Московский Университет имени С.Ю.Витте

QUI NON PROFICIT, DEFICIT

Московский университет имени С. Ю. Витте

«Информационная безопасность. Состояние и перспективы развития»

Доцент кафедры математики и информатики

ктн Зайцев Михаил Алексеевич

1. НОРМАТИВНО - ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И СПОСОБЫ ИХ ЗАКРЫТИЯ

3. ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

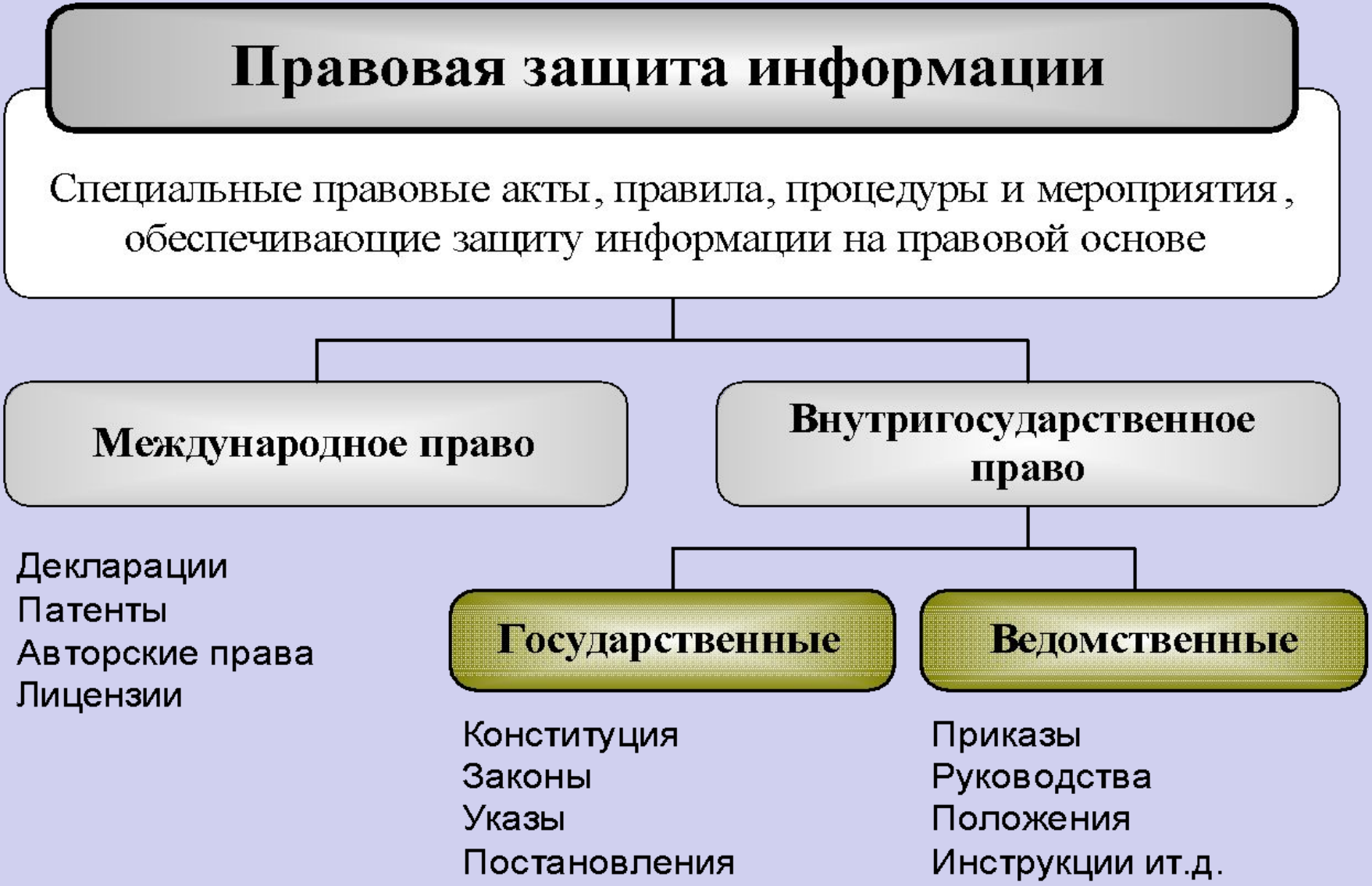
4. ПОНЯТИЕ ПРОГРАММНО – МАТЕМАТИЧЕСКОГО ВОЗДЕЙСТВИЯ И ВРЕДОНОСНОЙ ПРОГРАММЫ.

Литература:

1. Л.Л. Попов, Ю.И. Мигачев, С.В. Тихомиров «Информационное право», учебник, 2010 г.
2. С.Н. Семкин, А.Н. Семкин «Основы правового обеспечения защиты информации», учебное пособие для вузов, М.: Горячая линия – Телеком, 2008 г.
3. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. Учебник для вузов. – М.: ООО «Изд-во Машиностроение», 2009 – 508 с.
4. Хорев А.А. Техническая защита информации. Учебное пособие. М.: «Аналитика», 2008.

Структура основных органов государственной власти, решающих задачи в области ЗИ

СТРУКТУРА ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ



СИСТЕМА ДОКУМЕНТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Правовые документы по технической защите информации

Конституция Российской Федерации
Федеральные законы (Законы Российской Федерации)
Указы и распоряжения Президента Российской Федерации
Постановления Правительства Российской Федерации

Организационно-распорядительные документы по технической защите информации

Концепции
Положения

Специальные нормативные документы по технической защите информации

Государственные стандарты
Специальные нормативные документы

ФЕДЕРАЛЬНЫЕ ЗАКОНЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

«О безопасности»	Закон РФ от 28 декабря 2010 года № 390-ФЗ
«О государственной тайне»	Закон РФ от 21 июля 1993 года № 5485-I(с изменениями и дополнениями от 6 октября 1997 г. № 131-ФЗ; от 2003 г. № 86-ФЗ; от 2003 г. № 153-ФЗ; от 2004 г. № 58-ФЗ; от 2004 г. № 122-ФЗ)
«О лицензировании отдельных видов деятельности»	Федеральный закон от 4 мая 2011 года № 99-ФЗ
Кодекс Российской Федерации об административных правонарушениях	От 30 декабря 2001 года № 195-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 30 июня 2003 г. №86-ФЗ)
Уголовный кодекс Российской Федерации	От 13 июня 1996 года № 63-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 8 декабря 2003 г. №162-ФЗ)
«Об электронной цифровой подписи»	Федеральный закон от 6 апреля 2011 года № 63-ФЗ
«О техническом регулировании»	Федеральный закон от 27 декабря 2002 года № 184-ФЗ (с изменениями и дополнениями от 9 мая 2005 г. № 45-ФЗ)
«Об информации, информационных технологиях и о защите информации»	Федеральный закон от 27 июля 2006 года № 149-ФЗ
«О персональных данных»	Федеральный закон от 27 июля 2006 года № 152-ФЗ
«О коммерческой тайне»	Федеральный закон от 29 июля 2004 года № 98-ФЗ

ФЗ РФ «О КОММЕРЧЕСКОЙ ТАЙНЕ»

- ***Коммерческая тайна*** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

- ***Информация, составляющая коммерческую тайну*** (секрет производства), - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

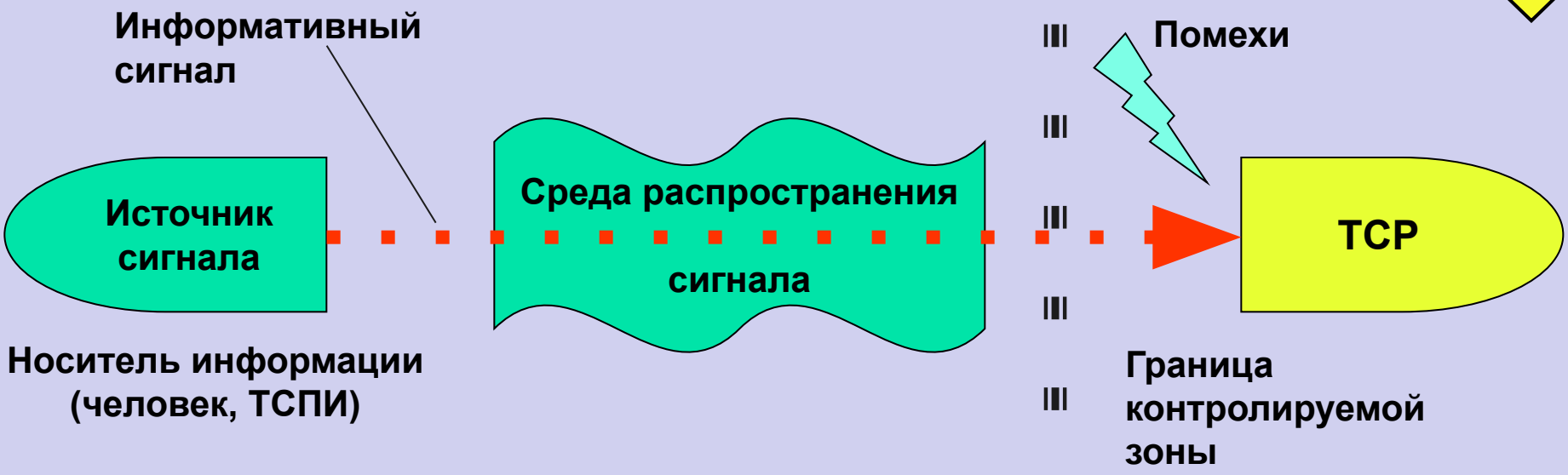
- ***Обладатель информации,*** *составляющей коммерческую тайну* – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайне.

- ***Доступ к информации****, составляющей коммерческую тайну* - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

- ***Разглашение информации, составляющей коммерческую тайну*** – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, или иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

ОБЩАЯ КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И СПОСОБЫ ИХ ЗАКРЫТИЯ



Технический канал утечки информации

совокупность носителя информации, технического средства, с помощью которого осуществляется перехват информации, и физической среды распространения информативного сигнала.

Носитель информации:
Материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин
Информативный сигнал
сигнал, по параметрам которого может быть определена защищаемая информация.

Классификация технических каналов утечки информации

Технические каналы утечки информации

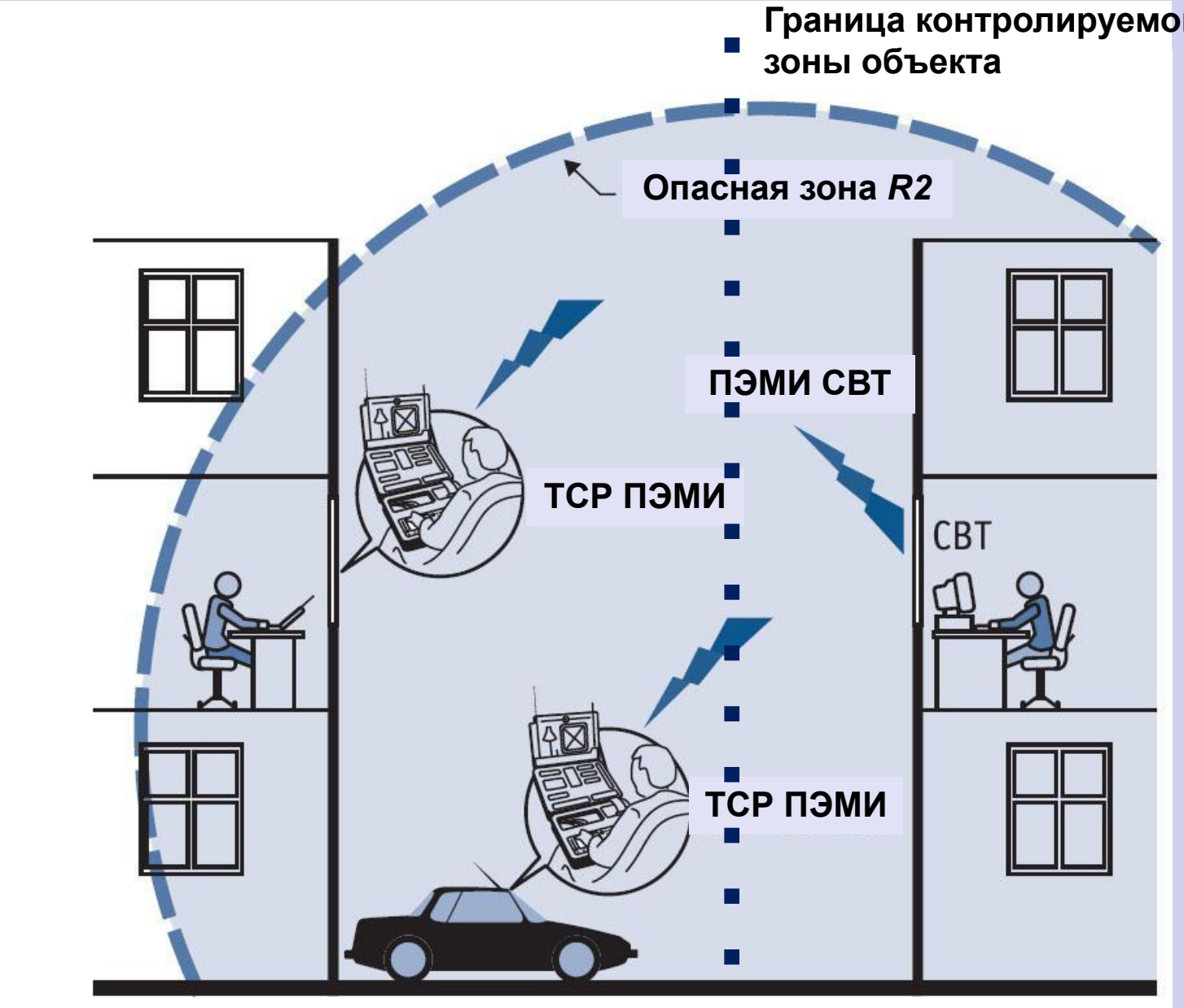
Технические каналы утечки информации, обрабатываемой техническими средствами

- возникающие за счет ПЭМИ;
- возникающие за счет наводок ПЭМИ;
- создаваемые путем «высокочастотного облучения» ТСПИ.
- создаваемые путем внедрения в ТСПИ закладных устройств

Технические каналы утечки речевой информации из выделенных помещений

- прямые акустические;
- акустовибрационные;
- акустооптический (лазерный);
- акустоэлектрические;
- акустоэлектромагнитные.

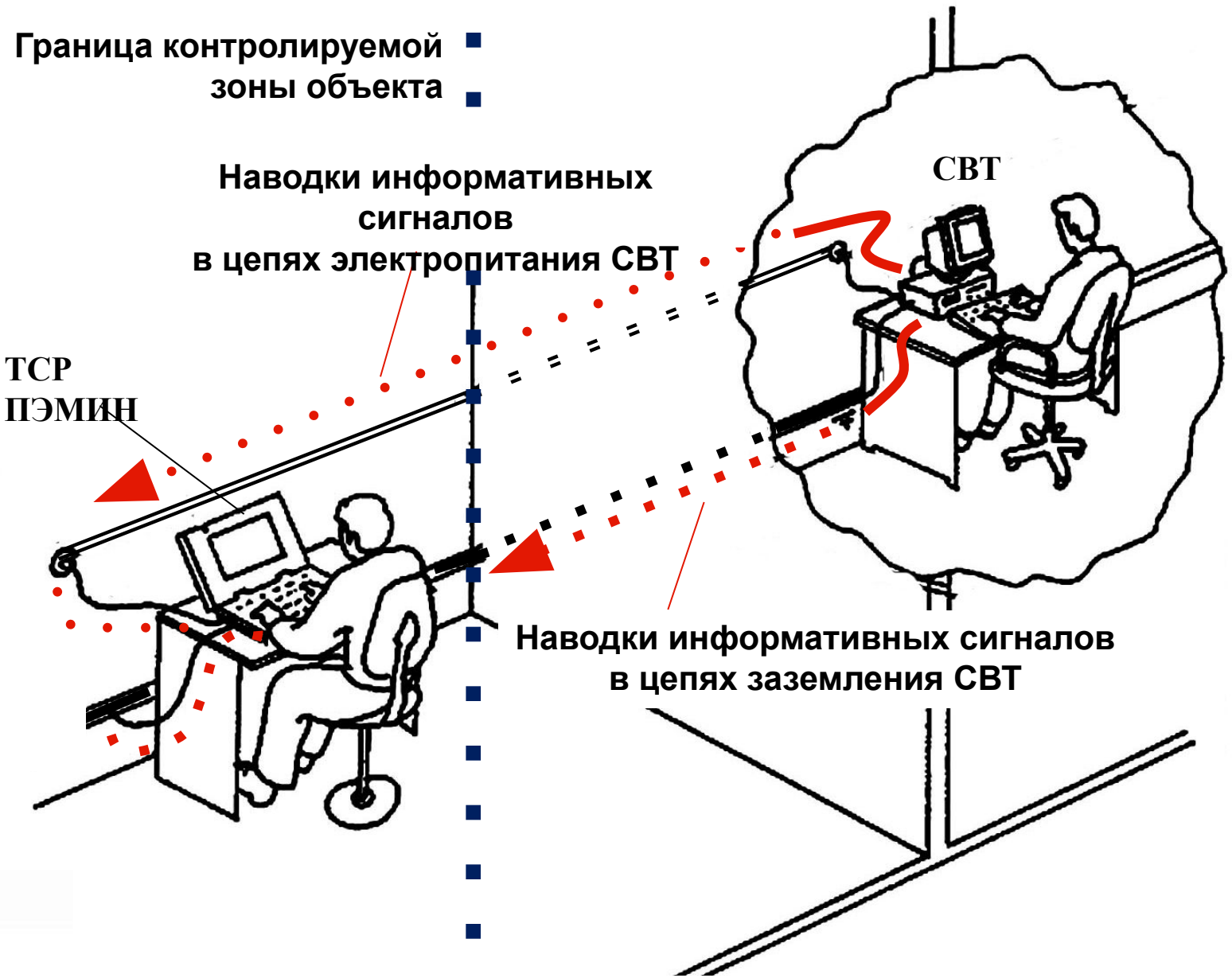
Технические каналы утечки видовой информации (скрытое видеонаблюдение и съемка)



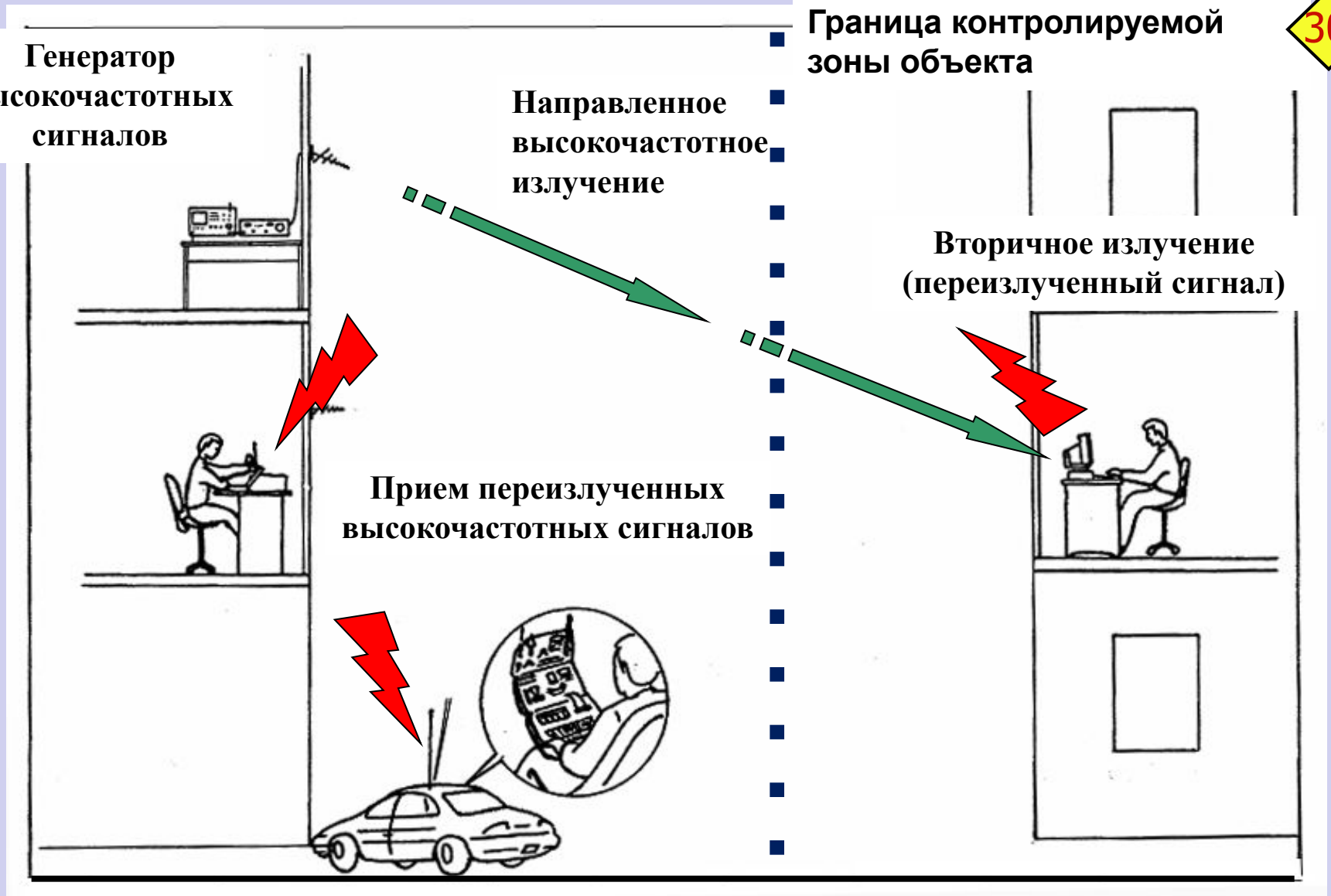
Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН

(электромагнитный канал утечки информации)

Перехват наведенных информативных сигналов с инженерных коммуникаций



Перехват наведенных информационных сигналов с цепей заземления и электропитания ТСПИ



Перехват информации, обрабатываемой СВТ, методом «высокочастотного облучения» СВТ

Стационарный комплекс приема информации

Излучение аппаратной радиозакладки

Мобильный комплекс приема информации

Перехват информации путем внедрения СВТ электронных устройств перехвата информации (закладных устройств)

Способы перехвата речевой информации из выделенных помещений по прямому акустическому каналу

Без проникновения в пределы контролируемой зоны (КЗ) объекта

Перехват акустических колебаний, возникающих при ведении разговоров, направленными микрофонами, размещенными за пределами КЗ в ближайших строениях или транспортных средствах

Перехват акустических колебаний, возникающих при ведении разговоров, скрытно установленными в выделенных помещениях закладными устройствами (с датчиками микрофонного типа), передающими информации по:

- радиоканалу;
- оптическому каналу (в ИК-диапазоне);
- специально проложенному кабелю;
- сети электропитания 220 В;
- телефонной линии и т.д.

С проникновением в пределы контролируемой зоны (КЗ) объекта

Прослушивание разговоров без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами, при их нахождении в коридорах или смежных помещениях (*непреднамеренное прослушивание*)

Запись речевой информации цифровыми диктофонами, скрытно установленными в выделенных помещениях

Защита информации от утечки по техническим каналам на объектах информатизации (объектах ТСПИ) достигается:

- проведением организационно-режимных мероприятий;
- использованием специальных технических средств защиты ТСПИ;
- выявлением электронных устройств перехвата информации (закладных устройств), внедренных в ТСПИ.

Организационное мероприятие – это мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств защиты.

Техническое мероприятие – это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений.

Выявление закладных устройств осуществляется проведением специальных обследований объектов ТСПИ, а также специальных проверок ТСПИ.

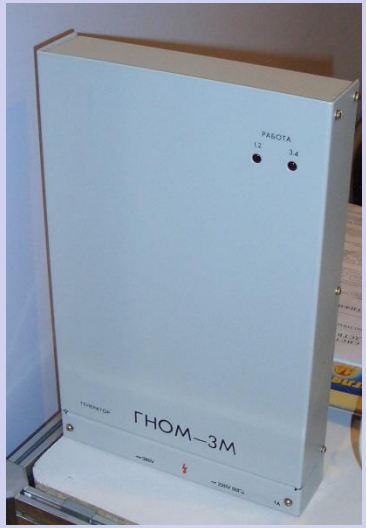
Специальные обследования объектов ТСПИ проводятся путём визуального осмотра помещений и ТСПИ без применения технических средств.

Специальная проверка ТСПИ проводится с использованием специальных технических средств.

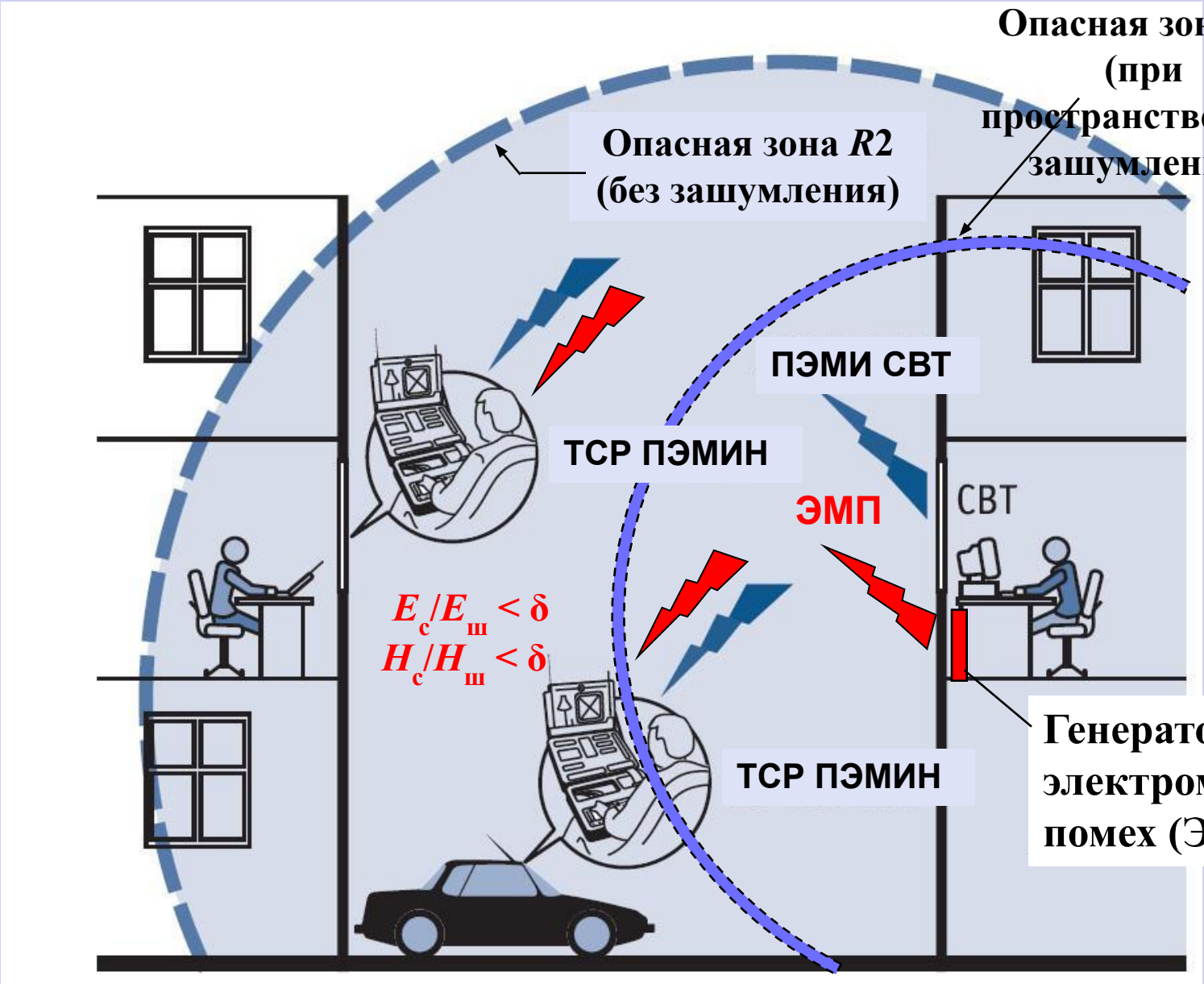
Защита объектов ТСПИ от утечки информации, возникающей за счет побочных электромагнитных излучений, достигается: экранированием и заземлением технических средств и их соединительных линий, экранированием помещений, а также использованием систем пространственного электромагнитного зашумления.

Защита объектов ТСПИ от утечки информации, возникающей за счет наводок побочных электромагнитных излучений, достигается: установкой помехоподавляющих фильтров в цепях электропитания ТСПИ, диэлектрических вставок в инженерные коммуникации и экраны кабелей электропитания, а также использованием систем линейного электромагнитного зашумления.

Генератор шума «Гном – 3»



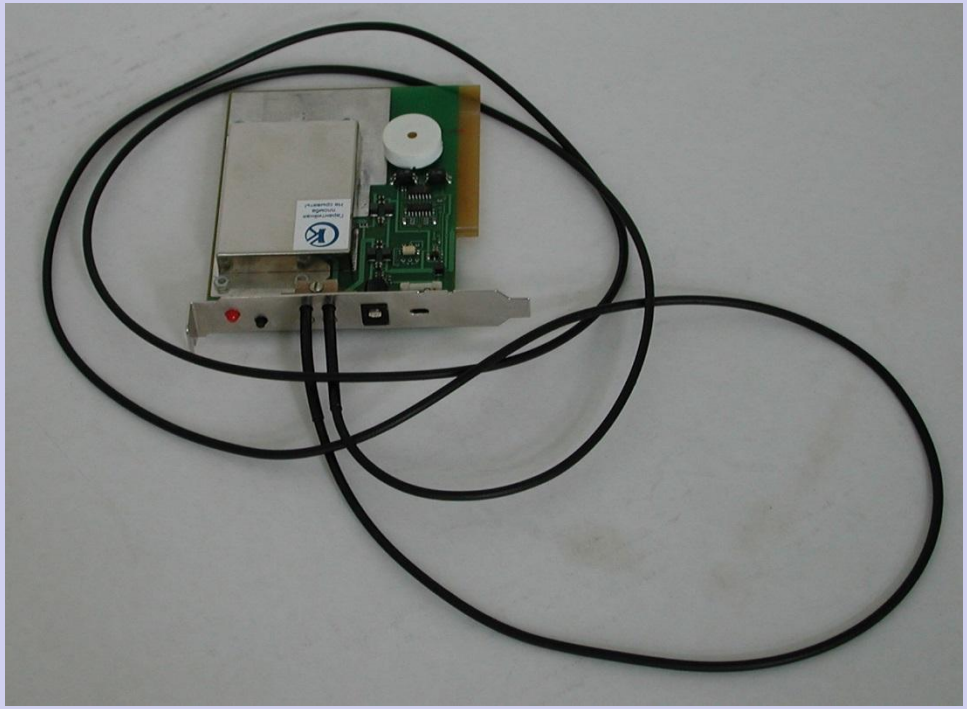
Генератор шума «Гном – 3М»



Пространственное электромагнитное зашумление

Дополнительная антенна

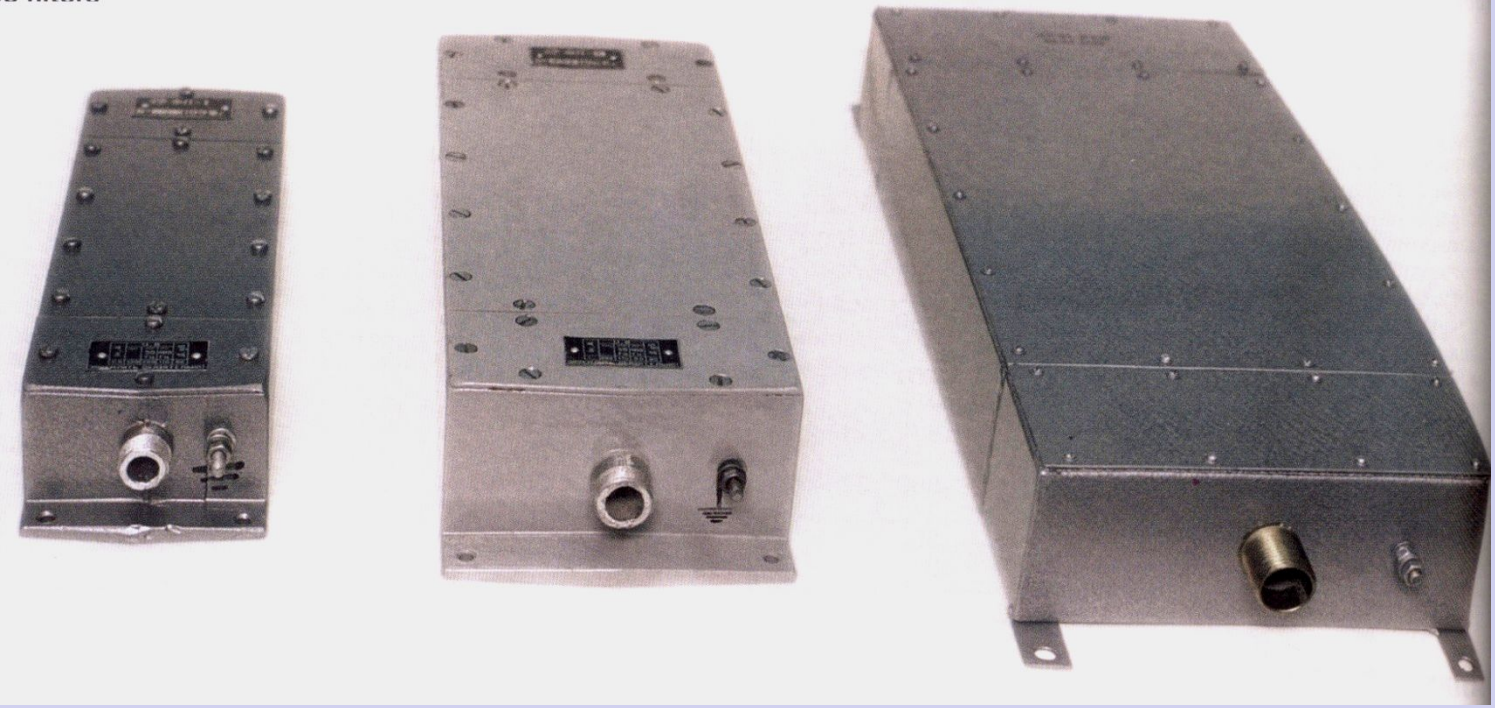
Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН "Соната-Р2"



Генератор шума ГШ – К – 1000М

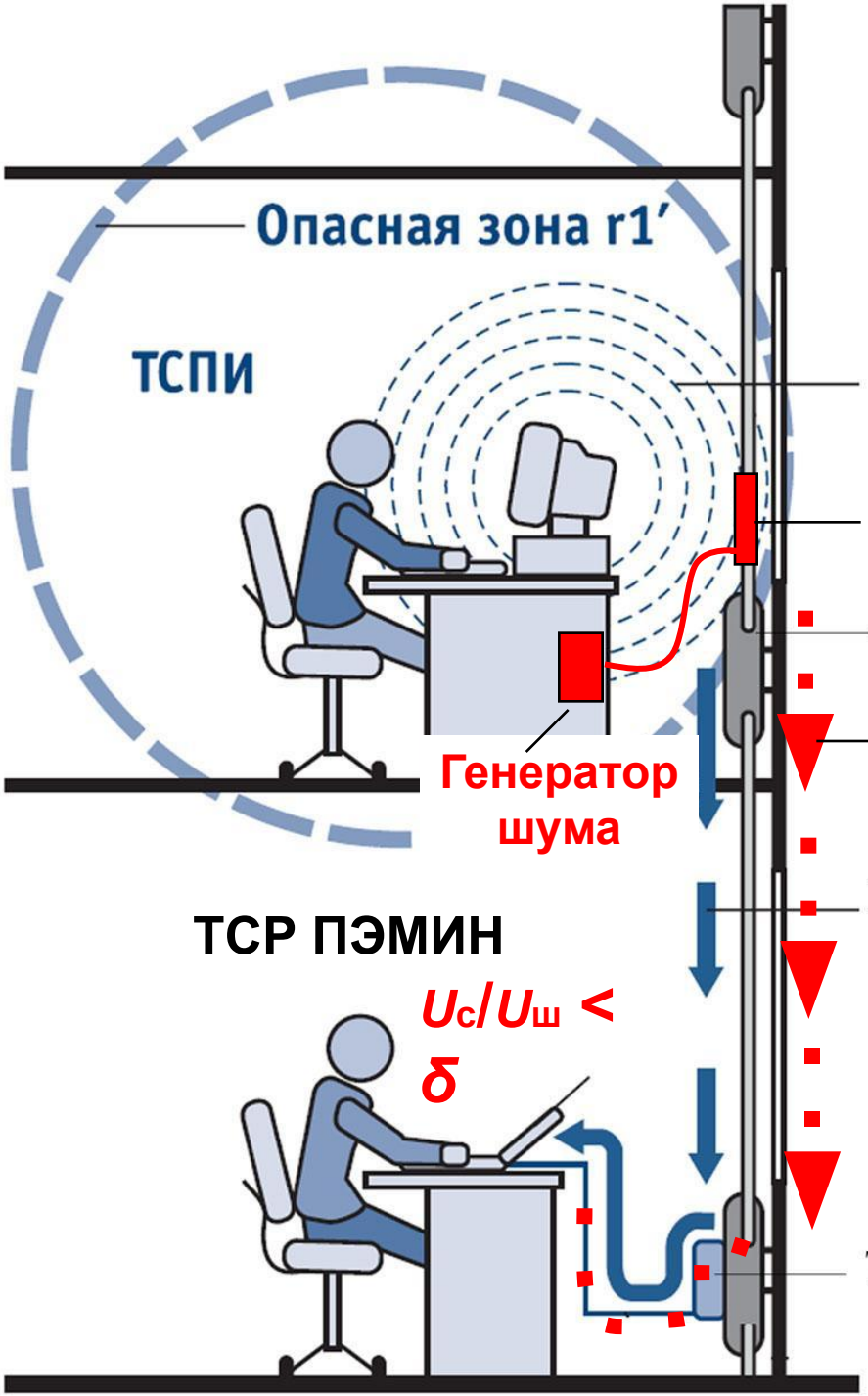
Генератор шума SEL SP - 21

Генератор шума SEL SP - 113



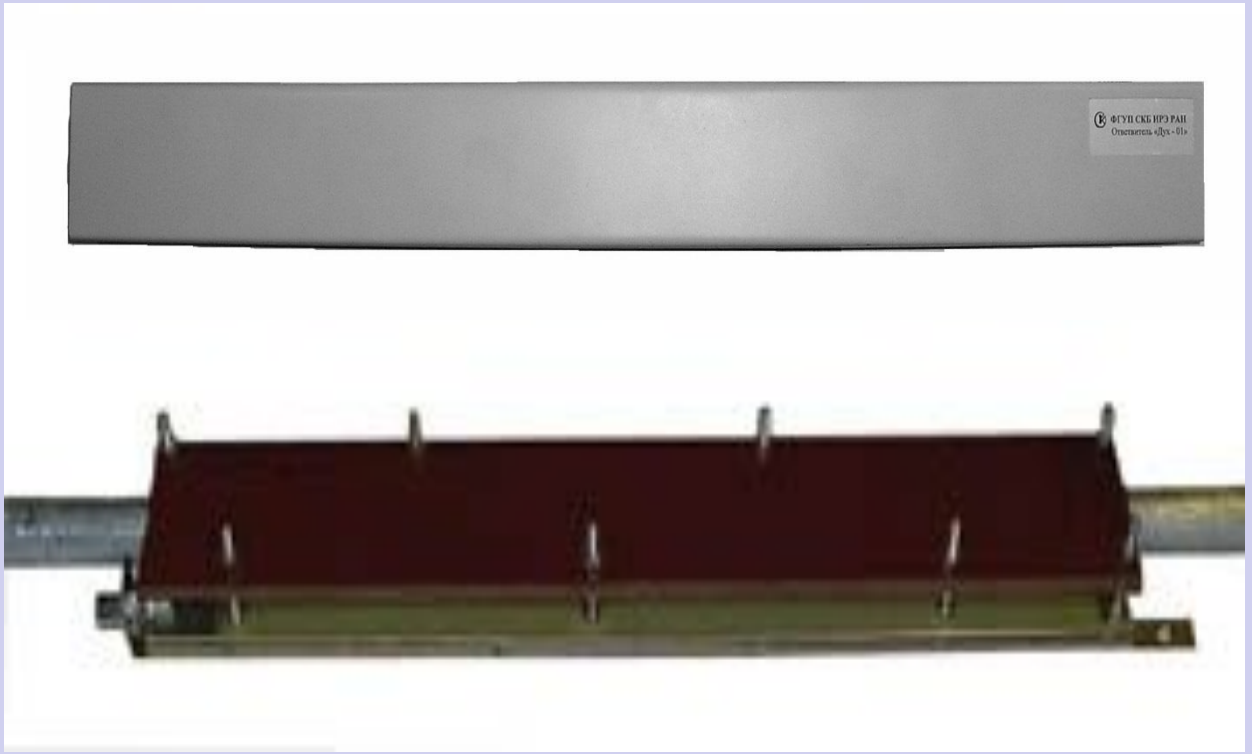
Внешний вид помехоподавляющих фильтров серии ФП

Внешний вид помехоподавляющих фильтров серии ФСПК



Создание шумовых помех в инженерных коммуникациях

Генератор шума ГШ – 1000У



Внешний вид и способ крепления ответвителя «Дух»

Защищенные ПЭВМ «Secret», «Обруч»

ПЭВМ семейства Secret являются модификацией серийных ПЭВМ, доработанных специальным образом для повышения характеристик защищенности обрабатываемой на них информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок (ПЭМИН) и НСД.

ПЭВМ выпускаются в трех модификациях:

1.0 размер зоны 2 по требованиям 2 и 3 категорий не более 5 м, по требованиям 1 категории - не более 800м;
2.0 размер зоны 2 по требованиям 2 и 3 категорий не более 10 м, по требованиям 1 категории - не более 1000 м;
3.0 размер зоны 2 по требованиям 2 и 3 категорий не более 15 м, по требованиям 1 категории - не нормируется.

В состав ПЭВМ включается фильтр-генератор для защиты цепей питания и заземления, который обеспечивает гарантированную защиту для сетей с изолированной и глухозаземленной нейтралью, а также в случае отсутствия защитного заземления.

Пассивные способы защиты речевой информации в выделенных помещениях (ВП)

Звукоизоляция ВП

- Звукоизоляция ограждающих конструкций.
- Звукоизоляция дверей.
- Звукоизоляция окон.
- Звукоизоляция воздуховодов.

Установка специальных упругих виброизолирующих прокладок в трубопроводы, выходящие за пределы контролируемой зоны

Экранирование ВП

Подавление сигналов сетевых закладок

- Установка фильтров нижних частот в линиях электропитания ВП

Подавление опасных сигналов в линиях ВТСС

- Установка в соединительных линиях ВТСС фильтров нижних частот

Ограничение опасных сигналов в линиях ВТСС

- Установка в соединительных линиях ВТСС ограничителей сигналов малой амплитуды

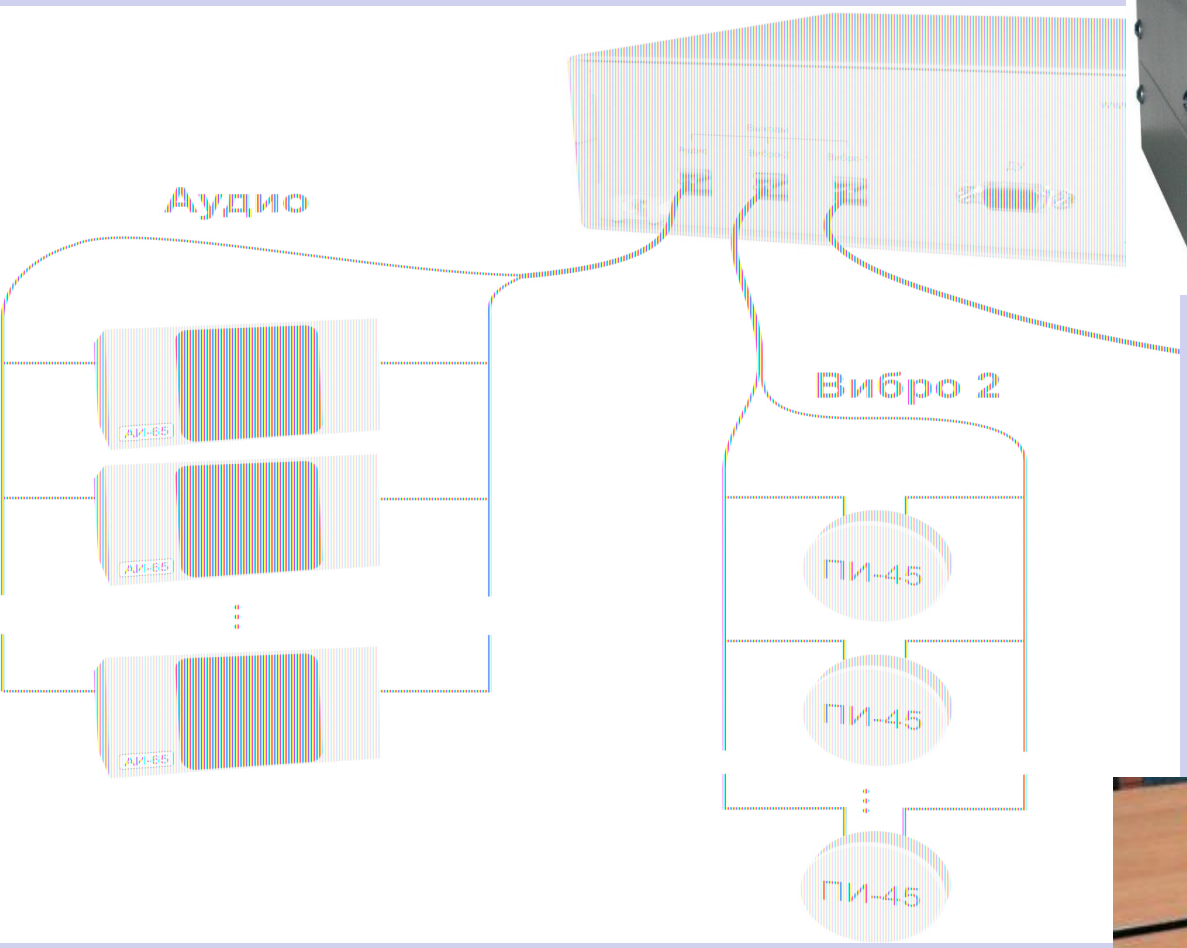
Отключение ВТСС от линии

- Установка в соединительных линиях ВТСС устройств защиты, отключающих преобразователи (источники) опасных сигналов от линии

Активные способы защиты речевой информации

- Виброакустическая маскировка
  - Создание маскирующих акустических помех в воздуховодах и дверных тамбурах
  - Создание маскирующих вибрационных помех в ограждающих конструкциях, окнах, инженерных коммуникациях, воздуховодах
- Линейное электромагнитное зашумление
  - Создание низкочастотных маскирующих электромагнитных шумовых помех в соединительных линиях ВТСС
  - Подавление средств перехвата информации, подключаемых к телефонной линии
- Подавление средств перехвата информации
  - Подавление диктофонов в режиме записи
  - Подавление радиозакладок
  - Подавление средств сотовой связи
  - Подавление сетевых закладок

Системы и средства виброакустической маскировки



Излучатели:
а) ВИ-45;
б) ПИ-45;
в) АИ-65

Виброизлучатели: VN - GL; VNT

Схема установки виброизлучателя на трубе

Источники информации для злоумышленника:

- не до конца удаленные файлы;
- файлы подкачки Windows;
- файлы-протоколы, создаваемые пользовательскими программами;
- файлы-протоколы, создаваемые клавиатурными шпионами.

Изменения, проводимые злоумышленником в аппаратных средствах:

- изменения в базах данных и файлах;
- установка программ-закладок;
- изменение алгоритмов программ;
- изменение аппаратной части;
- изменение режима обслуживания или условий эксплуатации;
- прерывание функционирования аппаратных средств.

Защищаемые ресурсы: системные блоки, платы расширения, клавиатуры, мониторы, рабочие станции, принтеры, дисковые накопители, коммуникационное оборудование, серверы, маршрутизаторы и т.д.

Особенности мероприятий по защите информации:

- Регулярное наблюдение за АС с непредсказуемым графиком;
- Обучение пользователей и администраторов правилам безопасности;
- Смена паролей через определенные промежутки времени.

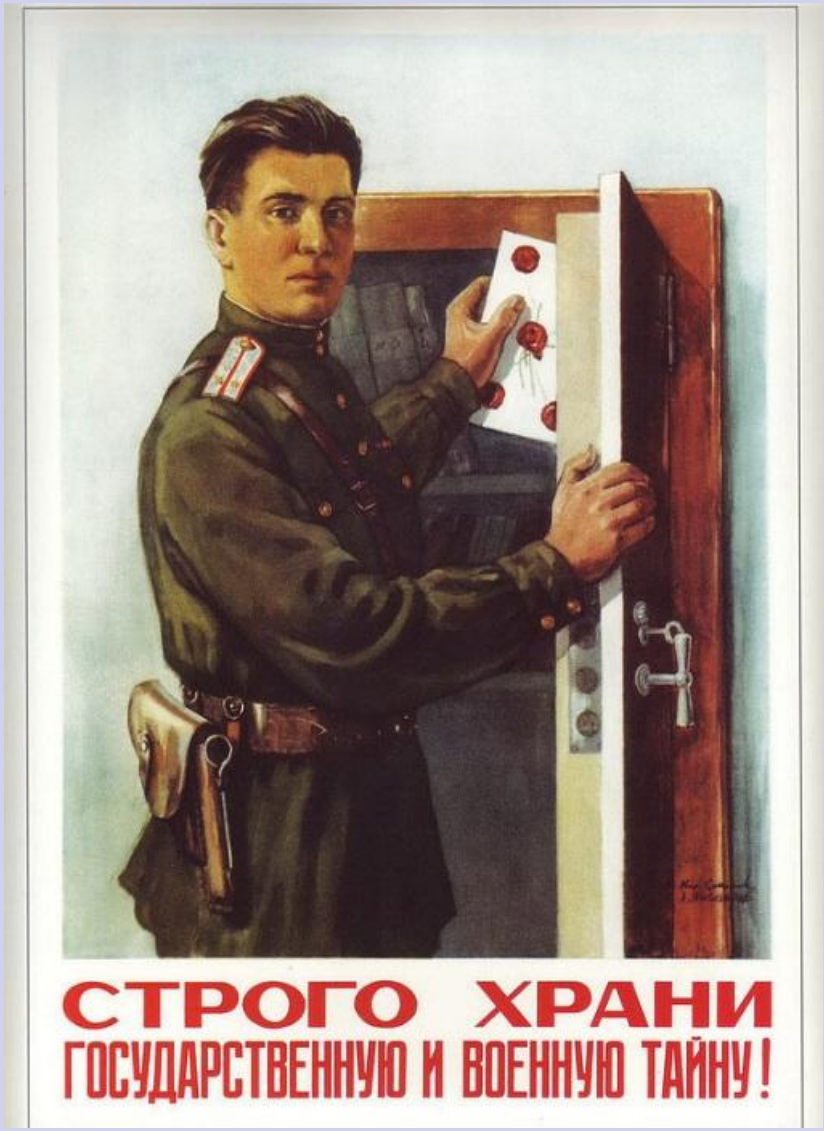
№п/п	Тематическая группа	Частота выбора пароля человеком, %	Раскрываемость пароля, %
1	Номера документов (паспорт, пропуск, удостоверение личности, зачетная книжка, страховой полис и т.п.)	3,5	90
2	Последовательность клавиш ПК, повторяющиеся символы	14,1	72,3
3	Номера телефонов	3,5	66,6
4	Адрес места жительства (или часть адреса – индекс, город, улица и пр.), место рождения	4,7	55,0
5	Имена, фамилии и производные от них	22,2	54,5
6	Дата рождения или знак Зодиака пользователя либо его родственников (возможно, в сочетании с именем, фамилией или производными от них)	11,8	54,5
7	Интересы (спорт, музыка, хобби)	9,5	29,2
8	Прочее	30,7	5,7

Основные правила защиты от сетевых угроз:

1. *крайне осторожно относитесь к программам и документам, изготовленных с помощью пакета Microsoft Office, которые вы получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу/презентацию/базу данных, обязательно проверьте их на наличие вирусов;*
2. *для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети: ограничение прав пользователей; установку атрибутов "только на чтение" или даже "только на запуск" для всех выполняемых файлов; скрытие (закрытие) важных разделов диска и директорий и т.д.;*
3. *приобретать дистрибутивные копии программного обеспечения у официальных продавцов;*
4. *не запускайте непроверенные файлы, особенно полученные из сети. Желательно использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами;*
5. *пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т.д.).*
6. *Периодически сохраняйте на внешнем носителе файлы (backup-копии), с которыми ведется работа.*


НЕ БОЛТАЙ ! СТРОГО ХРАНИ ВОЕННУЮ И ГОСУДАРСТВЕННУЮ ТАЙНУ!


БОЛТАТЬ — ВРАГУ ПОМОГАТЬ!


СТРОГО ХРАНИ
ГОСУДАРСТВЕННУЮ И ВОЕННУЮ ТАЙНУ!