



# **Защита информации от утечки по техническим каналам**

Выполнил: студент  
группы Р5-201  
Абдылдаев Кайрат

Москва, 2012



# Определения

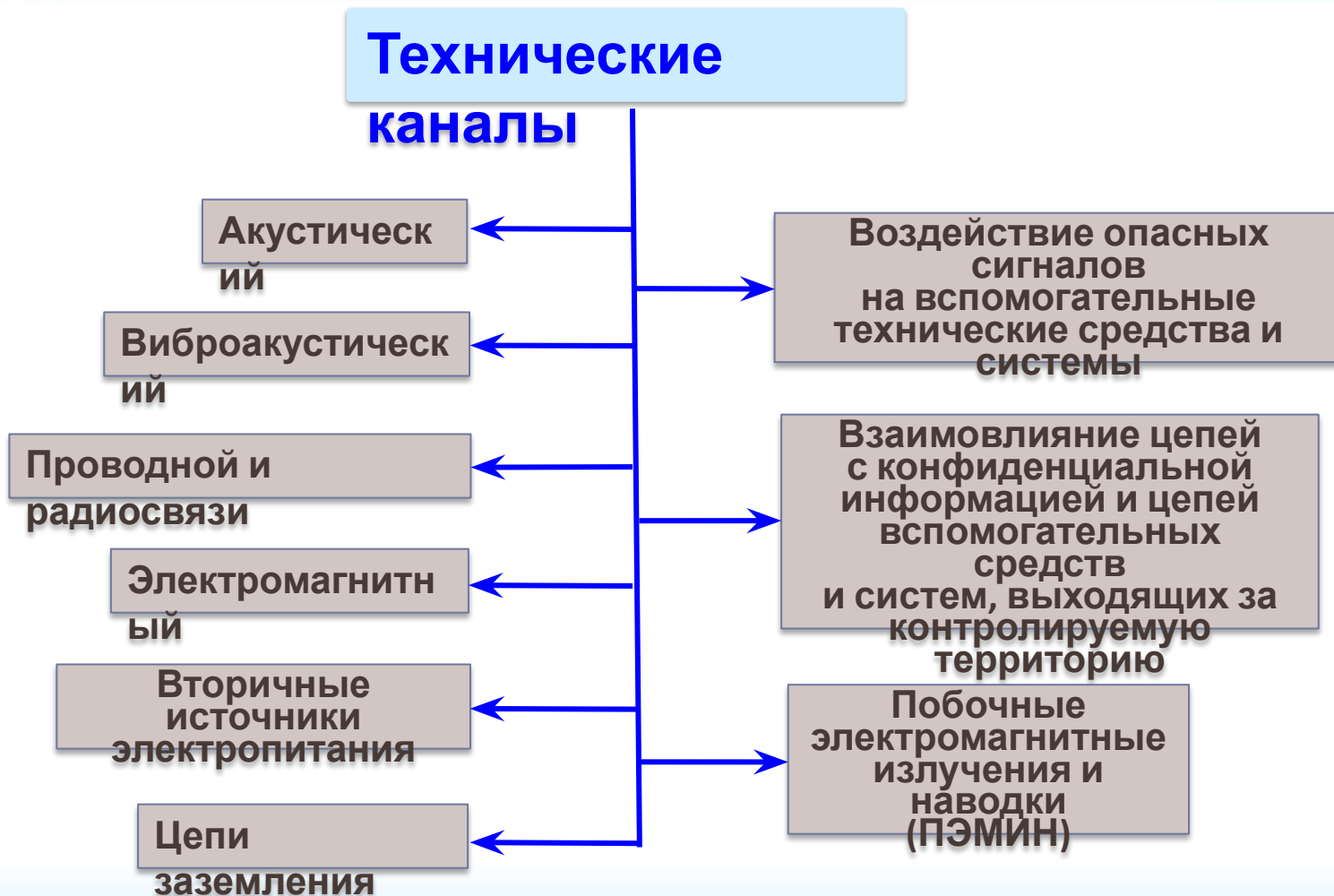
## Технический канал утечки информации

**Совокупность физических полей, несущих конфиденциальную информацию, конструктивных элементов, взаимодействующих с ними, и технических средств злоумышленника для регистрации поля и снятия информации**

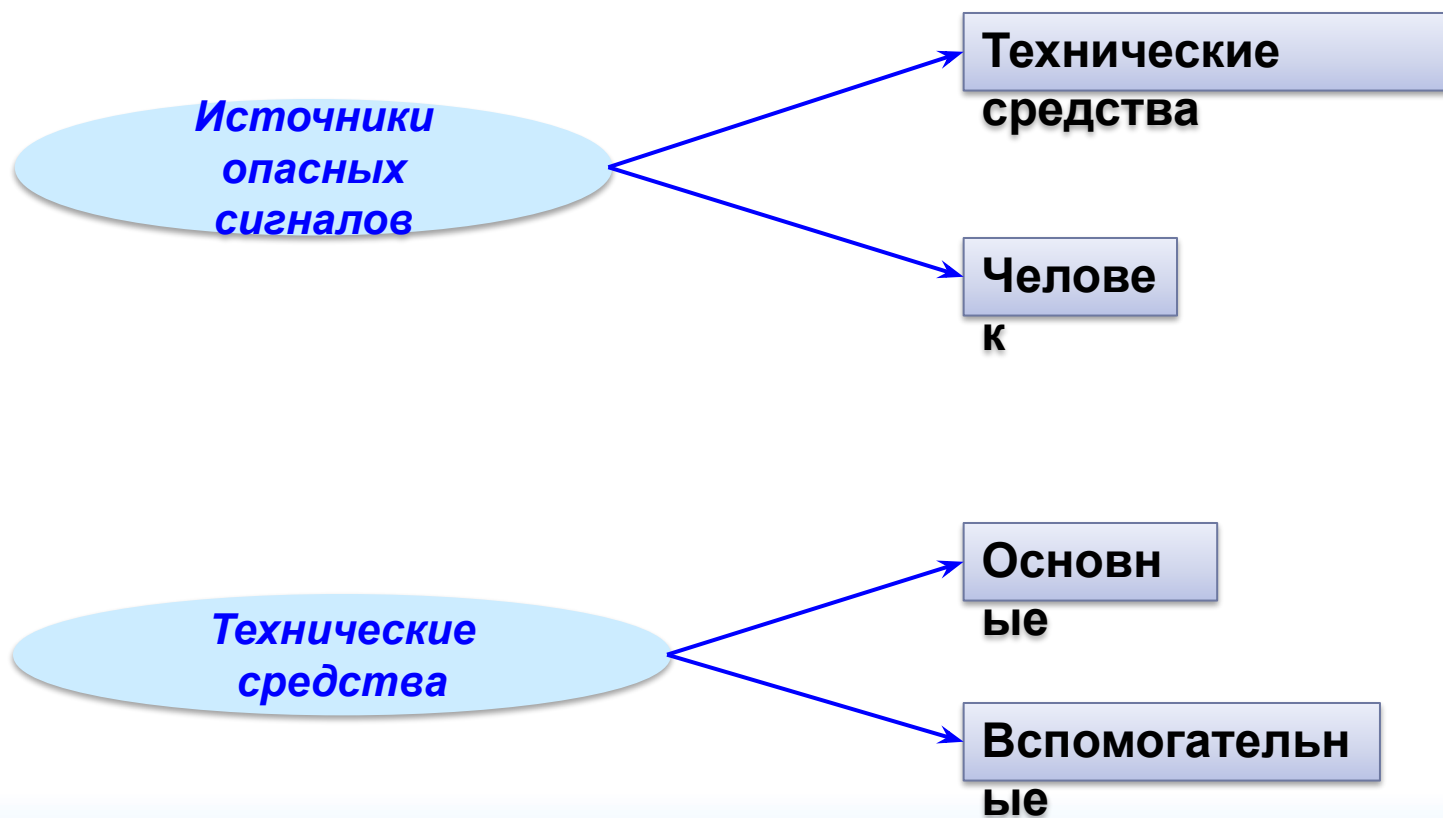
## Опасные сигналы

**Акустические, виброакустические, электрические и электромагнитные сигналы, представляющие конфиденциальную информацию**

# Виды технических каналов



# Виды технических каналов





# Виды технических каналов

## Основные технические средства

- ✓ Персональные ЭВМ с периферийным оборудованием, сети ЭВМ
- ✓ Телефонные аппараты городской АТС
- ✓ Телефонные аппараты местной АТС
- ✓ Радиотелефоны и сотовые телефоны
- ✓ Селекторная связь
- ✓ Телефакс
- ✓ Телетайп
- ✓ Средства размножения документов



# Виды технических каналов

## **Вспомогательные технические средства**

- ✓ Радиоаппаратура
- ✓ Радиотрансляционный громкоговоритель
- ✓ Датчики охранной и пожарной сигнализации
- ✓ Табельное электрооборудование помещений
- ✓ Кондиционеры



# Возможности злоумышленника

## Контроль акустической информации





# Возможности злоумышленника

## Контроль акустической информации

Электронный контроль речи

Использование радиоканала

Использование линий электропитания

Радиоканал

Закамуфлированные радиопередатчики

Линии электропитания

Передача сигнала с помощью ультразвука





# Возможности злоумышленника

## Контроль информации в каналах телефонной связи

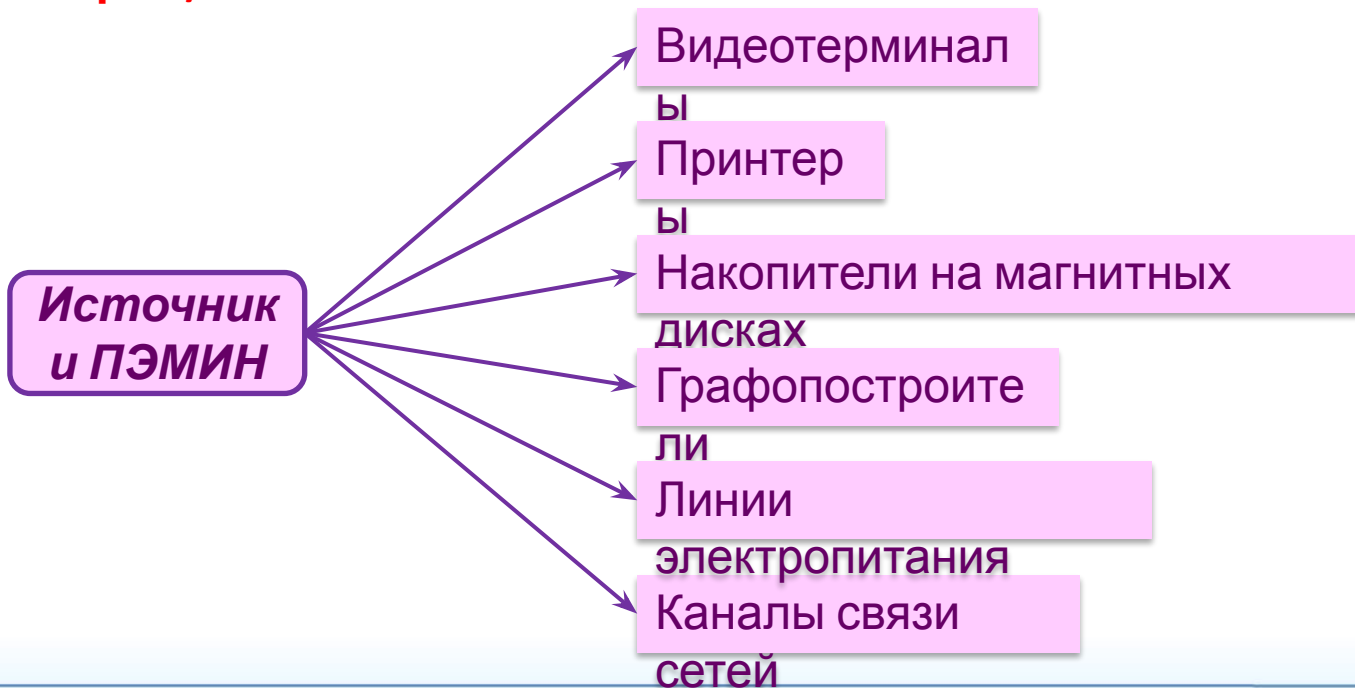
- ✓ Непосредственное подключение к телефонной линии
- ✓ Негальваническое подключение к телефонной линии (индуктивное)
- ✓ Использование микропередатчика с питанием от телефонной линии (подключается в любом месте от аппарата до АТС)
- ✓ Прослушивание помещений с помощью кодового микрофонного усилителя (встраивается в телефонный аппарат)
- ✓ Прослушивание помещений с помощью микрофона телефонного аппарата (модуляция высокочастотного сигнала сигналами от микрофона или корпуса телефонного аппарата)
- ✓ Прослушивание помещений с использованием телефонных аппаратов, содержащих электромагнитный звонок (в цепи звонка есть модулированный ток)
- ✓ Прослушивание телефонных разговоров, ведущихся по радиотелефонам или



# Возможности злоумышленника

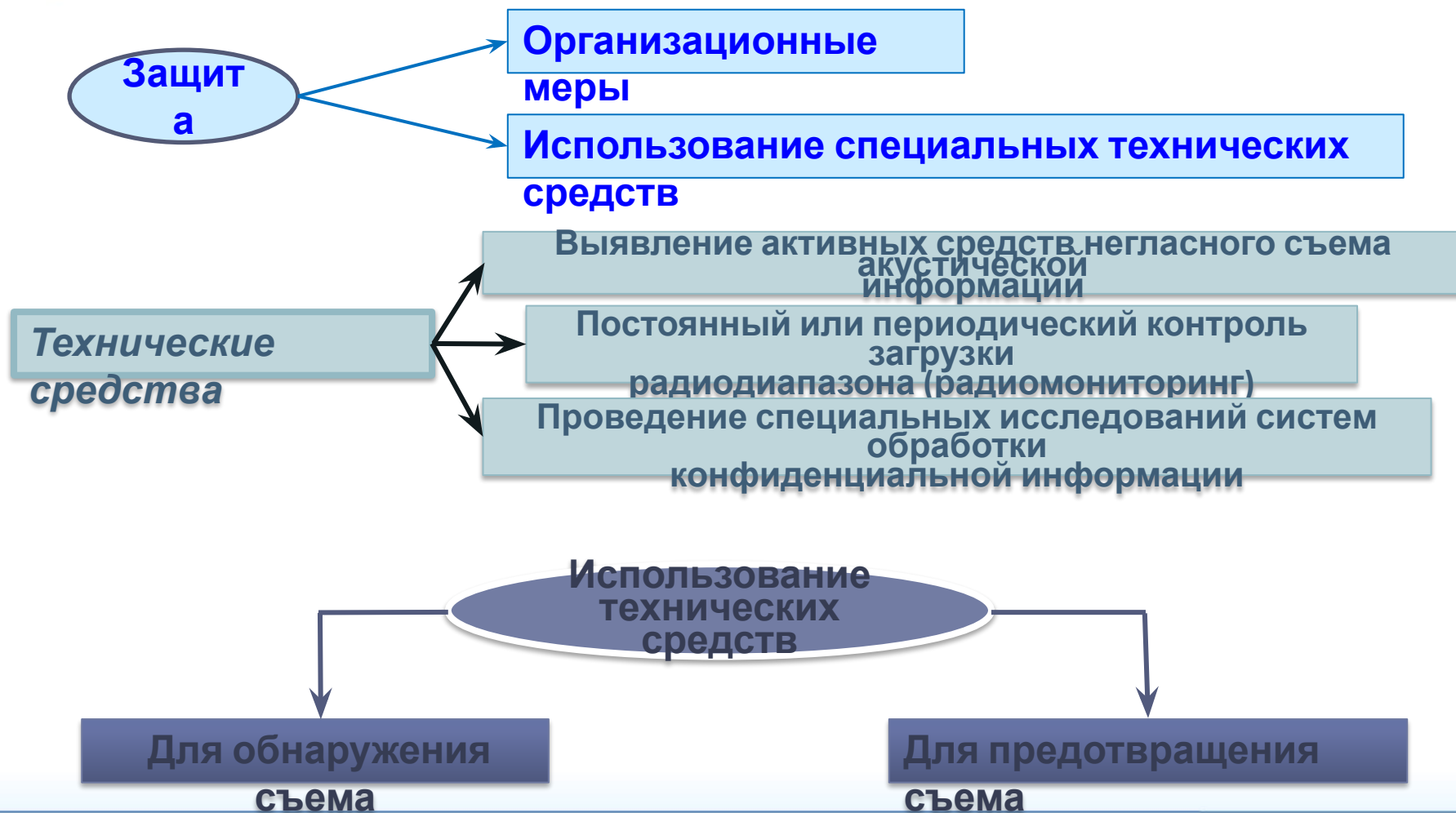
Контроль информации,  
обрабатываемой средствами вычислительной  
техники

**Перехват ПЭМИН (на расстоянии до нескольких сотен метров)**





# Способы предотвращения утечки информации по техническим каналам





# Способы предотвращения утечки информации по техническим каналам

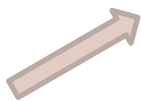
## Акустический канал

Обнаружение съема



*Достаточно сложно (практически можно обнаружить только работающие диктофоны)*

Обнаружение съема (электронный контроль речи)



*Поиск и контроль по электромагнитному излучению – работающие устройства*



*Аппаратура пассивного обнаружения – независимо от режима работы обнаруживаемых устройств (нелинейные локаторы, эндоскопы, дефектоскопы, металлоискатели, тепловизоры и т.п.)*

Предотвращение съема



*Генераторы аудиопомех (от миниатюрных до стационарных)*



# Способы предотвращения утечки информации по техническим каналам

## Каналы

### связи

Установление факта подключения к телефонным каналам подслушивающих устройств

Обнаружение съема

Спектральный анализ каналов связи

Предотвращение съема

Аналоговое скремблирование

Изменение характеристик речевого сигнала без изменения полосы частот

Дискретизация с последующим шифрованием

Исходный сигнал

АЦП

Исходный сигнал

Модем (ЦАП)

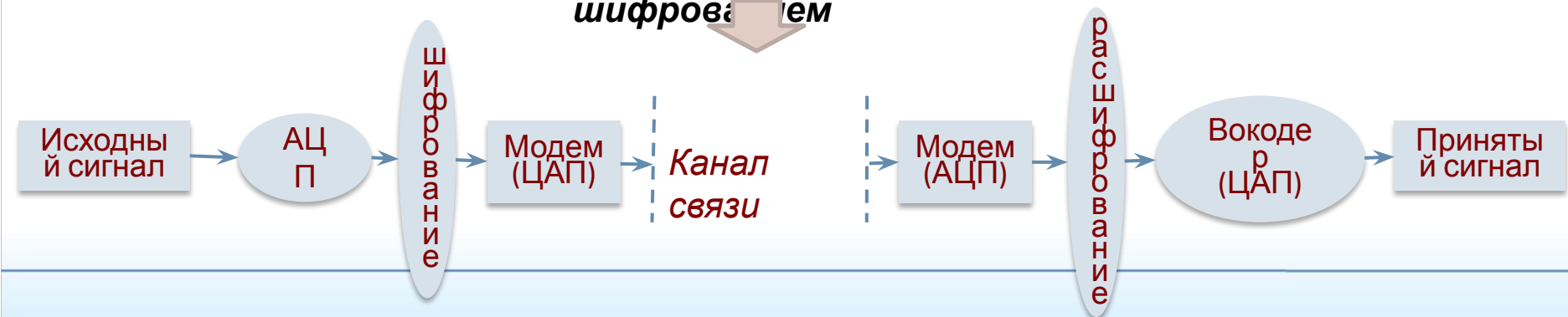
Канал связи

Модем (АЦП)

Исходный сигнал

Вокодер (ЦАП)

Принятый сигнал





# Способы предотвращения утечки информации по техническим каналам

## Канал ПЭМИН

Обнаружение  
съема



*Обнаружение техническими  
средствами  
невозможно*

Предотвращение  
съема



*Пассивная  
защита*

*Активная  
защита*



# Способы предотвращения утечки информации по техническим каналам

## Канал

## ПЭМИН

Пассивная

защита



*Размещение всего оборудования в экранирующей радиоизлучения среде (применимо только для малогабаритной аппаратуры)*



*Экранирование отдельных компонентов защищаемых систем, применение в линиях связи и питания различных фильтров, устройств подавления сигналов и*

**Допустимые уровни излучений аппаратуры и меры защиты информации**

**регламентируются специальными стандартами. Стоимость оборудования,**

**отвечающего стандартам, в 3-5 раз выше стоимости**

**соответствующего**

**незащищенного варианта.**



# Способы предотвращения утечки информации по техническим каналам

## Канал ПЭМИН Активная

Соккрытие информационных сигналов за счет шумовой или заградительной помехи с помощью специальных генераторов шума  
(радиомаскировка)

**Энергетическая**  
(экологически  
опасная)

**Широкий спектр**  
**Большая**  
**мощность**

**Неэнергетическая**  
(статистическая)

**Изменение вероятностной**  
**структуры**  
**сигнала, который может быть**  
**принят**  
**злоумышленником**