиксироваться при помощи магнитофо­нов либо передаваться в эфир.

Утечки информации через персонал. Многие исследователи, в том числе зарубежные, отмечают, что люди представляют наибольшую угрозу для информационной, и в частности компьютерной, безопасности. Наибольшую же угрозу представляют собственные сотруд­ники, которые могут уничтожать или искажать информацию, писать ком­пьютерные вирусы, похищать информацию в целях шпионажа.

По Г. Н. Мухину обстоятельствами, влекущими совершение подобных действий, могут быть:

* вербовка сотрудника криминальными структурами;
* внедрение этими же структурами или конкурирующими субъектами хо­зяйствования своего агента в штат предприятия или банка с целью вы­полнения разведывательных и иных функций;
* имеющиеся у сотрудника проблемы социально-психологического либо морально-этического порядка, обусловленные неудовлетворенностью им заработной платой или занимаемой должностью, пренебрежительным отношением к нему либо оскорбительным поведением со стороны руко­водства и др.

Проведенный анализ позволяет сделать вывод, что в основном работа злоумышленников по съему информации с каналов утечки сводится к полу­чению речевой информации.

Под речевой информацией понимают некоторый объем сведений, обра­ботанный человеческим сознанием и выданный в виде речевых сигналов акустическим речевым аппаратом человека. Речевая информация может быть записана на носитель, позволяющий считывать ее зрительным аппара­том человека или воспроизводить акустически.

В настоящее время в связи с бурным развитием электронной техники ре­чевая информация, передаваемая по каналам связи, становится все более уязвимой. Простейшие технические средства связи позволяют прослуши­вать телефонные переговоры, передаваемые по линиям связи, находясь на больших расстояниях от линии и объекта.

Любые средства передачи речевой информации могут быть одновремен­но и каналами ее утечки. По мнению Г. В. Давыдова и Ю. В. Шамгина, наиболее вероятными средствами передачи речевой информа­ции являются следующие акустические каналы:

человек - человек (слушатели);

человек - микрофон - усилитель - громкоговоритель - человек (слуша­тели);

человек - микрофон — магнитофон (запись речи на автоответчик);

магнитофон (считывание речи) — усилитель — громкоговоритель - чело­век (слушатели);

человек — тракт электросвязи (радиосвязи) - человек (слушатели);

автоответчик (считывание речи) - речевой сигнал - автоответчик (запись речи);

человек - устройство, управляющее голосом;

синтезатор искусственной речи - человек.

Наиболее распространенными средствами приема и регистрации сигна­лов речевой информации, распространяемой по акустическому каналу, яв­ляются:

микрофон и устройства, выполняющие его функцию;

пассивные отражатели светового луча, играющие роль мембраны для акустических волн (оконные стекла, иные тонкостенные отражатели);

волноводные тракты акустических волн различного типа (вентиляцион­ные каналы, стеновые панели);

лазерный луч, реагирующий на локальные изменения плотности воздуха в поле распространения акустической волны.

Наиболее очевидными каналами утечки речевой информации являются следующие:

1.На открытом пространстве (или в незащищенном помещении):

прямое подслушивание (скрытое или случайное);

узконаправленный микрофон

«жучки» в одежде, автомобиле, местных предметах и т. д.;

артикулярное считывание по мимике говорящих;

случайная или преднамеренная беседа, инициированная слушателем.

2. В помещении:

прослушивание через ограждающие конструкции из-за недостаточной звукоизоляции последних;

считывание со стекол окон;

прослушивание сигналов речи за счет передачи их по трубопроводам и вентиляционным системам;

прослушивание сигналов речи за счет акустоэлектрического преобразо­вания в системах телефонии, радиовещания и сигнализации;

визуальное считывание с носителей информации и дисплеев компьютеров.

**2. Каналы утечки информации из СКТ**

Эти каналы схематично представлены на рис. 3

|  |  |
| --- | --- |
| Каналы утечки информациииз СКТ | Утечка информации за счет введения программно-аппаратных закладок в СКТ |
| Утечки за счет побочного электромагнитного излучения и наводок (ПЭМИН) |
| Утечки за счет съема информации с принтера и клавиатуры по акустическому каналу |
| Утечка, модификации, уничтожение или блокирование информации с использованием компьютерных вирусов |
| Утеря носителей информации |
| Инициализация злоумышленником каналов утечки, вызванных несовершенством программного либо аппаратного обеспечения, а также систем защиты |

Рис. 3

***Утечка информации за счет введения программно-аппаратных за­кладок в СКТ.*** Весьма правильной представляется точка зрения авторов, отмечающих, что в настоящее время в основе производства технических средств и программного обеспечения вычислительных систем лежат комплектующие изделия зарубежного производства, что обеспечивает конкурентоспособность выпускаемых изделий. Однако при этом появля­ется угроза утечки информации, а также управляемого выведения из строя средств вычислительной техники, заложенная в них либо на этапе произ­водства, либо на этапе сборки. Подобные устройства могут быть установле­ны негласным образом и впоследствии при эксплуатации СКТ. Использова­ние закладных элементов (ЗЭ) представляется реальной и опасной угрозой при использовании вычислительной техники.

Аппаратные ЗЭ могут быть реализованы в аппаратуре персональных компьютеров и периферийных устройств. При этом возможны утечки ин­формации, искажение вычислительного процесса, а также управляемый вы­ход из строя вычислительной системы.

Программные ЗЭ могут быть представлены в виде модификации компь­ютерной программы, в результате которой данная программа способна вы­полняться несколькими способами в зависимости от определенных обстоя­тельств. При работе программные ЗЭ могут никак не проявляться, однако при определенных условиях программа работает по алгоритму, отличному от заданного (подобно компьютерным вирусам). В литературе описан при­мер внесения программистом в программу начисления заработной платы предприятия нежелательных изменений, работа которых началась после его увольнения, т. е. когда фамилия программиста исчезла из базы данных пер­сонала.

Существует классификация ЗЭ по следующим критериям:

способ у размещения ЗЭ;

способу активизации ЗЭ;

пути внедрения ЗЭ в систему;

разрушающему действию ЗЭ.

***Утечки за счет перехвата побочного электромагнитного излучении и наводок (ПЭМИН).*** При функционировании СКТ возникают побочные электромагнитные излучения и наводки, несущие обрабатываемую инфор­мацию. ПЭМИН излучаются в пространство клавиатурой, принтером, мо­нитором, накопителями на магнитных дисках, кабелями. Утечка данных обусловлена лишь излучением сигналов при перемене данных. Все прочие излучения сигналов от разных блоков СКТ являются вза­имными помехами.

Перехват ПЭМИН осуществляется радиоприемными устройствами, средствами анализа и регистрации информации. При благоприятных усло­виях с помощью направленной антенны можно осуществлять перехват на расстоянии до 1-1,5 км. В. И. Ярочкин отмечает, что перехват информации за счет ПЭМИН обладает рядом особенностей:

информация добывается без непосредственного контакта с источником;

на прием сигналов не влияет ни время года, ни время суток;

информация получается в реальном масштабе времени, в момент ее передачи или излучения;

реализуется скрытно;

дальность перехвата ограничивается только особенностями распространения радиоволн соответствующих диапазонов.

Утечки за счет съема информации с принтера и клавиатуры по акустическому каналу. Наличие указанного канала утечки позволяет перехватывать и декодировать акустические колебания, средой распространения которых является воздушная среда. Источником данных колебаний являются соответствующие устройства СКТ. Технически возможен перехват и декодирование кодов клавиш клавиатуры. Дальность действия подобных перехватов ограничена мощностью источника акустических и электромагнитных колебаний.

Утечка, модификация, уничтожение или блокирование информации с использованием компьютерных вирусов. Существует множество типов! вирусов, каждый из которых обладает собственными отличительными при-1 знаками. Анализ специальной научной литературы дает нам основание утверждать, что все вирусы изменяют либо файлы с данными, либо програм-1 мы внутри компьютера, либо разрушают сами компьютеры1. Большинство! из них представляют собой опасность только для IBM-совместимых компьютеров, однако именно этот тип компьютеров распространен в наибольшей! степени.

Последствия вирусной модификации могут быть различными - от нее значительных помех до полного уничтожения данных и программ. Вирусы, использующиеся правонарушителями для программного уничтожения, раз­рушают информацию в зависимости от определенных логических или вре­менных условий.

Попадание вирусов в компьютерную систему может быть спровоциро­вано различными способами от высокотехнологичного несанкционирован­ного подключения до основанного на личном доверии обмана оператора

системы путем переписывания заранее зараженных игр и сервисных про­грамм с умыслом на вывод компьютерной системы из строя. Вирус может попасть в систему и при неумышленных действиях операторов ЭВМ — при обмене дискетами, CD-ROM-дисками, файлами.

В настоящее время «рассадником» компьютерных вирусов стала гло­бальная сеть Internet. Особенно активно распространяются в этой сети так называемые макровирусы, которые передаются вместе с файлами докумен­тов MS-Word и файлами рабочих книг MS-Excel. Целесообразно привести краткий анализ традиционных воздействий компьютерных вирусов на СКТ, которые известны из специальной научной литературы. На рис. 5 приведена примерная видовая классификация компьютерных вирусов.

«Троянский конь» — специальная программа, которая разрешает дейст­вия, отличные от определенных в спецификации программы.

«Червь» - программа, которая создается для распространения своих ко­пий в другие компьютерные системы по компьютерным сетям путем поиска уязвимых мест в операционных системах.

«Логическая бомба» - программа, выполняемая периодически или в оп­ределенный момент с целью исказить, уничтожить или модифицировать данные. Наступление разрушающего эффекта, как правило, про­граммируется на заранее установленную календарную дату, время суток или иного значимого события.

Рис.5

Видовая классификация компьютерных вирусов

«Червь»

«троянский конь»

Файл-инфек-

торы

Вирусы

Начальной загрузки

Комбинированные (составные)

вирусы

Парные

Цепные

Полиморфные

Файл-инфекторы изменяют содержимое управляющих программ путем добавления нового кода в существующие файлы. Такой тип вируса поража­ет файлы, которые обозначены как COM, EXE, SYS, DLL. Файл-инфекторы распространяются через любой носитель данных, используемый для хране­ния и передачи управляемого кода. Вирус может храниться на хранения информации либо передаваться по сетям и через модемы.

Вирусы сектора начальной загрузки заражают основную загрузочную область на жестких дисках или загрузочный сектор на дискетах. Оригинальная версия обычно, но не всегда, хранится где-нибудь на диске. В результате вирус запустится перед загрузкой компьютера. Вирусы такого типа обычно остаются в секторе памяти до тех пор, пока пользователь не выйдет из системы.

Вирусы, результаты воздействия которых на компьютерные системы) их сети могут проявляться как применение нескольких отдельных вирусов, называются комбинированными (составными) вирусами. Вирус, который проникает как в сектор начальной загрузки, так и в файлы, имеет больше возможностей для размножения. В результате способности вируса проникать как в сектор начальной загрузки, так и в файлы, компьютерная система заражается вирусом независимо от того, была ли она загружена с зараженного диска или в результате запуска зараженной программы.

Парные вирусы поражают операционную систему таким образом, что нарушается последовательность выполнения файлов СОМ и ЕХЕ с одним именем. Этот тип вируса создает копию файла СОМ, но в размере файла ЕХЕ. Имя файла остается прежним. При запуске пользователем программы операционная система выполнит вновь созданный файл СОМ, в котором содержится код вируса, после чего загружает и выполняет файл ЕХЕ.

Цепными называются вирусы, модифицирующие таблицы расположения файлов и директорий таким образом, что вирус загружается и запускается до того, как запускается желаемая программа. Они связывают элементы таблицы расположения директорий с отдельным кластером, содержащим код вируса. Оригинальный номер первого кластера сохраняется в неисполь­зуемой части элемента таблицы директорий. Сама по себе программа физи­чески не изменяется, изменяется только элемент таблицы расположения ди­ректорий. Подобные вирусы также известны как вирусы системных файлов, секторные вирусы или вирусы таблиц расположения файлов.

Полиморфные вирусы производят копии самих себя. Эти копии различ­ны для каждого из незараженных файлов. Код вируса меняется после каж­дого нового заражения, но принцип его действия всякий раз остается неиз­менным. Известны, например, две так называемые утилиты мутации виру­са: Mutation Engine и Polymorphic Trident Engine. При использовании этих утилит любой вирус становится полиморфным, так как утилиты добавляют в его код определенные команды в произвольной последовательности.

По деструктивным возможностям компьютерные вирусы можно раз­делить на следующие 4 группы (рис. 6):

Классификация компьютерных вирусов по деструктивным возможностям

Безвредные

Неопасные

Опасные

Очень опасные

Рис. 6

1. Безвредные - никак не влияющие на работу компьютерной системы,
кроме уменьшения количества свободной памяти, указанной в результате
своего распространения.
2. Неопасные - влияние которых ограничивается уменьшением свобод­
ной памяти, а также графическими, звуковыми и прочими эффектами.
3. Опасные - которые могут привести к серьезным сбоям в работе ком­пьютерных систем.
4. Очень опасные — в алгоритм их работы введены процедуры, которые
могут вызвать потерю программ, уничтожить данные, стереть необходимую
для работы компьютера информацию, записанную в системных областях
памяти, способствовать быстрому износу движущихся частей механизмов
(например, вводить в резонанс и разрушать головки некоторых типов жест­ких дисков) и т. д.

Необходимо отметить, что существуют и другие классификации компь­ютерных вирусов, например по способу их воздействия на СКТ и обслуживающий их персонал.

1.Компьютерные вирусы, не повреждающие файловую структуру:

размножающиеся в оперативных запоминающих устройствах (ОЗУ);

раздражающие оператора (имитирующие неисправность аппаратуры; формирующие сообщения на терминале; формирующие звуковые эф­фекты; переключающие режимы настройки и др.);

сетевые.

2. Компьютерные вирусы, повреждающие файловую структуру:

повреждающие программы и данные пользователя;

повреждающие системную информацию (области диска, форматирую­щие носители, файлы операционной системы).

3. Компьютерные вирусы, воздействующие на аппаратуру и оператора:

повреждающие аппаратуру (микросхемы, диски, принтеры; выжигаю­щие люминофор);

воздействующие на оператора (в том числе на зрение, психику и др.).

***Утеря носителей информации***. Может произойти в результате:

хищения с полным или частичным разрушением места хранения;

физического уничтожения из-за умышленных несанкционированны действий персонала;

пожара либо воздействия на носитель высокой температуры, ионизирующего излучения, химических веществ, сильного электромагнитного поля;

стихийных бедствий (землетрясение, наводнение, ураган и др.);

иных форс-мажорных обстоятельств.

Инициализация злоумышленником каналов утечки, вызванных несовершенством программного либо аппаратного обеспечения, а такою систем защиты, как правило, производится на этапе подготовки к совершению информационного компьютерного преступления, реже - непосредственно при его совершении. Речь идет о так называемых атаках на инфор­мационные системы. Под атакой подразумевается любая попытка преодо­ления систем защиты