Практическая работа №3

Классы каналов несанкционированного получения информации (нарушения конфиденциальности);

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющим нанести ущерб любой из составляющих информационной безопасности является несанкционированный доступ. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Под несанкционированным доступом понимается получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации.

Рассмотрим относительно полное множество каналов несанкционированного получения информации, сформированного на основе такого показателя, как степень взаимодействия злоумышленника с элементами объекта обработки информации и самой информацией.

К **первому классу** относятся каналы от источника информации при НСД к нему.

1. Хищение носителей информации.
2. Копирование информации с носителей (материально-вещественных, магнитных и т. д.).
3. Подслушивание разговоров (в том числе аудиозапись).
4. Установка закладных устройств в помещение и съем информации с их помощью.
5. Выведывание информации обслуживающего персонала на объекте.
6. Фотографирование или видеосъемка носителей информации внутри помещения.

Ко **второму классу** относятся каналы со средств обработки информации при НСД к ним.

1. Снятие информации с устройств электронной памяти.
2. Установка закладных устройств в СОИ.
3. Ввод программных продуктов, позволяющих злоумышленнику получать информацию.
4. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

К **третьему классу** относятся каналы от источника информации без НСД к нему.

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.).

К **четвертому классу** относятся каналы со средств обработки информации без НСД к ним.

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 и т. д.

**Пример 1**

Классы каналов несанкционированного получения информации к данным, хранящимся на сервере организации

Утечка информации, хранящаяся на сервере возможно по следующим каналам:

* Радиоканалы - это каналы передачи информации, при которой в качестве носителя информации используются радиоволны, свободно распространяемые в пространстве.
* Инфракрасный канал - это канал передачи данных, не требующий для своего функционирования проводных соединений.
* Проводные линии - это линии связи, состоящие из направленных средств передачи, предназначенные для организации связи.

В качестве проводных линий при передаче информации к внешним средствам регистрации могут быть использованы:

* сети переменного тока;
* линии телефонной связи;
* радиотрансляционные и технологические линии;
* специально проложенные проводные линии.

**Пример 2**: сервер, содержащий бухгалтерские отчеты крупной компании

К рассматриваемому объекту из первого класса можно отнести такие угрозы, как:

* выведывание информации обслуживающего персонала на объекте.

Из второго класса:

* ввод программных продуктов, позволяющих злоумышленнику получать информацию.
* Каналы угроз третьего класса, относительно данного объекта:
* выведывания информации у обслуживающего персонала за пределами объекта;
* изучения выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т.д.);

Каналы угроз четвертого класса:

* электромагнитные излучения линий связи;
* подключения к линиям связи;
* подключение к базам данных и ПЭВМ по компьютерным сетям.

Практическая часть

Для своего варианта описать классы каналов несанкционированного получения информации.