**Практическая работа № 3**

**Анализ защищенности объекта защиты информации**

**Цель:** Формирование умений и навыков определения угроз и

защищённости объектов информации

**задание:**

необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. виды угроз;
2. характер происхождения угроз;
3. классы каналов несанкционированного получения информации;
4. источники появления угроз;
5. причины нарушения целостности информации;

*Наименование объекта защиты информации*

1. Сервер в бухгалтерии
2. Сеть с выделенным сервером с выхода в Интернет
3. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях
4. Средства телекоммуникации
5. Банковские операции (внесение денег на счет и снятие)
6. Операции с банковскими пластиковыми карточками.
7. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
8. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
9. Материалы для служебного пользования на твердых носителях и на электронных носителях в производстве.
10. Материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии
11. Материалы для служебного пользования на твердых носителях в архиве.
12. Материалы для служебного пользования на твердых носителях и на электронных носителях в налоговой инспекции.
13. Комната для переговоров по сделкам на охраняемой территории.
14. Комната для переговоров по сделкам на неохраняемой территории.
15. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).
16. Судебные материалы (твердая копия и на электронных носителях).
17. Паспортный стол РОВД (твердая копия и на электронных носителях).

**Характер происхождения угроз определяется типом каналов связи**, по которым передается информация, способам воздействия угроз на объект информационной безопасности, а также причинами, обстоятельствами (предпосылками) и условиями дестабилизирующего воздействия на информацию.

В свою очередь, каналы связи подразделяются на:

* + проводные;
  + волоконно - оптические;
  + беспроводные (радиотехнические).

Наиболее часто для передачи информации применяются телефонные линии в качестве проводных линий связи. Это связано с тем, что большинство компьютеров используют для передачи данных модемы, подключенные к телефонной линии. При этом способы подслушивания линии, связывающей компьютеры, включают в себя:

1. непосредственное подключение к телефонной линии:

1.1 контактное - последовательное или параллельное (прямо на АТС или где-нибудь на линии между телефонным аппаратом и АТС);

1.2 бесконтактное (индукционное) подключение к телефонной линии;

2. помещение радиоретранслятора («жучка») на телефонной линии:

2.1 последовательное включение;

2.2 параллельное включение.

В основном эти способы применяются для прослушивания телефонных разговоров, по причине того, что прослушивание компьютерного обмена данными требует значительных затрат ресурсов на его расшифровку. Несмотря на это, в настоящее время появились системы перехвата факсовой и модемной связи, которые при использовании персонального компьютера со специальным программным обеспечением позволяют расшифровать перехваченную информацию.

Способы воздействия угроз на объекты информационной безопасности подразделяются на информационные, программно-математические, физические, радиоэлектронные и организационно-правовые.

К информационным способам относятся:

1) нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

несанкционированный доступ к информационным ресурсам;

3) манипулирование информацией (дезинформация, сокрытие или искажение информации);

4) нарушение технологии обработки информации.

Программно-математические способы включают:

1) внедрение компьютерных вирусов;

2) установку программных и аппаратных закладных устройств;

3) уничтожение или модификацию данных в автоматизированных информационных системах.

Физические способы включают:

1) уничтожение или разрушение средств обработки информации и связи;

2) уничтожение, разрушение или хищение машинных, или других оригинальных носителей информации;

3) хищение программных или аппаратных ключей и средств криптографической защиты информации;

4) воздействие на персонал.

Радиоэлектронными способами являются:

1) перехват информации в технических каналах ее возможной утечки;

2) внедрение электронных устройств перехвата информации в технические средства и помещения;

3) перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи;

4) радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

1) невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;

2) неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

Что же касается причин и условий воздействия угроз, то рассмотрим только воздействия со стороны технических средств.

Причинами дестабилизирующего воздействия на информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи могут быть:

a) недостаток или плохое качество средств;

b) низкое качество режима функционирования средств;

c) перезагруженность средств;

d) низкое качество технологии выполнения работ;

e) дестабилизирующее воздействие на средства со стороны других источников воздействия.

К обстоятельствам (предпосылкам), вызывающим эти причины, следует отнести:

a) недостаточность финансовых ресурсов, выделяемых на приобретение и эксплуатацию средств;

b) плохой выбор средств;

c) старение (износ) средств;

d) конструктивные недоработки или ошибки при монтаже средств;

e) ошибки при разработке технологии выполнения работ, в том числе программного обеспечения;

f) дефекты используемых материалов;

g) чрезмерный объем обрабатываемой информации;

h) причины, лежащие в основе дестабилизирующего воздействия на средства со стороны других источников воздействия.

Условиями, обеспечивающими реализацию дестабилизирующего воздействия на информацию со стороны технических средств, могут являться:

a) недостаточное внимание к составу и качеству средств со стороны администрации, нередко из-за недопонимания их значения;

b) нерегулярный профилактический осмотр средств;

c) низкое качество обслуживания средств.

Классы каналов несанкционированного получения информации

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Каналы от источника информации при НСД к нему** | 1. **Каналы со средствами обработки информации при НСД к ним** | 1. **Каналы от источника информации без НСД к нему** | 1. **Каналы со средств обработки информации без НСД к ним** |
| 1. Хищение носителей информации. 2. Копирование информации с носителей (материально-вещественных, магнитных ит. д.). 3. Подслушивание разговоров (в том числе аудиозапись). 3. Установка закладных устройств в помещение и съем информации с их помощью. 4. Выведывание информации обслуживающего персонала на объекте. 5. Фотографирование или видеосъемка носителей информации внутри помещения. | 1. Снятие информации с устройств электронной памяти. 2. Установка закладных устройств в систему обработки информации (СОИ) 3. Ввод программных продуктов, позволяющих злоумышленнику получать информацию. 4. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.). | 1. Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов). 2. Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств). 3. Использование технических средств оптической разведки (биноклей, подзорных труб и т. д.). 4. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.) 5. Осмотр отходов и мусора. 6. Выведывание информации у обслуживающего персонала за пределами объекта. 7. Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.). | 1. Электромагнитные излучения СОИ (паразитные электромагнитные излучения (ПЭМИ), паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию). 2. Электромагнитные излучения линий связи.  3. Подключения к линиям связи.  4. Снятие наводок электрических сигналов с линий связи.  5. Снятие наводок с системы питания.  6. Снятие наводок с системы заземления.  7. Снятие наводок с системы теплоснабжения.  8. Использование высокочастотного навязывания.  9. Снятие с линий, выходящих за пределы объекта, сигналов, образованных на технических средствах за счет акустоэлектрических преобразований.  10. Снятие излучений оптоволоконных линий связи.  11. Подключение к базам данных и ПЭВМ по компьютерным сетям |

**Источники угроз**

Источники угроз для реализации угрозы используют уязвимости объектов и системы защиты.

|  |  |  |
| --- | --- | --- |
| **Обусловленные действиями субъекта**  **(антропогенные источники)** | **Обусловленные техническими средствами**  **(техногенные источники)** | **Стихийные источники** |
| субъекты, действия которых могут привести к нарушению безопасности информации, данные действия могут быть квалифицированы как умышленные или случайные преступления  Источники, действия которых могут привести к нарушению безопасности информации могут быть как внешними, так и внутренними.  Данные источники можно спрогнозировать, и принять адекватные меры. | источники угроз менее прогнозируемы и напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также могут быть как внутренними, так и внешними. | данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия, или др. обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить), такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех.  Такие источники угроз совершенно не поддаются прогнозированию и, поэтому меры против них должны применяться всегда.  Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы. |

**Причины нарушения целостности информации**

Целостность информации - это свойство информации, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному её состоянию).

|  |  |  |
| --- | --- | --- |
| **Субъективные (искусственные)**  вызванные воздействием на информационную сферу человека | | **Объективные (естественные)**  вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека |
| Преднамеренные  (умышленные) | Непреднамеренные  (случайные) | Непреднамеренные |
| Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).  - Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).  - Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием). | - Отказы обслуживающего персонала (гибель, длительный выход из строя).  - Сбои людей (временный выход из строя).  - Ошибки людей. | Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.  - Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.  - Стихийные бедствия (наводнения, землетрясения, ураганы).  - Несчастные случаи (пожары, взрывы, аварии).  - Электромагнитная несовместимость. |