КАЛИНИНГРАДСКИЙ ФИЛИАЛ
САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА МВД РОССИИ

УЧЕБНАЯ ДИСЦИПЛИНА
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ»

ТЕМА 3

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

(С) А.Н. Григорьев, Кафедра административно-правовых дисциплин и информационного обеспечения ОВД КФ СПбУ МВД России

ПЛАН ЛЕКЦИИ

1. Понятие и виды каналов утечки информации на объектах информатизации.
2. Технические каналы утечки информации.
3. Организационная и инженерно-техническая защита информации органов внутренних дел от утечки.

ЛИТЕРАТУРА

1. Григорьев А.Н. Основы информационной безопасности в органах внутренних дел: учебное пособие. – Калининград: Калининградский филиал СПбУ МВД России, 2014. – 236 с.
2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие. – М.; Берлин: Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php? page=book&id=276557. – ЭБС «Университетская библиотека ONLINE», по паролю.
3. Петренко В.И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие. – Ставрополь: СКФУ, 2015. – 222 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=458204. – ЭБС «Университетская библиотека ONLINE», по паролю.

1. ПОНЯТИЕ И ВИДЫ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ОБЪЕКТ ИНФОРМАТИЗАЦИИ – это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

УТЕЧКА ИНФОРМАЦИИ – это неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

РАЗГЛАШЕНИЕ ИНФОРМАЦИИ – это несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ (НСД) – получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Факторы, способствующие утечке информации органов внутренних дел:

– несовершенство правового обеспечения защиты информации в органах внутренних дел;
– нарушение установленных правил защиты информации;
– недостаточность сил и средств для перекрытия каналов утечки информации.

КАНАЛ УТЕЧКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ – физический путь несанкционированного распространения носителя с защищаемой информацией от ее источника к злоумышленнику.

АГЕНТУРНЫЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ – использование противником тайных агентов для получения несанкционированного доступа к защищаемой информации.

Для добывания защищаемой информации через агентуру используются следующие методы:

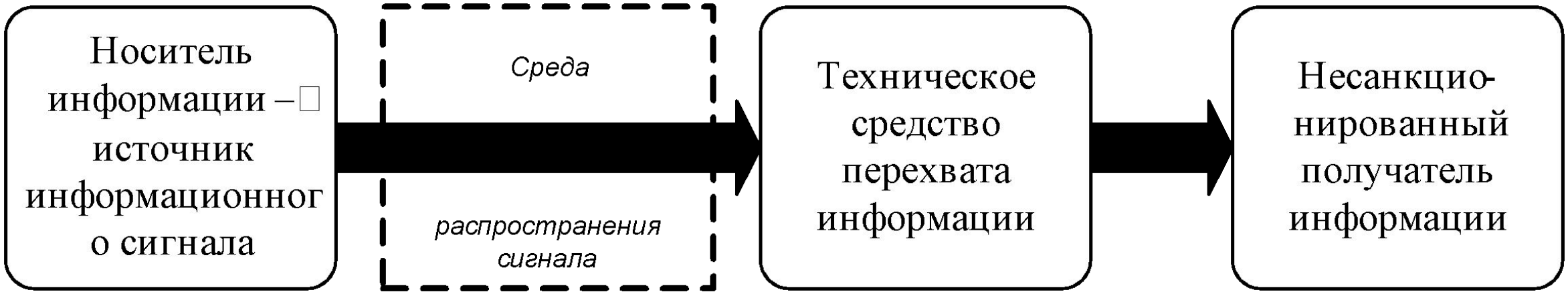
- доступ к конфиденциальной информации по службе;
- выведывание;
- наблюдение.

ЛЕГАЛЬНЫЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ – использование противником открытых источников информации.

Информация, полученная из открытых источников – не имеющая правовых ограничений публично доступная информация (т.е. информация, которую любой желающий может законно получить в результате сделанного запроса, проведенного наблюдения или ознакомления с материалами, распространяемыми по каналам массовой коммуникации), а также другая, не охраняемая в режиме тайны информация, которая имеет ограниченное публичное распространение или доступ.

2. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ – физический путь несанкционированного распространения информации от носителя защищаемой информации до технического средства, осуществляющего перехват информации.



ВИДЫ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ:

- технические каналы утечки информации, обрабатываемой техническими средствами приема и передачи информации;
- технические каналы утечки информации, передаваемой по каналам связи;
- технические каналы утечки речевой информации;
- технические каналы утечки видовой информации.

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ПРИЕМА И ПЕРЕДАЧИ ИНФОРМАЦИИ (ТСПИ)

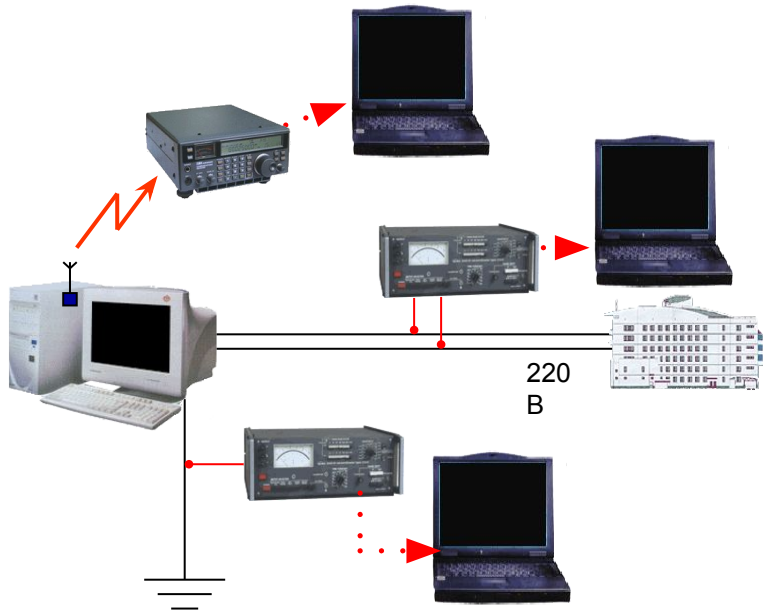
Электромагнитные: перехват побочных электромагнитных излучений (ПЭМИН) элементов ТСПИ.

Электрические:

– съем наводок электромагнитных излучений ТСПИ на соединительные линии и проводники;
– съем информационных сигналов с линий электропитания и цепей заземления ТСПИ;
– съем информации путем установки в ТСПИ аппаратных закладок;

Электромагнитный

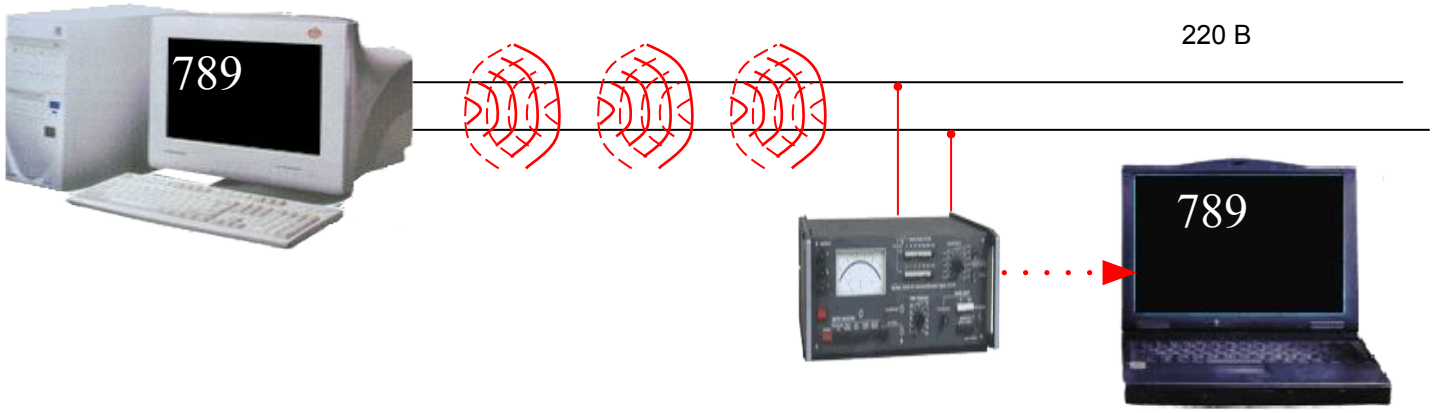
Электрический



ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ПРИЕМА И ПЕРЕДАЧИ ИНФОРМАЦИИ (ТСПИ)

Параметрический: перехват информации путем «высокочастотного облучения» технических средств ее приема и передачи.

Параметрический



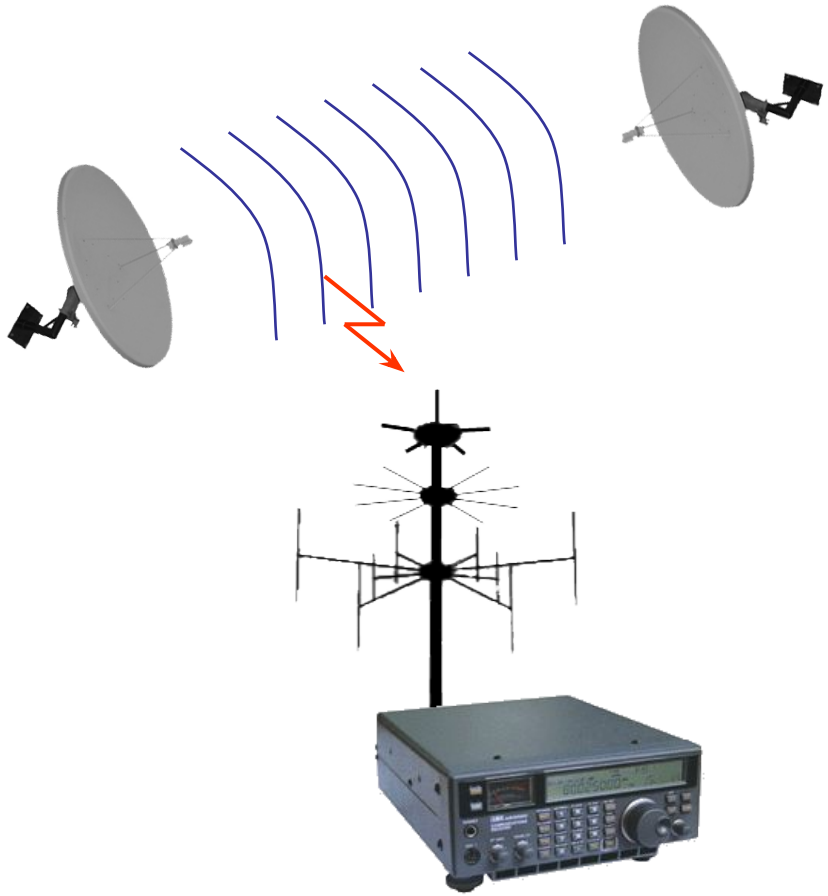
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛАМ СВЯЗИ

Электромагнитный: перехват высокочастотных электромагнитных излучений передатчиков средств связи, модулированных информационным сигналом.

Электрический: несанкционированное контактное подключение к проводным линиям связи и перехват передаваемых по ним информационных электрических сигналов.

Электрический

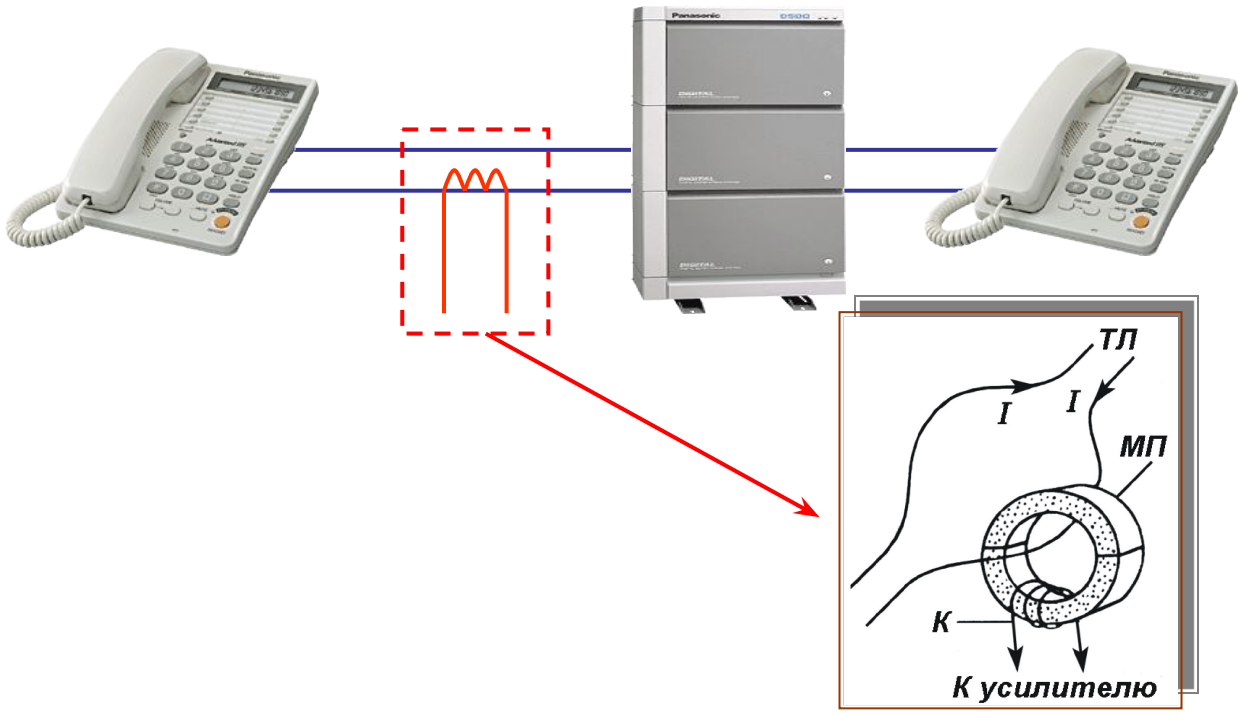
Электромагнитный



ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛАМ СВЯЗИ

Индукционный: детектирование и преобразование электромагнитного поля, возникающего вокруг проводных линий при прохождении по ним электрического информационного сигнала.

Индукционный

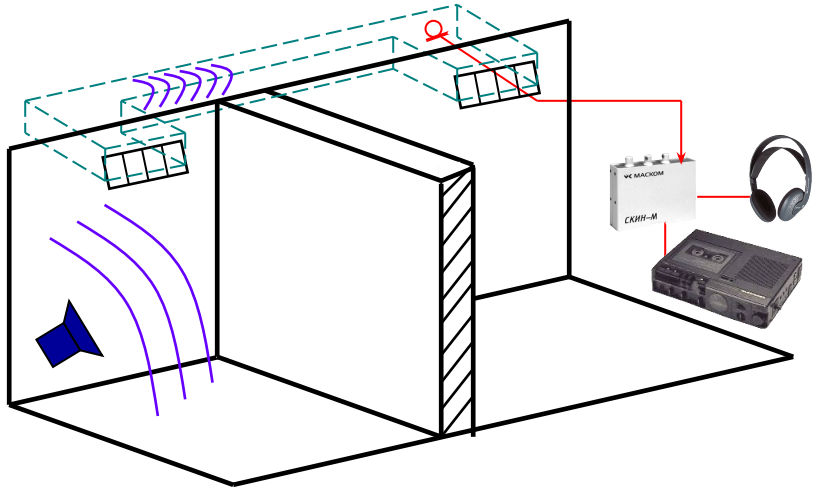


ТЕЧНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ:

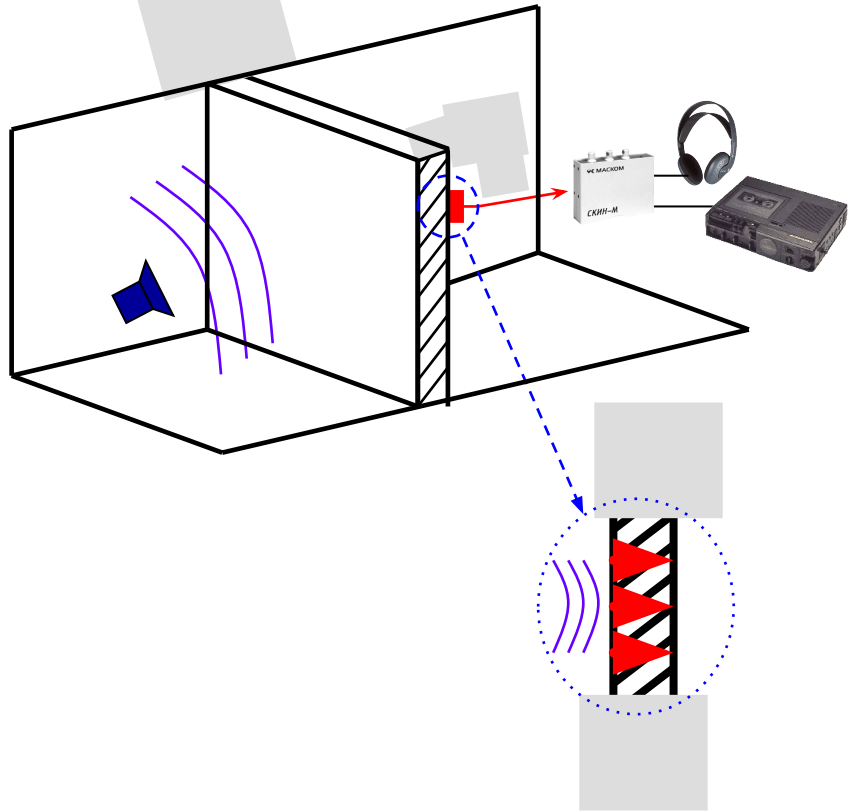
Акустические: перехват акустической информации, распространяющейся в газовых (воздушных) средах с помощью миниатюрных микрофонов, диктофонов и направленных микрофонов.

Виброакустические: перехват речевой информации, распространяющейся по строительным конструкциям и инженерным коммуникациям с помощью электронного стетоскопа.

Акустический



Виброакустический



ТЕХНИЧЕСКИЕ СРЕДСТВА ПЕРЕХВАТА ИНФОРМАЦИИ ПО ВОЗДУШНЫМ И ВИБРАЦИОННЫМ КАНАЛАМ

Акустические радиозакладные устройства

Направленный микрофон

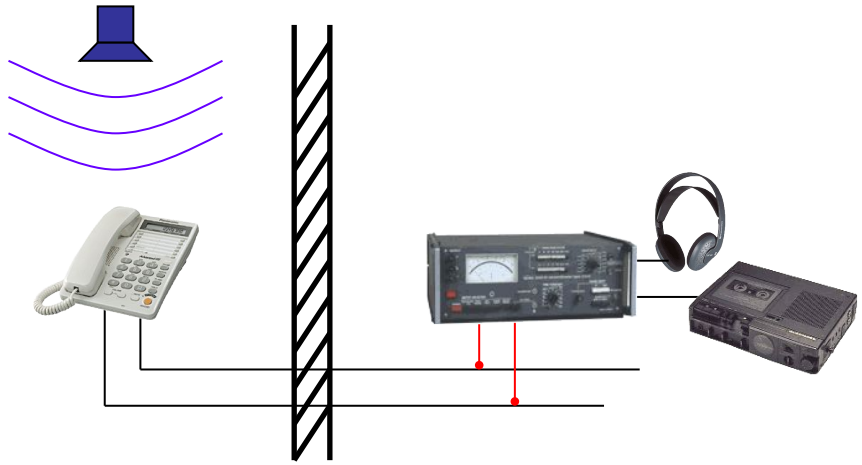
Радиостетоскоп

ТЕЧНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ:

Акустоэлектрические: возникают за счет преобразований акустических сигналов в электрические и включают перехват акустических колебаний через вспомогательные технические средства, обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания».

Параметрический: при взаимодействии акустической волны с элементами различных технических систем происходит изменение их электрических, магнитных и электромагнитных параметров. Эти изменения оказывают влияние на параметры электрических цепей, в которых они выполняют свои функции. За счет эффекта модуляции эти электрические или радиотехнические цепи будут нести информационный сигнал, соответствующий акустическому.

Акустоэлектрический

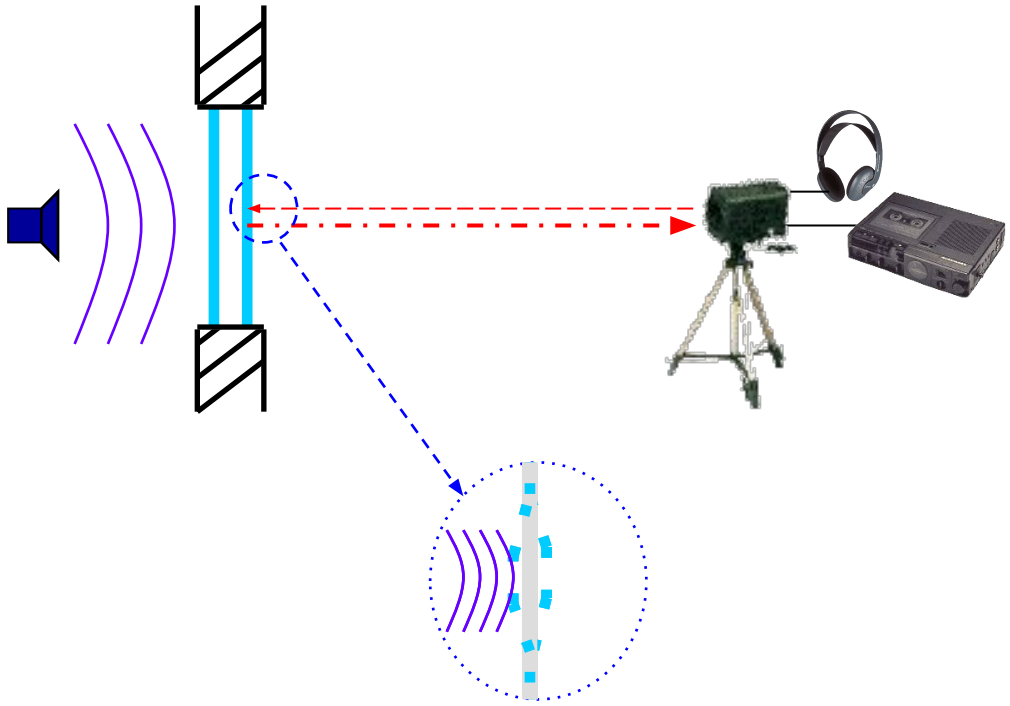


Источник акустического сигнала

Акустическая волна

ТЕЧНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ:

Оптико-электронный: образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, зеркал и т.п.).



ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ

Предполагают получение информации путем:

- визуального наблюдения;
- фото- и видеосъемки.

3. ОРГАНИЗАЦИОННАЯ И ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ ОВД ОТ УТЕЧКИ

Организационные мероприятия – это мероприятия по защите информации, проведение которых не требует применения специально разработанных технических средств защиты.

Основные ***организационные мероприятия по защите информации от утечки по техническим каналам***, проводимые на объектах информатизации ОВД:

- ✔ выбор помещения для установки основных и вспомогательных технических средств и систем;
- ✔ использование только сертифицированных технических средств и систем;
- ✔ установление контролируемой зоны вокруг объекта;
- ✔ отключение на период проведения закрытых совещаний технических средств обладающими качествами электроакустических преобразователей (телефоны, факсы, и т. п.) от соединительных линий;
- ✔ режимное ограничение доступа на объекты размещения основных технических средств и систем и в выделенные помещения;
- ✔ категорирование и аттестация объектов информатизации и выделенных помещений по требованиям безопасности информации.

СЕРТИФИКАЦИЯ – подтверждение соответствия продукции или услуг установленным требованиям или стандартам.

СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ – деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации.

Сертификат на средство защиты информации – документ, подтверждающий соответствие средства защиты информации требованиям по безопасности информации.

Одним из основных руководящих документов по сертификации средств защиты информации является **Положение о сертификации средств защиты информации, утвержденное Постановлением Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».**

Применительно к органам внутренних дел можно выделить следующие основные системы обязательной сертификации средств защиты информации по требованиям безопасности информации:

- **РОСС RU.0001.01БИОО:** Система сертификации средств защиты информации по требованиям безопасности информации (ФСТЭК России);
- **РОСС RU.0001.030001:** Система сертификации средств криптографической защиты информации (ФСБ России);
- **РОСС RU.0003.01БИ00:** Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (ФСБ России).

Система сертификации средств защиты информации по требованиям безопасности информации (РОСС RU.0001.01БИОО).

Обязательной сертификации подлежат:

- средства, предназначенные для защиты сведений, составляющих государственную тайну или относимых к иной информации ограниченного доступа, являющейся государственным информационным ресурсом и (или) персональными данными;
- средства, сведения о которых составляют государственную тайну.

Система сертификации средств криптографической защиты информации (РОСС RU.0001.030001).

Она устанавливает правила сертификации по требованиям безопасности информации:

- ✔ шифровальных средств;
- ✔ систем и комплексов телекоммуникаций высших органов государственной власти Российской Федерации;
- ✔ закрытых систем и комплексов телекоммуникаций органов государственной власти субъектов Российской Федерации, центральных органов федеральной исполнительной власти, организаций, предприятий, банков и иных учреждений, расположенных на территории Российской Федерации, независимо от их ведомственной принадлежности и форм собственности;
- ✔ информационно-телекоммуникационных систем и баз данных государственных органов, Центрального банка Российской Федерации, Внешэкономбанка и их учреждений, иных государственных учреждений Российской Федерации.

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (РОСС RU.0003.01БИ00).

Обязательному сертифицированию подлежат:

- ✔ технические средства защиты информации;
- ✔ технические средства и системы в защищенном исполнении;
- ✔ технические средства защиты специальных оперативно-технических мероприятий (специальных технических средств, предназначенных для негласного получения информации);
- ✔ технические средства защиты информации от несанкционированного доступа (НСД);
- ✔ программные средства защиты информации от НСД и программных закладок;
- ✔ защищенные программные средства обработки информации;
- ✔ программно-технические средства защиты информации;
- ✔ специальные средства защиты от идентификации личности;
- ✔ программно-аппаратные средства защиты от несанкционированного доступа к системам оперативно-розыскных мероприятий (СОРМ) на линиях связи.

Выделенное помещение – это специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера.

Контролируемая зона – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Объектам информатизации могут быть присвоены следующие категории:

- **первая категория** присваивается объектам информатизации, предназначенным для обработки информации с грифом ***«особой важности»***;
- **вторая категория** присваивается объектам информатизации, предназначенным для обработки информации с грифом не выше ***«совершенно секретно»***;
- **третья категория** присваивается объектам информатизации, предназначенным для обработки информации с грифом не выше ***«секретно»***;
- **Четвертая категория** присваивается объектам информатизации, которые предназначены для обработки информации, содержащей сведения, составляющие ***служебную или иную тайну***, а также информации, не составляющей тайну, если такая информация должна быть защищена.

При вводе основных технических средств и систем, выделенных помещений в эксплуатацию должна периодически проводиться их **аттестация по требованиям безопасности информации.**

Аттестация объекта информатизации органов внутренних дел по требованиям безопасности информации носит обязательный характер для объектов информатизации, предназначенных для обработки сведений, составляющих государственную тайну, а также для государственных информационных систем.

Нормативно-правовой основой проведения аттестации является **Положение по аттестации объектов информатизации по требованиям безопасности информации** (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.).

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Только лишь наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленный в «Аттестате соответствия».

ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ – это комплекс организационных и технических мероприятий, направленных на организацию активно-пассивного противодействия средствам технической разведки и формирование рубежей охраны территории, зданий, помещений, оборудования с помощью комплексов технических средств.

Включают в себя:

- ✔ сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здания и помещения;
- ✔ средства защиты технических каналов утечки информации;
- ✔ средства обеспечения охраны территорий, зданий, помещений;
- ✔ средства противопожарной охраны;
- ✔ технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, дисков и других носителей информации.

СТРУТУРА СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Подсистема физической защиты информации создается для противодействия преднамеренным угрозам воздействия злоумышленника и стихийным силам, прежде всего – пожару. В общем случае подсистема физической защиты информации включает в себя:

- ✔ комплекс инженерной защиты информации;
- ✔ комплекс технической охраны объекта защиты.

Инженерная защита информации обеспечивается, прежде всего, созданием различного рода преград на возможных путях движения злоумышленников и распространения стихийных явлений к источникам защищаемой информации (заборы, стены, окна и двери зданий, помещений и т.д.). К средствам инженерной защиты относятся и различного рода преграждающие устройства систем контроля и управления доступом: вращающиеся двери, раздвижные и вращающиеся турникеты и т.п.

Для обнаружения попыток преодоления злоумышленником различного рода преград (барьеров), созданных в целях защиты информации, применяются ***технические средства охраны объектов,*** к которым относятся, прежде всего, *системы охранной и пожарной сигнализации.*

Подсистема инженерно-технической защиты информации от утечки предназначена для снижения до допустимых значений величины риска (вероятности) несанкционированного распространения информации от ее источника, расположенного внутри контролируемой зоны, к злоумышленнику. Достижение этой цели осуществляется путем применения различных сил и средств обнаружения и нейтрализации угроз подслушивания, наблюдения, перехвата и утечки информации по различным каналам, прежде всего – техническим.

СХЕМА ВОЗМОЖНОЙ УТЕЧКИ ИНФОРМАЦИИ ИЗ РАБОЧЕГО КАБИНЕТА СОТРУДНИКА ОВД

1. Перехват акустической (речевой) информации с помощью закладных устройств, скрытно установленных в предметах мебели, бытовой техники и т.п.

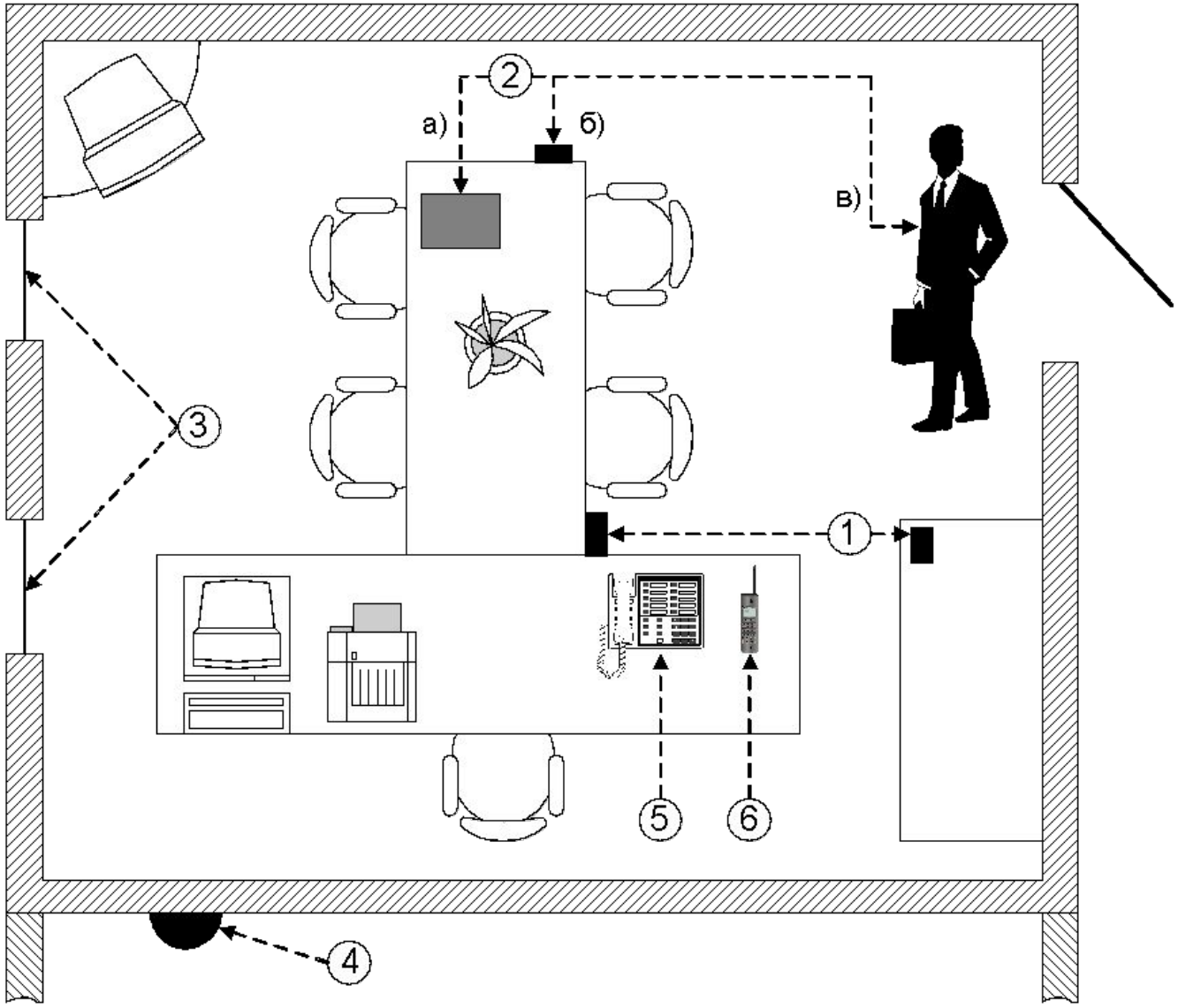
2. Перехват акустической (речевой) информации с помощью портативных диктофонов а) закамуфлированных под какие-либо предметы, например, ежедневник и т.п.; б) скрытно установленных, например, в предметы мебели и т.п.; в) находящихся у посетителей.

3. Перехват акустической информации через открытые окна с помощью направленных микрофонов.

4. Перехват акустической информации с помощью контактных микрофонов (стетоскопов).

5. Перехват а) акустической информации через телефонный аппарат за счет наводок и навязывания, или использования устройств типа «телефонное ухо»; б) информации, передаваемой по проводным линиям связи путем контактного или бесконтактного подключения к ним

6. Перехват информации, передаваемой по каналам радио-, радиорелейной связи (пейджинговая, сотовая связь).



ОСНОВНЫЕ УСЛОВИЯ ПО ОРГАНИЗАЦИИ И ОБОРУДОВАНИЮ РАБОЧЕГО КАБИНЕТА СОТРУДНИКА ОВД ПО ТРЕБОВАНИЯМ ЗАЩИТЫ ИНФОРМАЦИИ

1. Окна служебного кабинета должны выходить во внутренний двор, если он имеется.

2. Служебные кабинеты не должны располагаться в угловых помещениях, не должны являться смежными с помещениями других организаций.

3. В кабинет целесообразно установить пластиковые окна с трех или пятикамерными стеклопакетами с рельефным стеклом. Окна также должны быть оборудованы жалюзи. При проведении следственных действий и конфиденциальных переговоров окна кабинета должны быть закрыты, а жалюзи – опущены.

4. Необходимо обеспечить звукоизоляцию кабинета в местах возможного перехвата информации, которая должна исключать возможное прослушивания ведущихся в нем разговоров из-за пределов кабинета. Должен быть исключен несанкционированный доступ в кабинет.

5. Для защиты акустической информации от ее перехвата по акустическому и виброакустическому каналам с помощью закладных устройств следует оборудовать кабинет *системами виброакустического зашумления.* Они излучают шумоподобные сигналы речевого диапазона частот, снижая тем самым уровень разборчивости речи до необходимых значений.

Устройство защиты акустической речевой информации «ШОРОХ-5Л»

Генератор шума ГШ-1000М

6. В целях предотвращения утечки информации, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации, необходимо установить в кабинете шумогенераторы.

7. Кабинет может быть оборудован портативными системами обнаружения технических средств негласного получения информации.

8. Для исключения возможности утечки речевой информации посредством несанкционированного использования аппаратов систем сотовой связи в служебном кабинете может быть установлена система подавления сотовых телефонов.

Блокиратор сотовой и беспроводной связи ST 202 «UDAV-M»

Селективный обнаружитель цифровых радиопередающих устройств ST165

9. Избежать утечки акустической информации из служебного кабинета через сотовый телефон, принадлежащий сотруднику, в случае его негласной дистанционной активизации, поможет использование портативных акустических устройств для защиты сотовых телефонов от негласной активации.

10. При установке в рабочем кабинете сотрудника телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов с автоматическим определителем номера их следует отключать от сети на время проведения этих мероприятий или использовать соответствующие средства защиты.

Акустический сейф «Капсула-2»

Факторы, которые необходимо учитывать при анализе вероятности реализации угроз перехвата информации, используемой в ходе расследования

1. Потенциальная ценность информации – объекта возможных посягательств, для преступных сообществ, фигурантов по уголовному делу.

2. Круг фигурантов по уголовному делу, их связи в преступной среде, в среде бизнеса и правоохранительных органов, органах власти, их финансовые возможности.

3. Стоимость технических средств, необходимых для перехвата информации по тому или иному каналу.

4. Сложность организационных мероприятий по внедрению технических средств негласного получения информации на объект.

5. Сложность практического использования технических средств перехвата информации.

6. Наличие в регионе высококвалифицированных специалистов в области ведения технической разведки.

4. ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ СПЕЦИАЛЬНЫХ ПРОВЕРОК ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ ОВД

Специальная проверка – проверка объекта информатизации в целях выявления и изъятия возможно внедренных средств негласного получения информации.

Подобного рода проверки включают в себя:

- специальные проверки технических средств;
- специальные обследования помещений.

Порядок проведения специальной проверки определяется Правительством Российской Федерации и проводится соответствующими органами ФСБ России или организациями, имеющими необходимые лицензии.

Лицензирование – это процесс передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ.

Лицензия – специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

Для проведения работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, необходимо получения лицензий на проведение работ со сведениями соответствующей степени секретности.

Также подлежит лицензированию деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, деятельность по технической защите конфиденциальной информации.

Специальная проверка технических средств – это комплекс мероприятий по поиску электронных устройств съема информации («закладочных устройств»), возможно внедренных в технические средства.

Специальным проверкам подвергаются технические средства иностранного производства, а также технические средства отечественного производства, содержащие комплектующие иностранного производства в случае, если они предназначены для:

- обработки сведений, составляющих государственную тайну;
- размещения в защищаемых помещениях;
- обработки информации с ограниченным доступом.

Основные этапы специальной проверки технических средств:

1) прием-передача технического средства, формирование исходных данных для составления программы проведения специальной проверки;
2) разработка программы проведения специальной проверки технического средства;
3) проведение технических проверок;
4) анализ результатов.

Специальное обследование помещений – это комплекс инженерно-технических мероприятий, проводимых с использованием специализированных технических средств, с целью выявления возможно внедренных электронных средств съема информации в ограждающих конструкциях, мебели и предметах интерьера защищаемого помещения.

Специальные обследования помещений в обязательном порядке проводятся в отношении выделенных помещений первой категории. В остальных случаях – по решению руководителя организации.

Специальные обследования помещений проводятся:

- при аттестации помещений;
- периодически (в соответствии с заранее разработанным планом-графиком);
- после проведения в помещениях каких-либо работ (ремонта, монтажа оборудования, изменения интерьера и т.д.);
- после неконтролируемого посещения посторонними лицами;
- во всех случаях, когда возникает подозрение в утечке информации через возможно внедренные средства несанкционированного съема информации.

По глубине проводимых проверок поисковые мероприятия подразделяются на четыре уровня.

Первый уровень: в результате проверки могут быть обнаружены активные радиоизлучающие изделия, установленные непосредственно в проверяемом или смежных с ним помещениях (радиомикрофоны с автономным источником питания, телефонные радиопередатчики).

Второй уровень: могут быть обнаружены все устройства первого уровня плюс сетевые передатчики, использующие в качестве канала передачи сеть питания 220В, 50Гц.

Третий уровень: могут быть выявлены все изделия второго уровня плюс все типы кабельных микрофонных систем, а также оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

Четвертый уровень: могут быть выявлены все типы заносных и закладных электронных устройств перехвата информации и естественные каналы утечки информации.

Мероприятия по поиску средств съема информации могут проводиться как в служебных, так и в не служебных помещениях сотрудников органов внутренних дел и могут быть подразделены на *плановые*, *внеплановые* и *повседневные*.

Основные **этапы** проведения поисковых мероприятий:

1. Подготовка к проведению поисковых мероприятий.
2. Проведение поисковых мероприятий.
   - визуальный осмотр.
   - контроль и анализ радиоэфира.
   - проверка электронных приборов.
   - проверка предметов интерьера и мебели.
   - проверка проводных линий, электроустановочных и коммуникационных изделий.
   - обследование ограждающих конструкций.
3. Заключительный этап поискового мероприятия.

Презентацию подготовил начальник кафедры административно-правовых дисциплин и информационного обеспечения ОВД Калининградского филиала Санкт-Петербургского университета МВД России, доктор педагогических наук, кандидат юридических наук, доцент, полковник полиции **Григорьев А.Н.**

Презентация обсуждена и одобрена на заседании кафедры административно-правовых дисциплин и информационного обеспечения ОВД Калининградского филиала Санкт-Петербургского университета МВД России 8 сентября 2017 г., протокол № 1.