Уфимский Юридический Институт МВД России

Основы информационной безопасности в ОВД

Защита информации от утечки на объектах информатизации ОВД

Лекция тема № 3

План

1. **Каналы утечки информации.**
2. **Современные угрозы утечки информации.**
3. **Технические средства обнаружения угроз.**
4. **Методы и средства блокирования каналов утечки информации.**

1. Основные угрозы безопасности информации.
2. Понятие и виды каналов утечки информации ограниченного доступа.

Литература

- Конституция РФ
- Об информации, информационных технологиях и о защите информации. ФЗ РФ от 27.07.2006 №149–ФЗ
- Доктрина информационной безопасности РФ Указ Президента РФ от 9 сентября 2000 г. № Пр-1895
- ГОСТ Р 52069.0-2013. «Национальный стандарт РФ. Защита информации. Система стандартов. Основные положения». Приказ Росстандарта от 28.02.2013 № 3-ст

Литература

Амиров А.Р. и др. Основы информационной безопасности в ОВД : курс лекций – Уфа : УЮИ МВД РФ, 2011.

Баранова Е.К. Основы информатики и защиты информации: учеб.пособие - М. : РИОР : ИНФРА-М, 2013.

Рудаков Б.В. и др. Основы специальной техники органов внутренних дел (Общая часть): учеб. пособие - Тюмень : ТИПК МВД России, 2013.

2. Каналы утечки информации

Канал утечки информации

- физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям

Технический канал утечки информации

- совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

технические каналы утечки информации

В зависимости от способа перехвата, от физической природы возникновения сигналов, а также среды их распространения

- электромагнитные,
- электрические
- параметрические

Электромагнитные каналы

характерными являются побочные излучения:

- электромагнитные излучения технических средств обработки информации. Носителем информации является электрический ток. Сила тока, напряжение, частота или фаза которого изменяется по закону информационного сигнала;
- электромагнитные излучения на частотах работы высокочастотных генераторов технических средств обработки информации, вспомогательных средств обработки информации.

Электрические каналы

причины возникновения :

– наводки электромагнитных технических средств обработки информации

– просачивание электромагнитных сигналов в цепи электропитания

– просачивание информационных сигналов в цепи заземления

– съем информации с использованием закладных устройств

Параметрические каналы

- формируются путем «высокочастотного облучения» технических средств обработки информации, при взаимодействии электромагнитного поля с элементами технических средств обработки информации происходит переизлучение электромагнитного поля, промодулированного информационным сигналом

технические каналы утечки акустической информации

в зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов:

- воздушные,
- вибрационные,
- электроакустические,
- оптико-электронные
- параметрические

утечка видовой информации

- получаемой техническими средствами в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов

методы съема компьютерной информации

Основные возможности несанкционированного доступа обеспечиваются специальным математическим обеспечением, включающим в себя :

1) компьютерные вирусы,
2) «логические бомбы»,
3) «троянские кони»,
4) программные закладки

внутренние каналы утечки информации

связаны, как правило, с администрацией и обслуживающим персоналом, с качеством организации режима работы:

1) хищение носителей информации,
2) съем информации с ленты принтера и плохо стертых дискет,
3) использование производственных и технологических отходов,
4) визуальный съем информации с дисплея и принтера,
5) несанкционированное копирование

2. Современные угрозы утечки информации

Стратегии защиты от атак

1) приобретение самых расхваливаемых (хотя не всегда самых лучших) систем защиты от всех возможных видов атак
2) предварительный анализ вероятных угроз и последующий выбор средств защиты от них

Способы анализа угроз, или анализ риска

- анализ информационной системы, обрабатываемой в ней информации, используемого программно-аппаратного обеспечения

Источники атак

- Недобросовестные сотрудники
- Хакеры
- Конкуренты
- Зарубежные компании
- Зарубежные правительства

самый популярный канал утечки информации

сеть Интернет

Классификация угроз безопасности

По способу воздействия на сеть:

- в интерактивном режиме;
- в пакетном режиме.

По целям угрозы:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение работоспособности.

По используемой ошибке:

- неадекватность политики безопасности;
- ошибки администратора;
- ошибки в алгоритмах;
- ошибки в программах.

По объекту атаки:

- субъекты АСОИ;
- объекты АСОИ;
- процессы пользователя;
- пакеты данных и каналы связи.

По используемым средствам:

- стандартное программное обеспечение;
- специальное программное обеспечение.

По характеру воздействия:

- активное воздействие;
- пассивное воздействие.

По состоянию объекта атаки:

- хранение (на диске, ленте);
- передача по линии связи;
- обработка (когда объектом атаки является процесс пользователя).

По принципу воздействия:

- с использованием доступа субъекта к объекту;
- с использованием скрытых каналов.

По способу воздействия:

- непосредственное воздействие на объект;
- воздействие на систему разрешений.

3. Технические средства обнаружения угроз

обнаружители угроз безопасности

технические средства, используемые для обеспечения информационной безопасности:

1) для обнаружения радио-, видео- и телефонных закладок (жучков)
2) устройства поиска по электромагнитному излучению:

- приемники, сканеры, шумометры, детекторы инфракрасного излучения, анализаторы спектра, частотомеры, панорамные приемники, селективные микровольтметры

4. Методы и средства блокирования каналов утечки информации

Основные направления противодействия утечке информации

1) обеспечение физической (технические средства, линии связи, персонал)
2) логической (операционная система, прикладные программы и данные)

защиты информационных ресурсов