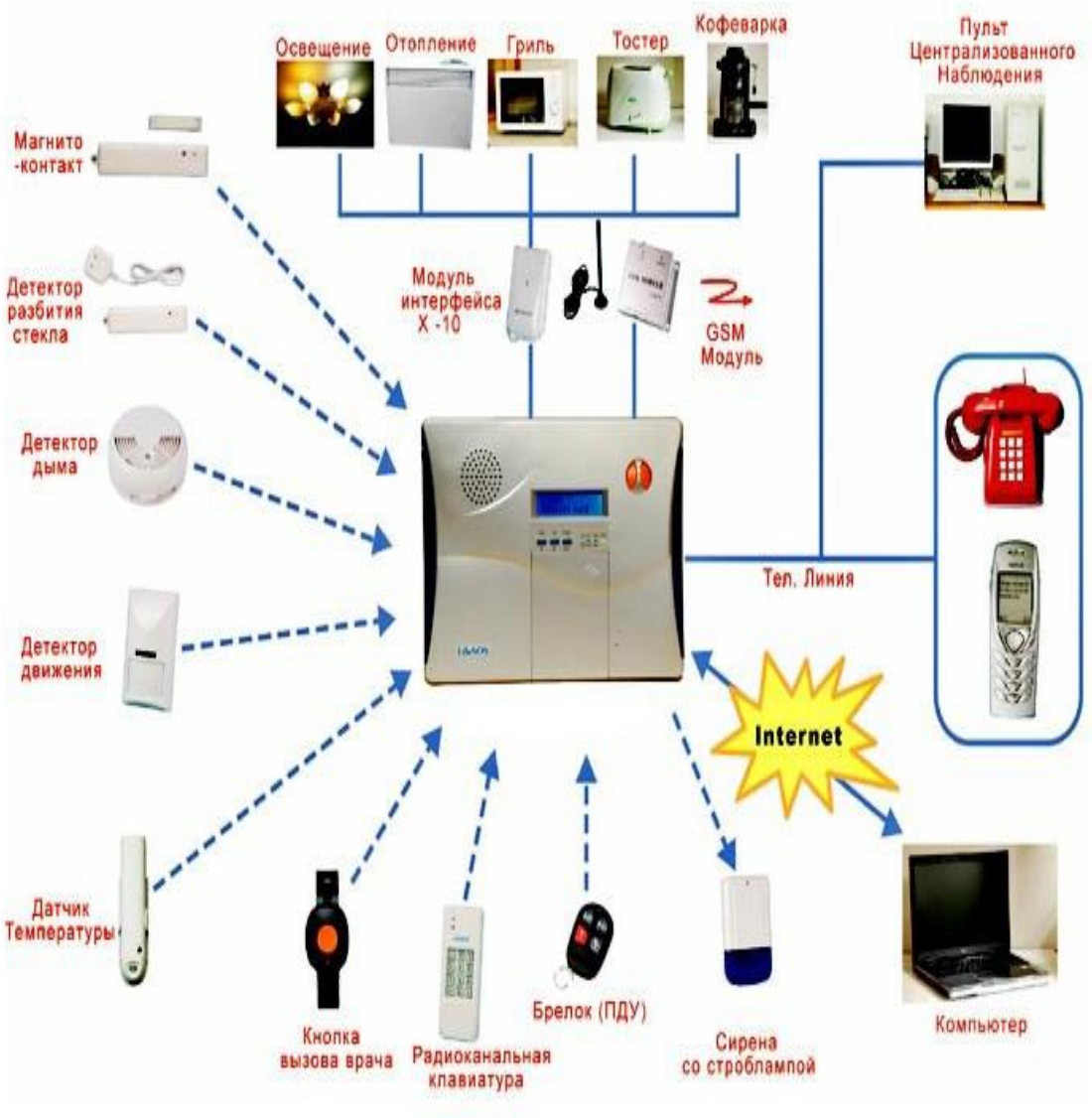
Защита собственной информации от несанкционированного доступа.

Подготовила ученица 10 класса
МКОУ Писаревская СОШ
Кантемировского р-на
Воронежской обл.

Плешканева Алена

Защита информации Несанкционированного Доступа



Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

По данным Миннесотского университета США, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули свой бизнес, причём половина из них заявила о своей несостоятельности немедленно.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Чем больше людей получает доступ к информационной технологии и компьютерному оборудованию, тем больше возникает возможностей для совершения компьютерных преступлений.

Компьютерным преступником может быть любой.

Типичный компьютерный преступник - это не молодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник - это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами.

ДЛЯ УСПЕШНОЙ ЗАЩИТЫ СВОЕЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЬ ДОЛЖЕН ИМЕТЬ АБСОЛЮТНО ЯСНОЕ ПРЕДСТАВЛЕНИЕ О ВОЗМОЖНЫХ *ПУТЯХ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА*. ПЕРЕЧИСЛИМ ОСНОВНЫЕ ТИПОВЫЕ ПУТИ НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ:

- Хищение носителей информации и производственных отходов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- мистификация (маскировка под запросы системы);
- использование недостатков операционных систем и **языков программирования**;
- использование программных закладок и программных б типа "троянский конь";
- перехват электронных излучений;
- перехват акустических излучений;
- дистанционное фотографирование;
- применение подслушивающих устройств;

ПРИЗНАКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ:

· неавторизованное использование компьютерного времени;

· неавторизованные попытки доступа к файлам данных;

· кражи частей компьютеров;

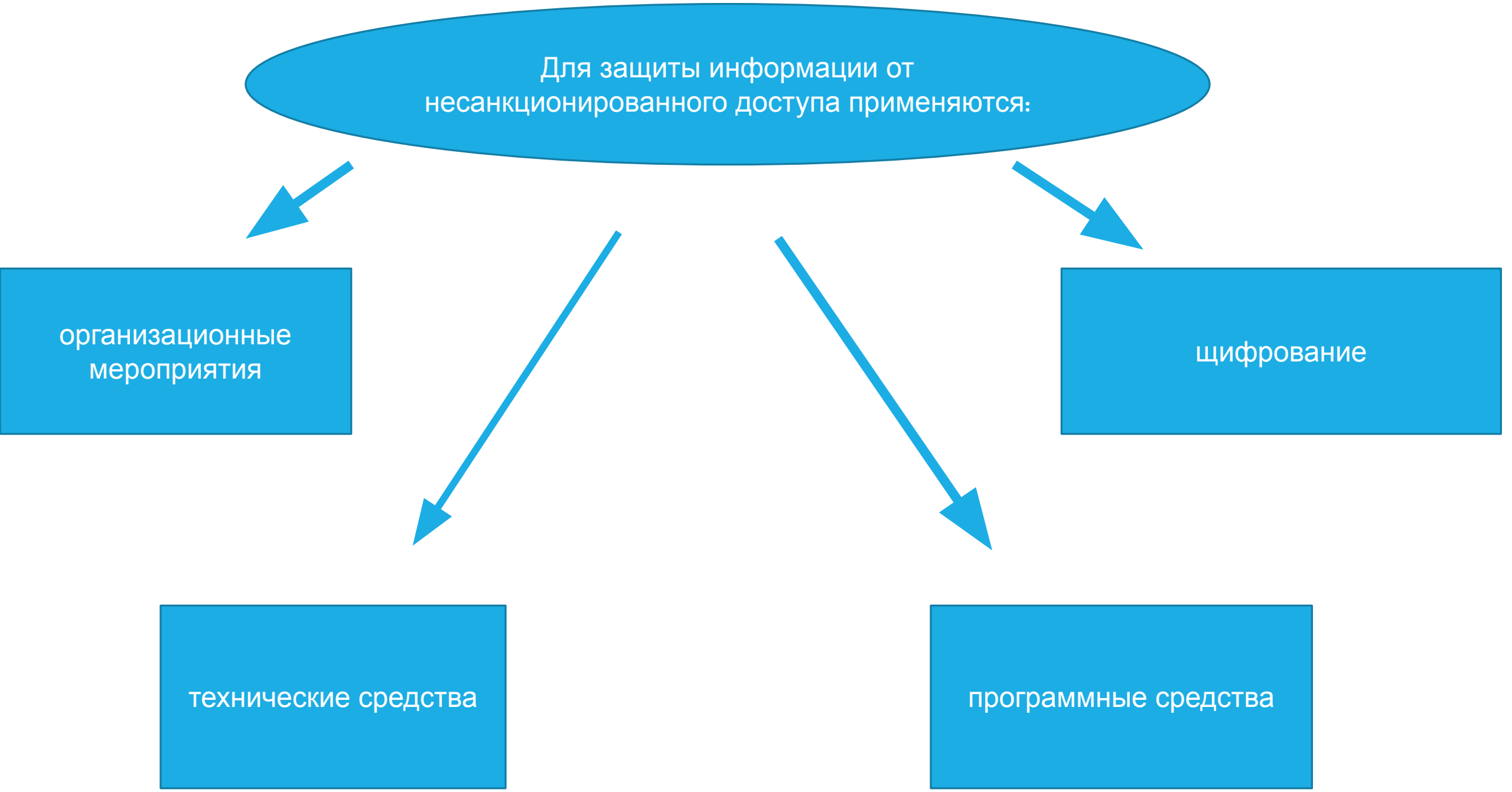
· кражи программ;

· физическое разрушение оборудования;

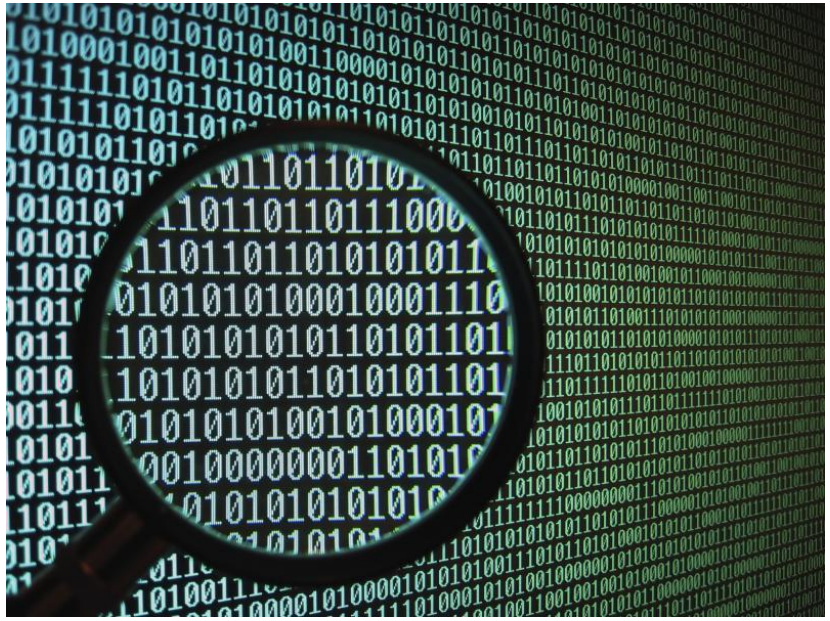
· уничтожение данных или программ;

· неавторизованное владение дискетами, лентами или распечатками.

Это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест и указать, где находится брешь в защите. В то время как признаки могут помочь выявить преступление или злоупотребление, меры защиты могут помочь предотвратить его.


Для защиты информации от несанкционированного доступа применяются:
организационные мероприятия
щифрование
технические средства
программные средства

Шифрование–это преобразование (кодирование) открытой информации в зашифрованную, не доступную для понимания посторонних. Шифрование применяется в первую очередь для передачи секретной информации по незащищенным каналам связи. Шифровать можно любую информацию — тексты, рисунки, звук, базы данных и т.д. Человечество применяет шифрование с того момента, как появилась секретная информация, которую нужно было скрыть от врагов. Первое известное науке шифрованное сообщение — египетский текст, в котором вместо принятых тогда иероглифов были использованы другие знаки. Методы шифрования и расшифровывания сообщения изучает наука ***криптология***, история которой насчитывает около четырех



ВИДЫ ШИФРОВАНИЯ

Криптостойкость шифра — это устойчивость шифра к расшифровке без знания ключа. Стойким считается алгоритм, который для успешного раскрытия требует от противника недостижимых вычислительных ресурсов, недостижимого объема перехваченных сообщений или такого времени, что по его истечении защищенная информация будет уже неактуальна.

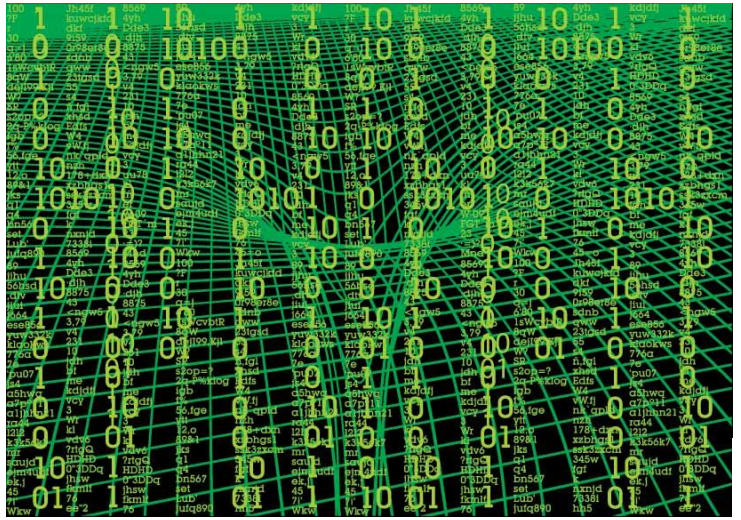
Один из самых известных и самых древних шифров – шифр Цезаря. В этом шифре каждая буква заменяется на другую, расположенную в алфавите на заданное число позиций k вправо от нее. Алфавит замыкается в кольцо, так что последние символы заменяются на первые. Шифр Цезаря относится к *шифрам простой подстановки*, так как каждый символ исходного сообщения заменяется на другой символ из того же алфавита. Такие шифры легко раскрываются с помощью частотного анализа, потому что в каждом языке частоты встречаемости букв примерно постоянны для любого достаточно большого текста.

Значительно сложнее сломать шифр Виженера, который стал естественным развитием шифра Цезаря. Для использования шифра Виженера используется ключевое слово, которое задает переменную величину сдвига. Шифр Виженера обладает значительно более высокой криптостойкостью, чем шифр Цезаря. Это значит, что его труднее раскрыть — подобрать нужное ключевое слово. Теоретически, если длина ключа равна длине сообщения, и каждый ключ используется только один раз, шифр Виженера взломать невозможно.

Виды Шифрования

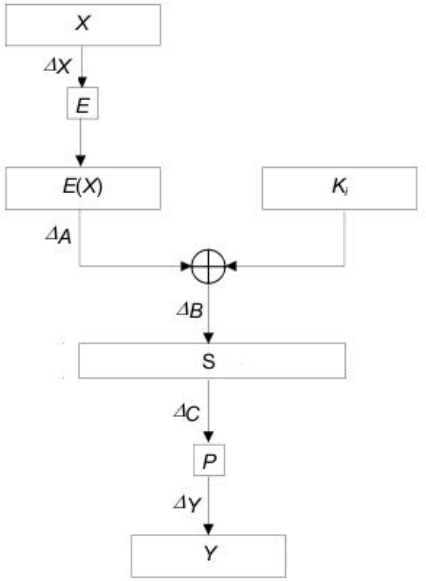
Ключ — это параметр алгоритма шифрования (шифра), позволяющий выбрать одно конкретное преобразование из всех вариантов, предусмотренных алгоритмом. Знание ключа позволяет свободно зашифровывать и расшифровывать сообщения.

Все шифры (системы шифрования) делятся на две группы — симметричные и несимметричные (с открытым ключом). *Симметричный шифр* означает, что и для шифрования, и для расшифровывания сообщений используется один и тот же ключ. В системах с *открытым ключом* используются два ключа — открытый и закрытый, которые связаны друг с другом с помощью некоторых математических зависимостей. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.



Криптография — это наука о способах шифрования информации.

Криптоанализ — это наука о методах и способах вскрытия шифров.



Обычно предполагается, что сам алгоритм шифрования известен всем, но неизвестен его ключ, без которого сообщение невозможно расшифровать. В этом заключается отличие шифрования от простого кодирования, при котором для восстановления сообщения достаточно знать только алгоритм кодирования.

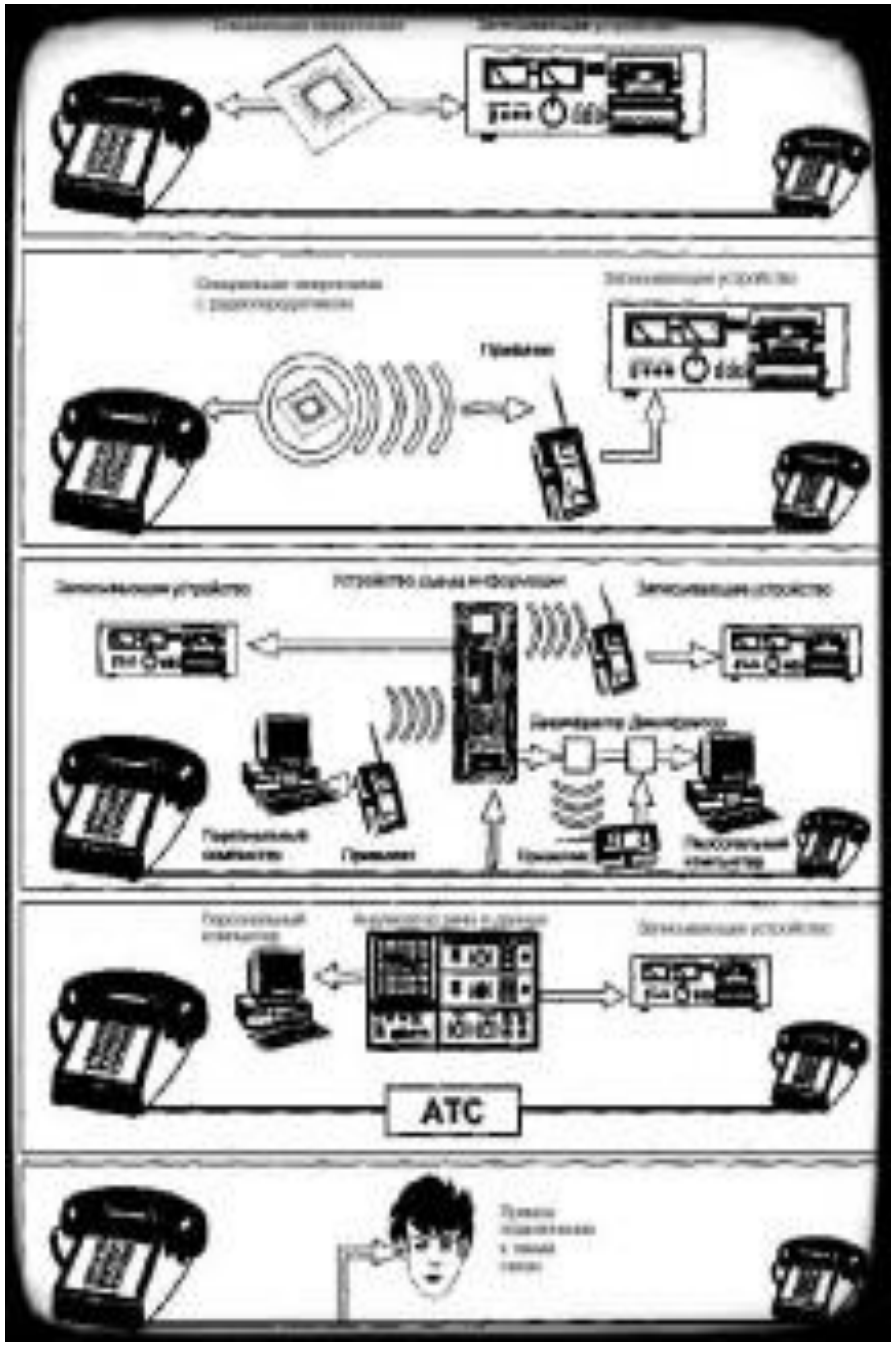
СПОСОБЫ НСД К ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНИЧЕСКИХ СРЕДСТВ

ЛЮБАЯ ЭЛЕКТРОННАЯ СИСТЕМА, КОТОРАЯ СОДЕРЖИТ СОВОКУПНОСТЬ УЗЛОВ, ЭЛЕМЕНТОВ И ПРОВОДНИКОВ И ОБЛАДАЕТ ПРИ ЭТОМ ИСТОЧНИКАМИ ИНФОРМАЦИОННОГО СИГНАЛА — ЕСТЬ КАНАЛАМИ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. СПОСОБЫ НСД И КАНАЛЫ УТЕЧКИ ОБЪЕКТИВНО СВЯЗАННЫ. ВАРИАНТЫ СВЯЗЕЙ ПОКАЗАНЫ В ТАБЛ. 1.

22363

22363

Способ НСД	Визуальный канал утечки	Акустический канал утечки	Электромагнитный канал утечки	Материальный канал утечки
Подслушивание		+	+	
Визуальное наблюдение	+			
Хищение			+	+
Копирование			+	+
Подделка			+	+
Незаконное подключение		+	+	
Перехват		+	+	
Фотографирование	+			



СПОСОБЫ НСД К ЛИНИЯМ СВЯЗИ
ЗАЧАСТУЮ В КАЧЕСТВЕ ЛИНИЙ СВЯЗИ ИСПОЛЬЗУЮТ ТЕЛЕФОННЫЕ ЛИНИИ ИЛИ ОПТОВОЛОКОННЫЕ ЛИНИИ. СПОСОБЫ ПРОСЛУШИВАНИЯ ТЕЛЕФОННЫХ ЛИНИЙ ПОКАЗАНЫ НА РИС.2.

ТАКЖЕ ЕСТЬ СИСТЕМЫ ПРОСЛУШИВАНИЯ ЛИНИЙ, КОТОРЫЕ НЕ ТРЕБУЮТ ПРЯМОГО КОНТАКТА С ТЕЛЕФОННОЙ ЛИНИЕЙ. ТАКИЕ СИСТЕМЫ ИСПОЛЬЗУЮТ ИНДУКТИВНЫЕ МЕТОДЫ СЪЕМА ДАННЫХ. ТАКИЕ СИСТЕМЫ НЕ ИМЕЮТ ШИРОКОГО ПРИМЕНЕНИЯ, ТАК КАК ОНИ СИЛЬНО БОЛЬШИЕ ИЗ-ЗА СОДЕРЖАНИЯ НЕСКОЛЬКО КАСКАДОВ УСИЛЕНИЯ СЛАБОГО НЧ-СИГНАЛА И В ДОБАВОК ВНЕШНИЙ ИСТОЧНИК ПИТАНИЯ.
НО НА СЕГОДНЯ ЛИНИИ ОПТОКОЛОКНА ИМЕЮТ БОЛЕЕ ШИРОКИЙ СПЕКТР РЕАЛИЗАЦИИ. ИНФОРМАЦИЯ ПО ТАКОМУ КАНАЛУ ПЕРЕДАЕТСЯ В ВИДЕ ПУЛЬСИРУЮЩЕГО СВЕТОВОГО ПОТОКА, НА КОТОРЫЙ В ПРИНЦИПИ НЕ ВЛИЯЮТ МАГНИТНЫЕ И ЭЛЕКТРИЧЕСКИЕ ПОМЕХИ. ТАКЖЕ ПО ТАКОМУ КАНАЛУ ТЯЖЕЛЕЕ ПЕРЕХВАТИТЬ ДАННЫЕ, ЧТО ПОВЫШАЕТ БЕЗОПАСНОСТЬ ПЕРЕДАЧИ. ПРИ ЭТОМ СКОРОСТЬ ПЕРЕДАЧИ ДОСТИГАЕТ ГИГАБАЙТ/СЕКУНДУ. ДЛЯ ПОДКЛЮЧЕНИИ К ТАКОМУ КАНАЛУ СВЯЗИ, УДАЛЯЮТ ЗАЩИТНЫЕ СЛОИ КАБЕЛЯ. ПОТОМ СТРАВЛИВАЮТ СВЕТООТРАЖАЮЩУЮ ОБОЛОЧКУ И ИЗГИБАЮТ КАБЕЛЬ ПО СПЕЦИАЛЬНЫМ УГЛОМ, ЧТО БЫ СНИМАТЬ ИНФОРМАЦИЮ. ПРИ ЭТОМ СРАЗУ БУДЕТ ЗАМЕТНО ПАДАТЬ МОЩНОСТЬ СИГНАЛА. ТАКЖЕ МОЖНО БЕСКОНТАКТНО ПОДКЛЮЧАТСЯ К КАНАЛУ СВЯЗИ, НО ДЛЯ ЭТОГО НУЖНО ИМЕТЬ ОПРЕДЕЛЕННЫЙ УРОВЕНЬ ЗНАНИЙ И ПОДГОТОВКИ.