



Дисциплина «Технические средства и методы защиты информации»

Лекция 1

Технические разведки и их виды

Преподаватель: Батыргалиев Асхат Болатканович, PhD,
ассоц.проф. кафедры «Кибербезопасность, обработка и
хранение информации»

askhat.b.b@gmail.com

Содержание

1. Основные термины
2. Основные принципы разведки
3. Виды разведки
4. Классификация технических разведок

По завершению урока Вы будете знать:

1. Основную терминологию технической разведки
2. Принципы ведения разведки
3. Модель и структуру технической разведки
4. Виды и классификацию технических разведок

Основные термины и определения

- ❑ **Техническая разведка** – деятельность по получению важной (защищаемой) информации с помощью технических средств.
- ❑ **Средство технической разведки** – аппаратура технической разведки, размещенная на стационарном или мобильном (возимом, носимом) объекте (помещении, транспортном средстве и т.д.), и обслуживаемая соответствующим персоналом.
- ❑ **Аппаратура технической разведки** – совокупность технических устройств, предназначенных для обнаружения, приема (перехвата), регистрации и обработки сигналов, содержащих важную (защищаемую) информацию.
- ❑ **Возможности технической разведки** – характеристики способности обнаружения, распознавания, приема и регистрации информативных сигналов средствами технической разведки.
- ❑ **Зона разведдоступности** – пространство вокруг объекта, в пределах которого реализуются возможности технической разведки.
- ❑ **Модель технической разведки** – описание средств технической разведки, содержащее их технические характеристики и тактику применения в объеме, достаточном для оценки возможностей технической разведки.
- ❑ **Информативный (опасный) сигнал** – акустические, электрические или электромагнитные сигналы и поля, по параметрам которых может быть раскрыта информация.

Основные принципы разведки

Добывание информации органами разведки основывается на следующих **принципах**:

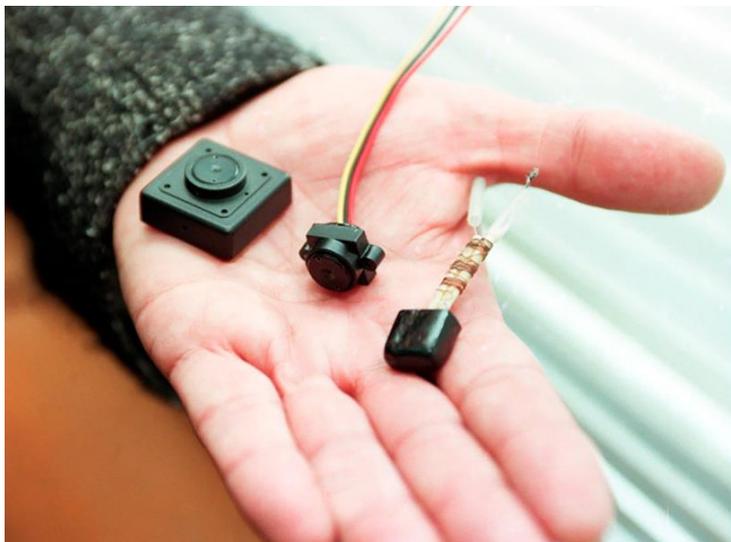
- **целеустремленности** - определение задач и объектов разведки, ведение её по единому плану и сосредоточение усилий на решении основных задач;
- **активности** - настойчивое стремление добыть необходимые разведывательные сведения;
- **плановости** - добыча информации ведется по заранее разработанным программам разведки;
- **оперативности** - разведка должна решать поставленные перед ней задачи в минимально возможные сроки;
- **непрерывности** - изменение условий, при которых ведется разведка не должно сказываться на качестве добываемой информации;
- **скрытности** - приоритет на использование пассивных технических средств разведки, маскировка и камуфлирование разведаппаратуры, широкое применение;
- **комплексности** - для добывания разведанных о конкретных объектах применяются различные сочетания технических средств, основанных на получении данных по различным техническим каналам утечки информации.

Виды разведки

Достаточно условно разведку можно разделить на агентурную и техническую.

Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а техническую разведку ведут люди.

Отличия - в преобладании человеческого или технического факторов.



Виды разведки

Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

Ведение **технической разведки** связано, с повышением ее технических возможностей, обеспечивающих:

- снижение риска физического задержания агента за счет дистанционного контакта его с источником информации;
- добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

Структура технической разведки



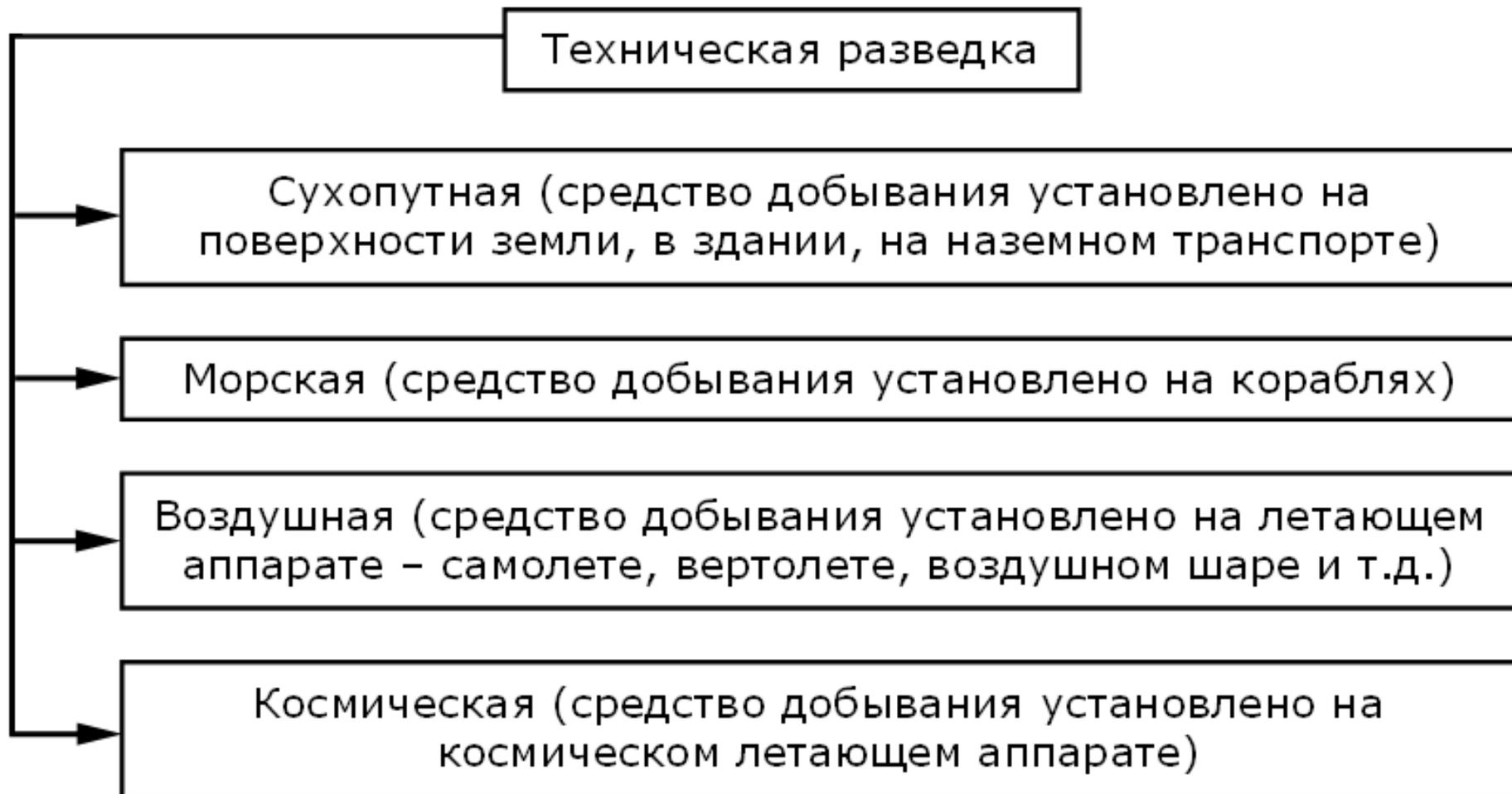
Модель технической разведки

- ТР известны схемы, алгоритмы функционирования технических средств
- ТР не известны значения настраиваемых параметров средств защиты информации
- ТР способна перехватить любые сигналы в полном и неискаженном виде, передаваемые по любым каналам связи, находящимся частично или полностью за пределами контролируемой зоны
- ТР способна регистрировать любые излучения технических средств обработки и передачи информации за пределами контролируемой зоны
- В распоряжении ТР есть вычислительные средства для анализа получаемой информации
- ТР способна осуществить любое радиоэлектронное воздействие на сигналы технических средств обработки и передачи информации
- ТР не способно осуществлять непосредственное воздействие на компоненты технических средств обработки и передачи информации

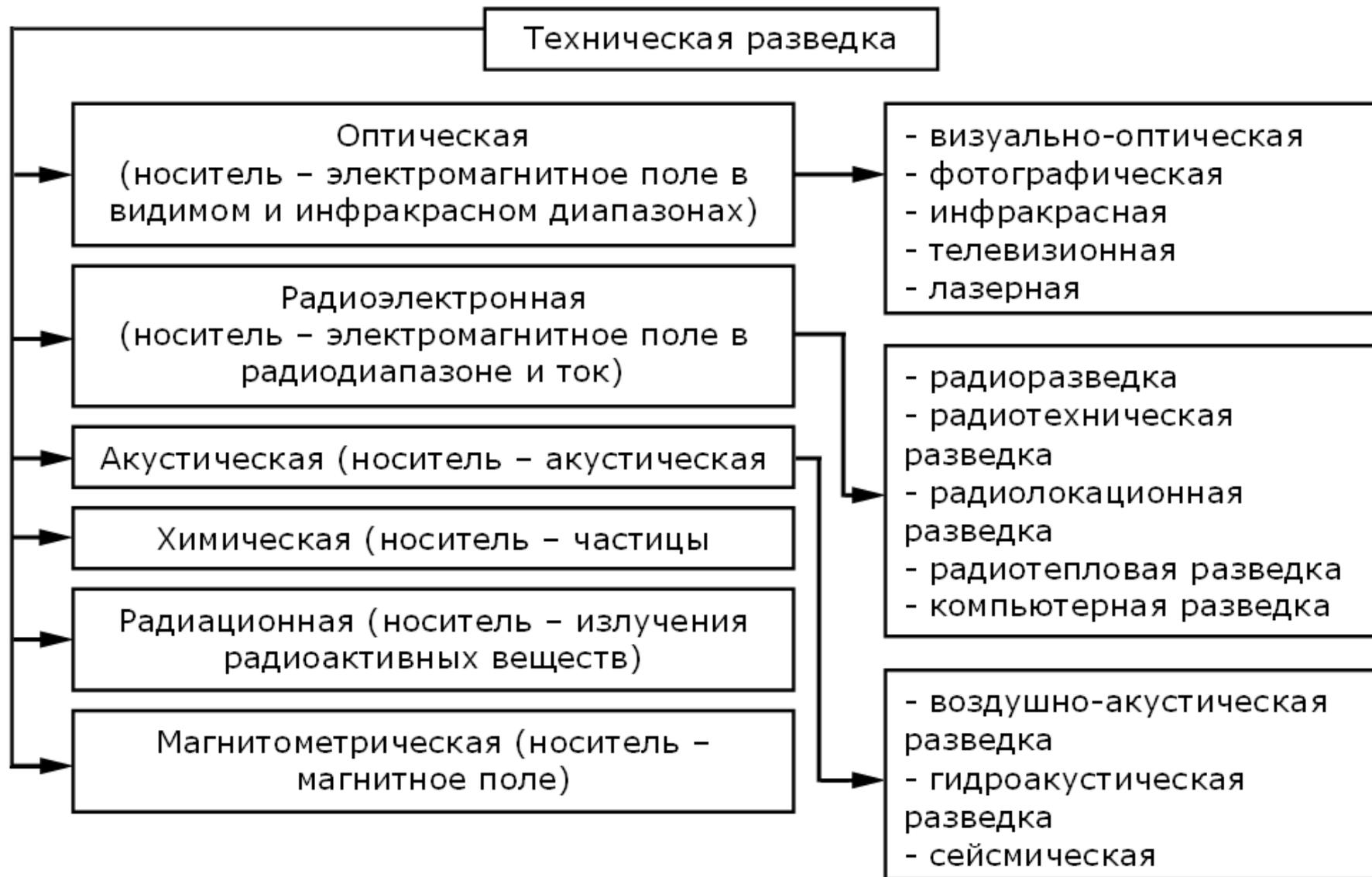
Стороны (субъекты и объекты) при ведении технической разведки

- Одно государство против другого государства
- Государство против потенциально неблагонадёжных граждан и организаций
- Государство или межправительственная организация против преступных сообществ
- Коммерческая организация против других коммерческих и общественных организаций, физических лиц и государственных органов
- Физическое лицо против других физических лиц или организаций
- Преступная организация против других преступных организаций, легальных организаций, физических лиц, а также государственных и международных правоохранительных организаций

Классификация по видам носителей технических средств добывания информации



Классификация по физической природе носителей информации



Электронные методы разведки.

Радиотехнические методы

Радиоэлектронная разведка (РЭР) - получение информации путём приема и анализа электромагнитного излучения (ЭМИ) радиодиапазона, создаваемого различными РЭС.

Радиоразведка - добывание сведений о противнике путём радиопоиска, перехвата, анализа излучений и радиопеленгования радиоэлектронных средств. Радиоразведка использует такие методы и средства, как:

- выделение и анализ сигнала из широкополосных линий связи;
- фильтрование, обработка и анализ факсов;
- анализ трафика, распознавание ключевых слов, получение текста и анализ тем;
- системы распознавания речи;
- непрерывное распознавание речи;
- идентификация говорящего и другие методы выбора голосовых сообщений;
- снижение нагрузки или подрыв криптографических систем.

Электронные методы разведки.

Радиотехнические методы

Радиотехническая разведка (РТР) — вид разведывательной деятельности, целью которого является сбор и обработка информации получаемой с помощью радиоэлектронных средств о радиоэлектронных системах по их собственным излучениям, и последующая их обработка с целью получения информации о положении источника излучения, его скорости, наличии данных в излучаемых сигналах, смысловом содержании сигналов. Объектами РТР являются: радиотехнические устройства различного назначения (РЛС, импульсные системы радиоперехвата, радиотелекодовые системы, а также ЭМИ, создаваемые работающими электродвигателями, электрогенераторами, вспомогательными устройствами и т. п.). Средства РТР устанавливаются на самолётах, спутниках, кораблях, других объектах и позволяют:

- установить несущую частоту передающих радиосредств;
- определить координаты источников излучения;
- измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);
- установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);
- определить структуру боковых лепестков излучения радиоволн;
- измерить поляризацию радиоволн;
- установить скорость сканирования антенн и метод обзора пространства РЛС;
- проанализировать и записать информацию.

Электронные методы разведки.

Радиотехнические методы

Радиолокационная разведка - вид технической разведки, в ходе которой информация добывается с помощью радиолокационных станций. РЛС могут быть стационарные наземные, переносные и установленные на самолётах, спутниках, кораблях, других мобильных объектах. Для ведения РЛР применяются:

- РЛС бокового обзора, РЛС широкополосного обзора, РЛС прожекторного обзора, которые устанавливаются на космических и воздушных носителях и используются для получения видовой информации о местности и объектах на ней, над которыми пролетает носитель с аппаратурой;
- наземные и корабельные РЛС, объектами которых являются морские, воздушные и космические цели;
- передвижные и переносные РЛС наблюдения за полем боя, обеспечивающие обнаружение движущихся целей (живой силы и техники) в зоне обзора, приблизительное определение количества целей и скорости их перемещения.

Электронные методы разведки.

Электронно-оптические методы

Оптоэлектронная разведка - получение информации путём приема и анализа электромагнитных излучений ультрафиолетового, видимого и инфракрасного (ИК) диапазонов, которые создаются или переотражаются объектами разведки

Фотографическая разведка - получение видовой информации с помощью специальных фотокамер, которые могут быть установлены на космических и воздушных носителях и в наземных условиях

Телевизионная разведка - получение информации с помощью телевизионных камер

Инфракрасная разведка — получение информации об объектах при использовании в качестве источника информации либо собственного теплового излучения объектов, либо переотраженного ИК-излучения луны, звёздного неба, а также переотраженного излучения специальных ИК-прожекторов подсвета местности. В соответствии с этим все приборы ИКР делятся на 2 группы: тепловизоры, тепlopеленгаторы, радиометры; приборы ночного видения.

Фотометрическая разведка - используется для обнаружения и распознавания устройств, в которых используются лазерные источники излучения

Лазерная разведка - процесс получения видовой информации с использованием лазерных сканирующих камер, которые устанавливаются на воздушных носителях

Электронные методы разведки.

Электронно-акустические методы

Акустическая разведка - получение информации путём приема и анализа акустических сигналов, распространяющихся в воздушной среде от различных объектов. Акустическая разведка осуществляется перехватом производственных шумов объекта и перехватом речевой информации. В акустической разведке используются: пассивные методы перехвата; активные методы перехвата; контактные методы перехвата.

- Дистанционное подслушивание разговоров — используется для перехвата речевых сигналов с использованием микрофонов направленного действия, закладок и других средств
- Обнаружение и распознавание источников шумового акустического излучения — используется для распознавания источников повышенного звукового давления

Гидроакустическая разведка - вид технической разведки, в ходе которой добывается информация о противнике путём приёма, регистрации, обработки и анализа принятых гидроакустических сигналов. Гидроакустическая разведка позволяет обнаружить и классифицировать морские цели, определить расстояние до них и параметры их движения, то есть получить данные для применения оружия.

Электронные методы разведки. Методы с использованием электронных датчиков

Сейсмическая разведка - получение информации путём обнаружения и анализа деформационных и сдвиговых полей, возникающих в грунте при различных воздействиях на неё.

Магнитометрическая разведка - получение информации путём обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой.

Электронные методы разведки. Методы разведки в телекоммуникационных системах

Разведка в системах телекоммуникаций включает в себя получение несанкционированного доступа к информации, перехват сообщений, перехват данных о кредитных карточках, прослушивание телефонных разговоров в мобильных и проводных сетях, определение географического местоположения владельцев сотовых телефонов, расшифровку закодированных сообщений, отслеживание действия пользователя в разных сетях и многие другие функции.

Сетевая разведка - комплекс мероприятий по получению и обработке данных об информационной системе клиента, ресурсов информационной системы, средств защиты, используемых устройств и программного обеспечения и их уязвимостях, а также о границе проникновения.

Компьютерная разведка (интернет-разведка) - комплекс информационных технологий для систематического нахождения информации в открытых источниках и, возможно, доставки данных в машиночитаемой форме.