**ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»**

***Утверждены решением***
***Ученого совета ДГУНХ,***
***протокол № 11***
***от 06 июня 2023 г.***

# КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

# ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

# ПО ДИСЦИПЛИНЕ «ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ РАЗВЕДКАМ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ 10.03.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат



Махачкала – 2023

**УДК**681.518(075.8)
**ББК** 32.81.73

**Составитель –** Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент –** Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, зав. кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент –** Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

**Представитель работодателя** - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

*Оценочные материалы по дисциплине «Противодействие техническим разведкам» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»*

Оценочные материалы по дисциплине «Противодействие техническим разведкам» размещены на официальном сайте www.dgunh.ru

Гасанова З.А. Оценочные материалы по дисциплине «Противодействие техническим разведкам» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г. – 52 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

**СОДЕРЖАНИЕ**

## Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Противодействие техническим разведкам» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Противодействие техническим разведкам» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценочные материалы сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.

## РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

### 1.1 Перечень формируемых компетенций

| Код компетенции | Формулировка компетенции |
|---|---|
| **ПК** | **ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ** |
| **ПК-2.** | Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации |
| **ПК-3.** | Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем |

### 1.2. Перечень компетенций с указанием видов оценочных средств

| ***Формируемые компетенции*** | ***Код и наименование индикатора достижения компетенции*** | ***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*** | ***Уровни освоения компетенций*** | ***Критерии оценивания сформированности компетенций*** | ***Виды оценочных средств*** |
|---|---|---|---|---|---|
| ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации | ИПК-2.1. Устанавливает и налаживает средства защиты информации в автоматизированных системах | **Знать:**<br>– современные методы и средства технической разведки;<br>– основные подходы к созданию средств технической защиты. | Пороговый уровень | Обучающийся слабо (частично) знает современные методы и средства технической разведки, основные подходы к созданию средств технической защиты | **Блок А –** задания репродуктивного уровня<br>– тестовые задания;<br>– вопросы для устного опроса |
| | | | Базовый уровень | Обучающийся с незначительными ошибками и отдельными | |

| *Формируемые компетенции* | *Код и наименование индикатора достижения компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|---|
| | | | | пробелами знает современные методы и средства технической разведки, основные подходы к созданию средств технической защиты | |
| | | | Продвинутый уровень | Обучающийся с требуемой степенью полноты и точности знает современные методы и средства технической разведки, основные подходы к созданию средств технической защиты | |
| | | **Уметь:**<br>– выбирать и устанавливать технические средства защиты информации оценивать их эффективность | Пороговый уровень | – Обучающийся слабо (частично) умеет выбирать и устанавливать технические средства | **Блок В** – задания реконструктивного уровня<br>– тематика рефератов;<br>- тематика презентаций. |

| *Формируемые компетенции* | *Код и наименование индикатора достижения компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|---|
| | | средства защиты информации;<br>– оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов. | | защиты информации оценивать их эффективность средства защиты информации, оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов | - практическая работа |
| | | | Базовый уровень | – Обучающийся с незначительными затруднениями умеет выбирать и устанавливать технические средства защиты информации оценивать их эффективность средства защиты информации, оформлять рабочую техническую документацию с учетом действующих | |

| *Формируемые компетенции* | *Код и наименование индикатора достижения компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|---|
| | | | | нормативных и методических документов | |
| | | | Продвинутый уровень | – Обучающийся умеет выбирать и устанавливать технические средства защиты информации оценивать их эффективность средства защиты информации, оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов | |
| | | **Владеть:**<br>- методами технической защиты информации;<br>- навыками внедрение и эксплуатации современных средств технической защиты информации методиками | Пороговый уровень | Обучающийся слабо (частично) владеет методами технической защиты информации, навыками внедрение и эксплуатации современных средств технической | **Блок С** – задания практико-ориентированного уровня<br>– практические задания.<br>- лабораторные работы. |

| ***Формируемые компетенции*** | ***Код и наименование индикатора достижения компетенции*** | ***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*** | ***Уровни освоения компетенций*** | ***Критерии оценивания сформированности компетенций*** | ***Виды оценочных средств*** |
|---|---|---|---|---|---|
| | | проверки защищенности объектов информатизации | | защиты информации методиками проверки защищенности объектов информатизации | |
| | | | Базовый уровень | Обучающийся с небольшими затруднениями владеет методами технической защиты информации, навыками внедрение и эксплуатации современных средств технической защиты информации методиками проверки защищенности объектов информатизации | |
| | | | Продвинутый уровень | Обучающийся свободно владеет методами технической защиты информации, навыками внедрение и эксплуатации современных | |

| ***Формируемые компетенции*** | ***Код и наименование индикатора достижения компетенции*** | ***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*** | ***Уровни освоения компетенций*** | ***Критерии оценивания сформированности компетенций*** | ***Виды оценочных средств*** |
|---|---|---|---|---|---|
| | | | | средств технической защиты информации методиками проверки защищенности объектов информатизации | |
| ПК-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем | ИПК-3.2. Учитывает особенности средств защиты информации при проектировании системы защиты информации | **Знать:**<br>– технические каналы утечки информации. | Пороговый уровень | Обучающийся слабо (частично) знает технические каналы утечки информации. | **Блок А –** задания репродуктивного уровня<br>– тестовые задания;<br>– вопросы для устного опроса |
| | | | Базовый уровень | Обучающийся с незначительными ошибками и отдельными пробелами знает технические каналы утечки информации | |
| | | | Продвинутый уровень | Обучающийся с требуемой степенью полноты и точности знает технические каналы утечки информации | |

| *Формируемые компетенции* | *Код и наименование индикатора достижения компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|---|
| | | **Уметь:**<br>– определять источники угрозы информационной безопасности;<br>– анализировать и оценивать угрозы информационной безопасности объекта. | Пороговый уровень | Обучающийся слабо (частично) умеет определять источники угрозы информационной безопасности, анализировать и оценивать угрозы информационной безопасности объекта. | **Блок В** – задания реконструктивного уровня<br>– практические задания;<br>- тематика рефератов;<br>- тематика презентаций. |
| | | | Базовый уровень | Обучающийся с незначительными затруднениями умеет определять источники угрозы информационной безопасности, анализировать и оценивать угрозы информационной безопасности объекта. | |

| *Формируемые компетенции* | *Код и наименование индикатора достижения компетенции* | *Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций* | *Уровни освоения компетенций* | *Критерии оценивания сформированности компетенций* | *Виды оценочных средств* |
|---|---|---|---|---|---|
| | | | Продвинутый уровень | Обучающийся умеет определять источники угрозы информационной безопасности, анализировать и оценивать угрозы информационной безопасности объекта. | |
| | | **Владеть:**<br>– методами формирования документации;<br>– методами расчета и инструментального контроля показателей технической защиты информации | Пороговый уровень | Обучающийся слабо (частично) владеет методами формирования документации, методами расчета и инструментального контроля показателей технической защиты информации | **Блок С** – задания практико-ориентированного уровня<br>– лабораторные работы. |
| | | | Базовый уровень | Обучающийся с небольшими затруднениями владеет методами формирования документации, методами | |

| ***Формируемые компетенции*** | ***Код и наименование индикатора достижения компетенции*** | ***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*** | ***Уровни освоения компетенций*** | ***Критерии оценивания сформированности компетенций*** | ***Виды оценочных средств*** |
|---|---|---|---|---|---|
| | | | | расчета и инструментального контроля показателей технической защиты информации | |
| | | | Продвинутый уровень | Обучающийся свободно владеет методами формирования документации, методами расчета и инструментального контроля показателей технической защиты информации | |

## РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

### Для проверки сформированности компетенции ПК-2. Способен учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации

### ИПК-2.1. Устанавливает и налаживает средства защиты информации в автоматизированных системах

### Блок А. Задания репродуктивного уровня («знать»)

**А.1 Тестовые задания по дисциплине**

1. Основные технические средства и системы – это:

А) Технические средства и системы, непосредственно участвующие в обработке информации ограниченного доступа.

Б) Технические средства и системы обработки открытой информации.

В) Технические средства и системы обработки информации.

Г) Средства вычислительной техники и автоматизированные системы обработки информации.

Д) Технические средства и системы, установленные на объекте информатизации.

2. Вспомогательные технические средства и системы – это:

А) Технические средства и системы, участвующие в обработке информации ограниченного доступа.

Б) Технические средства и системы обработки открытой информации.

В) Технические средства и системы обработки информации.

Г) Технические средства и системы, установленные на объекте информатизации.

Д) Технические средства и системы, установленные на объектах информатизации или в выделенных (защищаемых) помещениях, непосредственно не участвующие в обработке (приеме, передачи, записи, хранения и ит.д.) информации ограниченного доступа.

3. Выделенное (защищаемое) помещение – это:

А) Помещение, предназначенное для установки технических средств обработки информации.

Б) Помещение, предназначенное для установки вспомогательных технических средств и систем.

В) Служебный кабинет, актовый зал, конференц-зал.

Г) Специальное помещение (служебный кабинет, актовый, конференц-зал и т.д.), предназначенное для регулярного проведения совещаний, обсуждений,

конференций, переговоров, бесед и других мероприятий секретного (конфиденциального) характера.
Д) Помещение в котором размещены средства вычислительной техники и автоматизированные системы обработки информации.

4. Контролируемая зона – это:
А) Охраняемая территория.
Б) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц.
В) Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц или транспортных средств.
Г) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска.
Д) Пространство (территория, здание, часть здания), в котором исключено пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

5. Применительно к области информационной безопасности информация – это:
А) Сведения (сообщения, данные) независимо от формы их представления.
Б) Факты, данные, характеризующие кого-л., что-л.
В) Отчет с цифровыми данными.
Г) Сведения, предназначенные для передачи по каналу связи.
Д) Сведения, представленные в форме, пригодной для постоянного хранения, передачи и (автоматизированной) обработки.

6. Основные свойства защищаемой информации:
А) Конфиденциальность информации.
Б) Доступность информации.
В) Целостность информации.
Г) Конфиденциальность и целостность информации.
Д) Конфиденциальность, целостность и доступность информации.

7. К информации ограниченного доступа относятся:
А) Сведения с грифом «для служебного пользования».
Б) Сведения, составляющие коммерческую тайну, служебную тайну и иную тайну.
В) Сведения, составляющие государственную тайну, а так сведения конфиденциального характера.
Г) Секретные сведения.
Д) Сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации.

8. Конфиденциальность информации – это:

А) Обеспечение достоверности и полноты информации.
Б) Обеспечение правомерного (с разрешения обладателя информации) доступа к информации.
В) Обеспечение достоверности, полноты информации и возможности использования информации.
Г) Условия передачи информации третьим лицам.
Д) Обеспечение возможности получения информации и ее использования.

9. Утечка информации – это:
А) Неконтролируемое распространение защищаемой информации в результате ее разглашения.
Б) Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.
В) Неконтролируемое распространение защищаемой информации в результате несанкционированного доступа к ней.
Г) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.
Д) Неправомерное разглашение или распространение сведений ограниченного доступа.

10.Несанкционированный доступ к информации – это:
А) Доступ к информации с использованием технических средств разведки.
Б) Доступ к информации путем похищения документов, подкупа или угроз, а равно иным незаконным способом.
В) Доступ к информации, осуществляемый с применением СВТ.
Г) Доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации с применением штатных средств, предоставляемых СВТ или АС, или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.
Д) Доступ к информации, приводящий к разрушению, уничтожению, искажению, незаконному перехвату и копированию к информации.

11.Техническая защита информации –
А) Защита информации с помощью ее криптографического преобразования.
Б) Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
В) Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Г) Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
Д) Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации путем проведения организационных мероприятий и применения технических, программных и программно-аппаратных средств.

12.Основные задачи защиты информации от утечки по техническим каналам:
А) Предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических обработки информации.
Б) Предотвращение утечки речевой информации по техническим каналам из выделенных (защищаемых) помещений.
В) Выявление электронных устройств перехвата информации, внедренных в технические средства и выделенные (защищаемые) помещения.
Г) Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации.
Д) Предотвращение хищения носителей информации и несанкционированного снятия копий с носителей информации.

13.Утечка информации по техническому каналу:
А) Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.
Б) Неконтролируемое распространение информационного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.
В) Неконтролируемого распространения защищаемой информации в результате ее разглашения.
Г) Неконтролируемого распространения защищаемой информации в результате получения защищаемой информации иностранными разведками.
Д) Получение возможности ознакомления с информацией с использованием программных и (или) технических средств.

14.Носитель информации:
А) 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.
Б) Материальный объект, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
В) Физическое поле, в котором информация находит свое отображение в виде количественных характеристик физических величин.

Г) Материальный объект, в котором информация находит свое отображение в виде технических решений и процессов.
Д) Материальный носитель информации с реквизитами, позволяющими определить обладателя информации.

15.Перехват информации:
А) Неправомерное получение информации с использованием программно-аппаратных средств.
Б) Получение возможности ознакомления с информацией, обработки информации и (или) воздействия на информацию с использованием программных и (или) технических средств.
В) Получение возможности ознакомления с информацией с использованием технических средств. Г) Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.
Д) Действия, направленные на получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации.

16.Технический канал утечки информации:
А) Совокупность источника информативного сигнала, технического средства, с помощью которого осуществляется перехват информации, и физической среды распространения информативного сигнала.
Б) Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.
В) Получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными документами прав разграничения доступа к защищаемой информации.
Г) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками.
Д) Неконтролируемое распространение защищаемой информации в результате получения защищаемой информации иностранными разведками.

## **А2. Вопросы для устного опроса**

1. Место технической разведки в системе защиты информации.
2. Общая модель защиты от технической разведки на скрываемом объекте.
3. Принципы защиты объектов от технических разведок.
4. Общая классификация и характеристика способов защиты.
5. Классификация технической разведки. Возможности видов технической разведки

6. Защита объектов от акустической речевой разведки
7. Защита объектов от акустической сигнальной разведки
8. Оптико-механические приборы
9. Приборы ночного видения
10. Средства для проведения скрытой фотосъемки
11. Защита от визуально-оптических и фотографических средств разведки
12. Способы пассивного скрытия (маскировка)
13. Активные способы защиты от ОЭСР.
14. Пассивная радио- и радиотехническая маскировка
15. Активная радио- и радиотехническая маскировка
16. Типовые ситуации защиты РЭС
17. Зоны подключения
18. Перехват телефонных переговоров в зонах «А», «Б», «В»
19. Телефонные радиозакладки
20. Перехват побочных электромагнитных сигналов и наводок
21. Перехват телефонных переговоров в зоне «Г»
22. Перехват телефонных переговоров в зоне «Д»
23. Перехват телефонных переговоров в зоне «Е»
24. Перехват телеграфных разговоров
25. Защита телефонных аппаратов
26. Архитектура GSM сети. Особенности работы
27. Безопасность GSM
28. Перехват информации в GSM

## Блок В. Задания реконструктивного уровня («уметь»)

### В1. Тематика рефератов

1. Нормативно-правовые документы технической ЗИ
2. Структура контролирующих органов по ЗИ
3. Классификация демаскирующих признаков (ДП)
4. История развития технической разведки
5. Каналы утечки информации в технических средствах информатизации
6. Характеристики способов и средств наблюдения в оптическом диапазоне.
7. Визуально-оптические приборы (бинокли, трубы. Телескопы)
8. Приборы ночного видения и тепловизоры.
9. Способы и средства наблюдения в радиодиапазоне.
10. Виды и характеристики антенн.
11. Радиоприёмники и их характеристики.
12. Способы и средства прослушивания, слуховая система человека.
13. Типы микрофонов и их характеристики.
14. Направленные и лазерные микрофоны.
15. Методы и средства защиты речевой информации.
16. Мобильные системы связи и их использование в информационных атаках.

17.Защита информации от атак с помощью сотовых телефонов и диктофонов.

## В2. Тематика презентаций

1. «Детекторы лжи» и их использование для получения информации.
2. Способы и принципы инженерно технической защиты информации.
3. Контролируемая зона и критерий защищённости СВТ.
4. Средства и методы (не меньше двух) обнаружения закладных устройств.
5. Способы подключения и защита телефонной линии.
6. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него.
7. Характеристики способов и средств наблюдения в оптическом диапазоне.
8. Визуально-оптические приборы (бинокли, трубы. Телескопы)
9. Приборы ночного видения и тепловизоры.
10. Способы и средства наблюдения в радиодиапазоне.
11. Виды и характеристики антенн.
12. Радиоприёмники и их характеристики.
13. Способы и средства прослушивания, слуховая система человека.
14. Типы микрофонов и их характеристики.
15. Направленные и лазерные микрофоны.
16. Методы и средства защиты речевой информации.
17. Мобильные системы связи и их использование в информационных атаках.
18. Защита информации от атак с помощью сотовых телефонов и диктофонов.

## В3. Практическая работа

### Практическая работа 1.

**Цель работы:** Приобрести практические навыки по обеспечению защиты информации в кабинете руководителя организации.

Основные этапы и процедуры защиты информации:

- моделирование кабинета руководителя как наиболее сложного объекта защиты;
- моделирование угроз информации в кабинете руководителя организации;
- выбор рациональных мер по защите информации в кабинете руководителя организации.

### Характеристика информации, защищаемой в кабинете руководителя

***Виды информации в кабинете руководителя***

**В** кабинете руководителя могут находиться на различных носителях почти все виды защищаемой в организации информации, в том числе:

- семантическая информация в документах, с которыми работает руководитель или которые приносят его заместители, другие сотрудники,

представители других организаций, а также на чертежах и плакатах, развешиваемых на стенах или проецируемых во время докладов и совещаний;

- семантическая речевая информации во время конфиденциального разговора руководителя с посетителями и выступлений участников совещания;
- информация о видовых признаках VIP-персон, посещающих руководителя и по характеру деятельности которых можно определить тематику обсуждаемых вопросов;
- видовые демаскирующие признаки продукции, макетов и опытных образцов, которые демонстрируются руководителю на разных этапах их производства, а также их изображения на плакатах, экранах видеопроектора или телевизора;
- демаскирующие признаки веществ, приносимых руководителю для демонстрации соответствующей продукции, а также образцы исходных материалов.

Основными видами информации в кабинете руководителя являются: речевая информация, семантическая информация на плакатах и экране видеопроектора, информация о видовых демаскирующих признаках продукции.

***Источники информации в кабинете руководителя***

Основными источниками информации в кабинете руководителя являются:

- руководитель организаций;
- должностные лица организации, посещающие кабинет;
- представители других организаций, с которыми руководитель обменивается секретной (конфиденциальной) информацией в ходе встреч или совещаний;
- посетители во время приема по личным вопросам, разговор с которыми может содержать сведения, содержащие коммерческую или иную тайну;
- документы на столах, плакаты на стенах, аудио- и видеодокументы;
- приносимая в кабинет продукция, сведения о которой и ее демаскирующие признаки содержат государственную, коммерческую или иную тайну;
- приносимые в кабинет материалы и продукция в виде веществ, информация о составе и технологии изготовления которых защищается. Характеристика информации и ее источников дана в табл.1.

*Таблица 1.*

| *№ п/п* | *Вид информации в кабинете* | *Источник информации* | *Максимальная цена информации* | *Место нахождения источника информации в кабинете* |
|---|---|---|---|---|
| 1 | Семантическая документальная | Документы | \ Очень высокая | В сейфе, на столах, на плакатах, на стене, на экране монитора, плакатах, доске, экране видеопроектора |

| | | | | |
|---|---|---|---|---|
| 2 | Семантическая речевая акустическая | Люди | Очень высокая | В кабинете |
| 3 | Семантическая речевая, читаемая по губам | Люди | Средняя | В кабинете |
| 4 | Видовые признаки | Продукция | Средняя | На столе, изображения на плакатах, экране монитора, телевизора, видеопроектора |
| 5 | Видовые признаки | Люди | Низкая | В кабинете |
| 6 | Видовые признаки | Вещества и материалы | Очень низкая | На столах |
| 7 | Вещественные признаки | Продукция: | | |
| | | химического производства; | Средняя | На столах |
| | | — других производств | Низкая | На столах |
| 8 | Вещественные признаки | Материалы | Очень низкая | На столах |

При определении цены защищаемой в кабинете руководителя информации используется качественная шкала:

- очень высокая — цена информации, утечка которой может нанести государству очень большой ущерб или привести к банкротству фирмы;
- очень низкая — цена информации, потеря которой не имеет последствий.

С учетом этого остальные значения цены информации принимают следующее градации:

- высокая — цена информации, утечка которой может нанести государству большой ущерб или заметно ухудшить финансовое положение фирмы;
- средняя — цена информации, потеря которой может привести к существенным для государства и фирмы финансово-экономическим потерям, но может компенсироваться внутренними резервами фирмы;
- низкая — цена информации, утечка которой приводит к малым потерям.

Для государственных структур признаком цены информации может служить ее гриф секретности: «чрезвычайной важности» — чрезвычайно высокая, «совершенно секретно»— очень высокая, секретно — высокая, для «служебного пользования» — низкая.

**План кабинета как объекта защиты**

Кабинет размещен на 3-м этаже 5 этажного кирпичного здания, примыкающего к тротуару улицы. Окна кабинета выходят на улицу. Ширина

улицы составляет около 50 м. На противоположной стороне улицы расположены жилые 12 этажные дома. Территория организации обнесена бетонным забором высотой 2 м, соединенного с наружной стеной административного здания. Вход людей в организацию обеспечивается через контрольно-пропускной пункт **(КПП),** въезд автотранспорта — через ворота. Вход в здание через дверь, открываемую во двор. Окна 1-го этажа укреплены стальными решетками.

Схема расположения организации представлена на рис. 1.

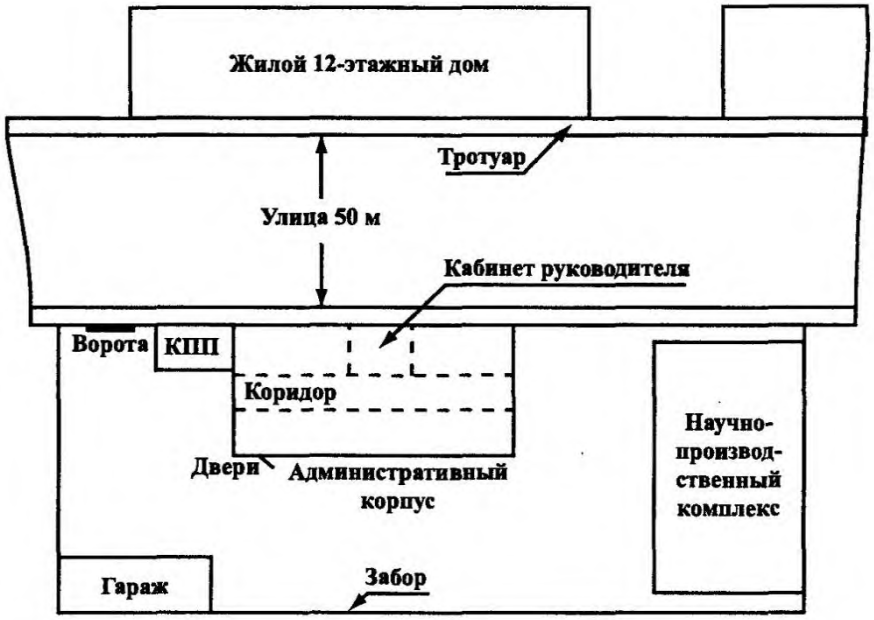



*Рис. 1.* Схема расположения организации

Кабинет имеет два окна, выходящие на улицу, и дверь в приемную. Площадь кабинета составляет около 30 м2, приемная 20 м2. Схематический чертеж варианта кабинета приведен на рис. 2.

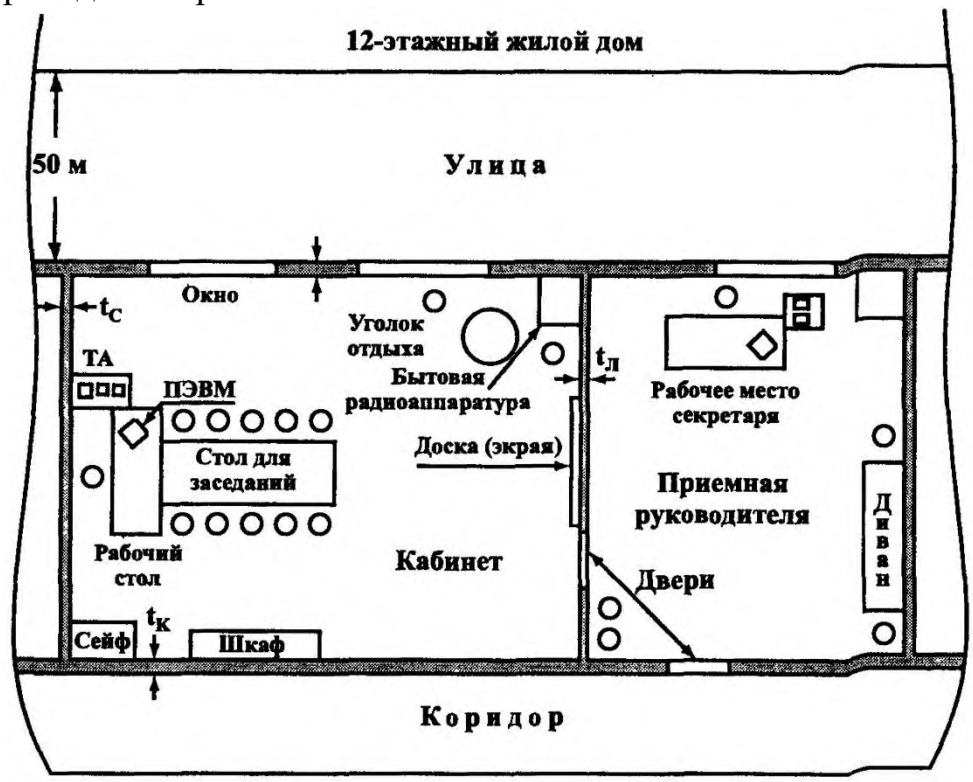


*Рис. 2.* Модель кабинета руководителя

Для описания (моделирования) факторов, влияющих на защищенность информации в кабинете, проводится его обследованиеие. Модель (описание) помещения содержит 5 групп факторов1

- общая характеристика помещения;
- ограждения;
- предметы мебели и интерьера;
- радиоэлектронные средства и электрические приборы;
- средства коммуникаций.

Результаты обследования помещены в табл. П.1.2.

| **1 № \п/п** | ***Факторы влияния*** | ***Параметры*** | ***Примеча-\ ние*** |
|---|---|---|---|
| **1** | ***2*** | ***3*** | ***4*** |
| 1 | **Общая характеристика помещения** | | |
| 1.1 | ГЭтаж | 3 | |
| 1.2 | Площадь, м2 | 30 | |
| 1.3 | : Смежные помещения | справа — приемная; слева — кабинет заместителя; вверху — служебное помещение организации; внизу — служебное помещение организации | |
| 2 | **Ограждения** | | |
| 2.1 | Стены | *наружная* — железобетонная толщи-1 ной 400 мм, на стене укреплены 2 чугунные батареи отопления, соединенные металлическими трубами с трубами в боковых стенах; ***смежная с коридором* — железобетонная** толщиной 140 мм; 2 вентиляционных отверстия | |
| | | ***смежная с приемной* — кирпичная** толщиной в 1 кирпич (270 мм); ***смежная с кабинетом заместителя*** — железобетонная толщиной 140 мм | |
| 2.2 | Потолок | железобетонная плита толщиной 400 мм, окрашенная водо-эмульсионной краской | |
| 2.3 | Пол | железобетонная плита толщиной 400 мм, покрытый паркетом и ковролином | |
| 2.4 | Окна | количество — 2, двухрамные, обращены на улицу, толщина стекла — 3 мм | |
| 2.5 | Дверь | типовая щитовая, без доводчика, выход в приемную | |
| 3 | **Пред [меты мебели и интерьера** | | |
| 3.1 | Картина | размеры рамы 700 х 500 мм, она повешена под углом к стене, смежной с ко-ридором | |
| 3.2 | 1 Шкаф книжный | дверцы стеклянные, на 4 полках книги и папки с документами | |
| 3.3 | Сейф напольный | замок механический кодовый | |
| 3.4 | Стол приставной | имеет под столешницей полку | |
| 3.5 | Столик под телевизионную аппаратуру | **1** ШТ. | |

| | | | |
|---|---|---|---|
| 3.6 | Доска-экран | размер 2000 * 1200 мм, из белого пластика, на котором можно рисовать фломастером и использовать в качестве экрана | |
| 3.7 | Кресло кожаное вращающееся | 1 шт. | |
| 3.8 | Кожаные кресла для отдыха | 2 шт. | |
| 3.9 | Журнальный столик | 1 шт. | |
| 3.10 | Стол для заседаний | рассчитан на 10 человек | |
| 3.11 | Стулья | деревянные полужесткие, 10 шт. | |
| 4 | **Радиоэлектронные средства и электрические приборы** | | |
| | а) Основные | | |
| 4.1 | Компьютер | состав: системный блок, монитор, мышь, клавиатура, 2 динамика, на письменном столе | |
| 4.2 | Телефон закрытой связи (ЗАС) | на приставном столике | |
| 4.3 | Видеодвойка (телевизор +видеомагнитофон) | в случае просмотра видеокассет с закрытой информацией | |
| | б) Вспомогательные | | |
| 4.4 | Телефон городской АТС | на приставном столике | |
| 4.5 | Телефон внутренней АТС | на приставном столике | |
| 4.6 | Концентратор | под столешницей приставного столика | |
| 4.7 | 1 Видеодвойка | 1 просмотр видеокассет с открытой информацией | |
| 4.8 | Вентилятор | на письменном столе | |
| 4.9 | Вторичные часы единого времени | на стене, смежной с приемной | |
| 4.10 | Громкоговоритель оповещения | на стене, смежной с коридором | |
| 4.11 | Настольная лампа | 1 шт. | |
| 4.12 | Люстра из 5 рожков | на потолке | |
| 4.13 | Извещатели пожарные | 2 шт. на потолке | |
| 5 | **Средства коммуникаций** | | |

| | | | |
|---|---|---|---|
| 5.1 | Розетки электропитания | одна возле письменного стола, другая возле видеодвойки | |
| 5.2 | Телефонные розетки | 2 шт,, возле письменного стола | |
| 5.3 | Электропровод ка | скрытая в стенах | |
| 5.4 | Кабели теле-фонных линий | наружные, на стене возле письменно-го стола | |
| 5.5 | Кабель локальной сети ЭВМ | витая пара, укрепленная на стене | |
| 5.6 | Шлейф пожарной сигнализации | наружный, на потолке и стене возле письменного стола | |

## Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

### С.1. Практическая работа

Моделирование технической разведки, по исходным данным для объекта информатизации

**Цель работы:** Приобрести практические навыки в определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации и угрозы несанкционированного доступа.

В качестве изучаемого объекта была взята МУЗ ГБ№6. Тип деятельности: осуществление специализированной медицинской помощи по: контролю качества медицинской помощи; стоматологии; терапевтической; ортопедической; хирургической; ортодонтии; экспертизе временной нетрудоспособности, а так же плановые осмотры для предприятий на прилегающей территории.

1. Специфика организации работы.
    1. Режим работы объекта.

Рабочее время: 8:00 – 18:00. Без перерыва на обед. Рабочие дни: понедельник – пятница. Выходные: суббота, воскресенье. Работа по праздникам, возможны сокращенные рабочие дни.

2. Режим доступа на организацию – свободный, в рабочие дни. Имеется КПП для машин, охранные пункты для пешеходов – отсутствуют. Доступ к оборудованию имеет только специализированный персонал, за каждым закреплено свое рабочее место.
3. Состав сотрудников и посетителей.

Количество сотрудников – 72 человека. Штат: 30 врачей, 5 операторы ПК, 3 бухгалтерия, 5 экономисты, 30 санитары, 2 охранника, 2 плотника.

Количество посетителей – от 1 до 1000 человек в день, стихийно.

1.4.Возможные нарушители среди персонала.

Малооплачиваемые работники - санитары, операторы ПК. Климат в коллективе доброжелательный, конфликты редкие, умеренное уважение к начальству.


2. Специфика расположения организации.

*1. Территория организации и прилегающее к нему пространство в том числе состав и настроение населения, экономические условия, криминогенная обстановка.*

Организация находится в жилом секторе. Южная часть здания окружена лесными посадками. Рядом находятся 3 хозяйственных здания; подсобки, склады, скорая. Территория здания занимает около 10000 кв.м. Сама организация занимает 1700 кв.м.

Процедура доступа на территорию персонала и транспортных средств.

Транспортные средства осуществляют проезд на территорию через контрольно – пропускной пункт; парковка для транспорта клиентов и персонала осуществляется в разных специально отведенных местах. Пропуск посетителей и персонала не контролируется, свободный доступ в помещение, не представляющие важности.

*2. Существующие меры охраны, технические средства защиты.*

По внешнему периметру здание обнесено железобетонным забором высотой 2 м. КПП оборудован камерой: для фиксации проезда транспортных средств на территорию. На КПП находится охранник. Главный вход охраняется охранником. Доступ персонала осуществляется через те же самые входы, что для посетителей. Установлены датчики пожарной безопасности. НА каждом окне имеется датчик – обьемник. В любом кабинете, содержащем важный объект информатизации на окнах навешены решетки и установлена железная дверь.

*3. Условия окружающей среды, возможности обеспечения объекта необходимым в случае чрезвычайных ситуаций.*

Расположенный рядом лес может послужить очагом возгорания, особенно в летний период. Так же лес опасен обвалом деревьев на здание и представляет опасность для каналов связи и энергоснабжения.

## С.2. Лабораторная работа

### Лабораторная работа № 1: Обнаружение полупроводниковых элементов с помощью нелинейного локатора «ЛЮКС»

**Порядок выполнения работы**

1. По техническому описанию прибора и изучить устройство, технические характеристики, инструкцию по эксплуатации нелинейного локатора «ЛЮКС» и меры безопасности при работе с ним.
2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из зоны действия локатора мощных помеховых объектов.
4. Провести обследование эталонных объектов: интегральной микросхемы, металлического предмета, МОМ структуры и элемента, содержащего одновременно полупроводник и МОМ структуру. Выявить и тщательно зафиксировать их отличительные признаки, пользуясь всеми возможностями нелинейного локатора.
5. Провести обследование контрольных образцов, скрытых в специальных коробочках и провести их идентификацию.
6. Составить отчет о проделанной работе, который должен включать: описание нелинейного локатора, принципа его действия, характеристик и основных приемов работы; данные, полученные при исследовании эталонных образцов; результаты идентификации контрольных образцов с подробным обоснованием принятого решения.
7. Отчет составляется персонально каждым студентом, и полученные в нем результаты подлежат защите у преподавателя.

### Лабораторная работа № 3: Обнаружение и определение местоположения радиоизлучающих СТС с помощью многофункционального поискового прибора ST-031 «Пиранья»

Порядок выполнения работы

1. По техническому описанию прибора изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.

2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.
4. Провести обследование помещения в одном из режимов, указанном преподавателем, при обнаружении посторонних сигналов провести их идентификацию и определить характеристики. По возможности установить источник этих излучений и его примерное местоположение.
5. Составить отчет о проделанной работе.
6. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

## Лабораторная работа № 4: Поиск технических средств негласного получения информации в линиях сети переменного тока с помощью многофункционального поискового прибора ST-031 «Пиранья»

Порядок выполнения работы

7. По техническому описанию прибора изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.
8. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
9. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.
10. Провести обследование помещения, линии сети переменного тока и токопроводящих линий.
11. Составить отчет о проделанной работе.
12. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

## Лабораторная работа № 5: Поиск технических средств негласного получения информации в телефонных линиях с помощью многофункционального поискового прибора ST-031 «Пиранья».

Порядок выполнения работы

13. По техническому описанию прибора изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.
14. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
15. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.
16. Провести обследование помещения, телефонных линий, линий пожарной и охранной сигнализации.
17. Составить отчет о проделанной работе.
18. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

## Лабораторная работа № 6: Поиск средств высокочастотного навязывания многофункционального поискового прибора ST-031 «Пиранья».

Порядок выполнения работы

1. По техническому описанию прибора изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.
2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.

4. Провести обследование помещения на наличие средств высокочастотного навязывания.
5. Составить отчет о проделанной работе.
6. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Лабораторная работа № 7: Поиск технических средств негласного получения информации в телефонных линиях, линиях пожарной и охранной сигнализации многофункционального поискового прибора ST-031 «Пиранья».

Порядок выполнения работы

19. По техническому описанию прибора изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.
20. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
21. Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.
22. Провести обследование помещения, телефонных линий, линий пожарной и охранной сигнализации.
23. Составить отчет о проделанной работе.
24. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя, проводящего занятие.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

**Блок Д. Задания для использования в рамках промежуточной аттестации**

## Д1.Перечень контрольных вопросов

1. Общая модель защиты от ТР на скрываемом объекте.
2. Принципы защиты объектов от технических разведок
3. Общая классификация и характеристика способов защиты от ТР
4. Демаскирующие признаки объектов
5. Защита объектов от акустической речевой разведки
6. ВЧ-навязывание. Устройства для перехвата речевой информации в проводных каналах.
7. ВЧ-навязывание. Перехват речевой информации с использованием радиоканала.
8. Защита информации от высокочастотного навязывания.
9. Оптические средства добывания информации.
10. Перехват информации в линиях связи. Зоны подключения.
11. Зоны подключения. Перехват телефонных переговоров в зонах «А», «Б», «В».
12. Перехват информации в GSM.
13. Основные способы несанкционированного доступа в компьютерных сетях.
14. Криптографические методы и средства защиты. Аналоговое преобразование.
15. Криптографические методы и средства защиты. Цифровое шифрование.

**Для проверки сформированности компетенции ПК-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем**
**ИПК-3.2. Учитывает особенности средств защиты информации при проектировании системы защиты информации**

### Блок А. Задания репродуктивного уровня («знать»)

## А.1 Тестовые задания по дисциплине

1. К естественным техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ТСПИ), относятся:

А) Электромагнитные технические каналы утечки информации.
Б) Электрические технические каналы утечки информации.
В) Акустоэлектромагнитные технические каналы утечки информации.
Г) Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ.
Д) Технические каналы утечки информации, создаваемые путем внедрение в ТСПИ электронных устройств перехвата информации (закладных устройств).

2. К специально создаваемым техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ТСПИ), относятся:
А) Электромагнитные технические каналы утечки информации.
Б) Электрические технические каналы утечки информации.
В) Акустоэлектромагнитные технические каналы утечки информации.
Г) Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ.
Д) Технические каналы утечки информации, создаваемые путем внедрение в ТСПИ электронных устройств перехвата информации (закладных устройств).

3. К техническим каналам утечки информации (ТКУИ), обрабатываемой техническими средствами (ТСПИ), относятся:
А) Электромагнитные технические каналы утечки информации.
Б) Электрические технические каналы утечки информации.
В) Акустоэлектромагнитные технические каналы утечки информации.
Г) Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ.
Д) Технические каналы утечки информации, создаваемые путем внедрение в ТСПИ электронных устройств перехвата информации (закладных устройств).

4. К техническим каналам утечки речевой информации относятся:
А) Прямой акустический технический канал утечки информации.
Б) Акустовибрационный технический канал утечки информации.
В) Акустооптический технический канал утечки информации.
Г) Акустоэлектрический технический канал утечки информации.
Д) Акустоэлектромагнитный технический канал утечки информации.

5. К естественным техническим каналам утечки речевой информации относятся:
А) Прямые акустические технические каналы утечки информации.
Б) Акустооптический технические каналы утечки информации.
В) Акустоэлектромагнитный (пассивный) технический канал утечки информации.
Г) Акустовибрационные технические каналы утечки информации.
Д) Акустоэлектрический (пассивный) технический канал утечки информации.

6. К специально создаваемым техническим каналам утечки речевой информации относятся:
А) Акустоэлектрический (пассивный) технический канал утечки информации.
Б) Акустооптический технический канал утечки информации.
В) Акустоэлектромагнитный (активный) технический канал утечки информации.
Г) Акустовибрационные технические каналы утечки информации.
Д) Акустоэлектрический (активный) технический канал утечки информации.

7. По каким техническим каналам возможен перехват речевой информации без проникновения в пределы КЗ объекта:

А) Прямые акустические технические каналы утечки информации.
Б) Акустовибрационный технический канал утечки информации.
В) Акустооптический технический канал утечки информации.
Г) Акустоэлектрический технический канал утечки информации.
Д) Акустоэлектромагнитный технический канал утечки информации.

8. Какие способы перехвата речевой информации требуют проникновения в выделенное помещение:

А) Перехват акустических колебаний, возникающих при ведении разговоров, закладными устройствами с датчиками микрофонного типа.
Б) Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, закладными устройствами с датчиками контактного типа.
В) Перехват вибрационных колебаний, возникающих при ведении разговоров в ограждающих конструкциях и инженерных коммуникациях, электронными стетоскопами.
Г) Перехват информативных электрических сигналов, возникающих вследствие акустоэлектрических преобразований акустических сигналов элементами ВТСС, техническими средствами, построенными на базе низкочастотных усилителей, подключаемыми к соединительных линий ВТСС.
Д) Перехват акустической (речевой) информации методом «высокочастотного облучения» ВТСС, имеющих в своем составе акустоэлектрические преобразователи.

9. Для передачи информации, перехваченной закладными устройствами перехвата речевой информации, используются:

а) Специально проложенная линия.
б) Линия электропитания 220 В, 50 Гц.
в) Телефонная линия.
г) Радиоканал.
д) Оптический канал.

**А2. Вопросы для устного опроса**

1. Типовая структура и виды технических каналов утечки информации.
2. Каналы утечки речевой информации.
3. Каналы утечки информации при её передаче по каналам связи.
4. Каналы утечки видовой информации.
5. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.
6. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

7. Общие принципы выявления
8. Методы поиска закладных устройств как физических объектов
9. Методы поиска ЗУ как электронных средств
10. Панорамные приемники и их основные характеристики
11. Принципы построения и виды панорамных приемников
12. Компьютерные программы для управления панорамными приемниками
13. Программно-аппаратные комплексы
14. Нелинейные радиолокаторы
15. Назначение и содержание технического контроля
16. Контроль эффективности принятых мер защиты от радиотехнической разведки
17. Контроль эффективности принятых мер защиты от инфракрасной разведки
18. Контроль состояния защиты информации при эксплуатации слаботочного оборудования
19. Методологический подход к определению нормативных показателей эффективности защиты

## Блок В. Задания реконструктивного уровня («уметь»)

### В1. Тематика рефератов

1. «Детекторы лжи» и их использование для получения информации.
2. Способы и принципы инженерно технической защиты информации.
3. Контролируемая зона и критерий защищённости СВТ.
4. Средства и методы (не меньше двух) обнаружения закладных устройств.
5. Способы подключения и защита телефонной линии.
6. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него.

### В2. Тематика презентаций

1. «Детекторы лжи» и их использование для получения информации.
2. Способы и принципы инженерно технической защиты информации.
3. Контролируемая зона и критерий защищённости СВТ.
4. Средства и методы (не меньше двух) обнаружения закладных устройств.
5. Способы подключения и защита телефонной линии.
6. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него.

### В3. Практическая работа

**Практическая работа №1.**

**Цель работы:** Приобрести практические навыки в определении степени защищенности объекта *информатизации* путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации.

**Определение потенциальных и реальных ТКУИ**

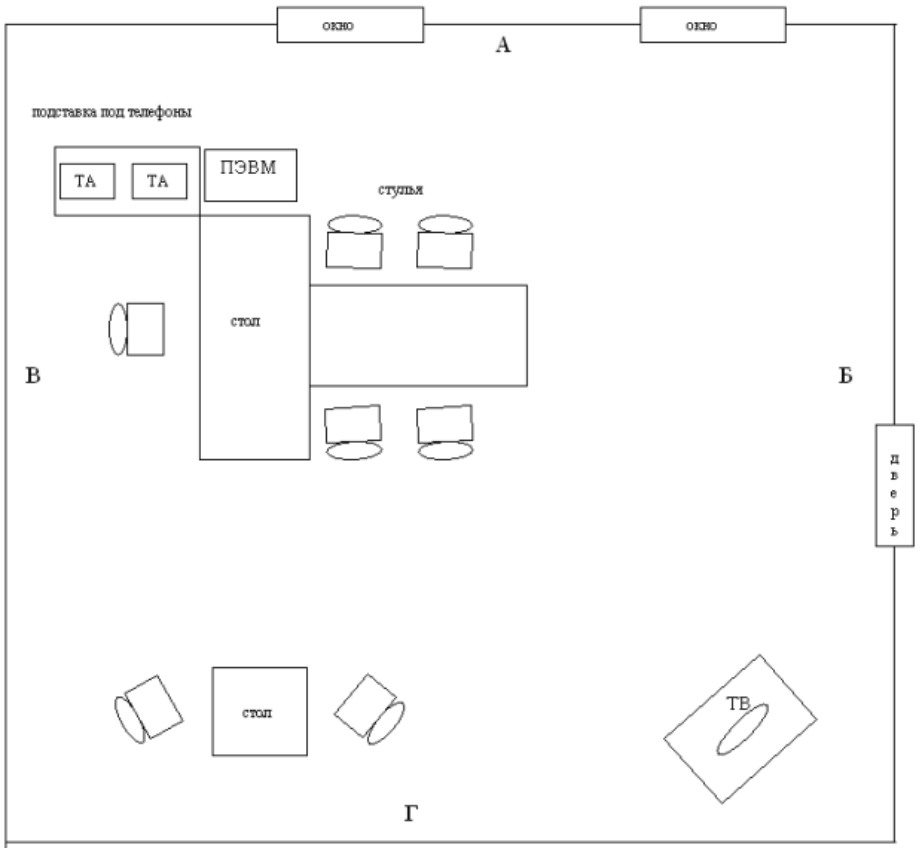
Ниже приведена примерная характеристика защищаемого объекта (исходные данные).

1. Защищаемое помещение расположено на четвертом этаже 7-этажного здания. Все здание принадлежит одной организации:
   - Сверху расположены служебные помещения.
   - Снизу расположены технические помещения (туалет, электрощитовая).
   - Со стороны стены Б расположена приемная.
   - Со стороны стены Г расположен общий коридор.

   Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением.

   Окна помещения оборудованы шторами, смотрят на жилой дом расположенный на расстоянии 30 метров.
2. Из мебели в помещении установлены рабочий и журнальный столы, стулья, подставки под: телефоны, ПЭВМ и *телевизор*.
3. Из основных технических средств в помещении установлен телефон внутренней конфиденциальной связи, ПЭВМ включенная в локальную сеть.
4. Из вспомогательных технических средств в помещении установлен телефон ГТС, *телевизор*, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, питание оборудования).
5. Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.
6. Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. В ночное время помещение закрывается на ключ, сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.
7. Доступ штатных сотрудников к служебной информации не разграничен.

Схема объекта




В качестве примера представим порядок рассуждения защищенности объекта со стороны окон. При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допущено использование оговорок типа " если.... то....".

1. Просмотр помещения со стороны улицы, ввиду того, что помещение находится на 4 этаже, не возможен. Так как возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, существует потенциальный канал утечки видовой информации.
   Однако, если организационными мероприятиями (соответствующим инструктажем ответственных лиц) введено обязательное зашторивание окон во время проведением совещаний, работы с документами и т.п., то реального визуально оптического *канала утечки информации* нет.
   В качестве дополнительных мер можно ввести периодический контроль за соблюдением сотрудниками правила зашторивания, а также поставить тонированные или рифленые стекла.
2. Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустический информации.
   Однако, если организационными мероприятиями введено обязательное закрытие окон и форточек во время проведения совещаний, реального акустического *канала утечки информации* нет.

В качестве дополнительной меры можно установить кондиционер или приобрести генератор белого шума и включать его во время проведения совещаний.

3. Так как возможен съем информации о ведущихся в помещении разговорах с оконных стекол, за счет их вибрации, при использовании лазерного микрофона, при расположении поста перехвата в жилом доме, существует еще один потенциальный канал утечки акустической информации.

   В данном случае с помощью одних организационных мероприятий устранить канал утечки не представляется возможным. Однако реальное существование канала утечки может быть констатировано лишь после проведения инструментальных измерений.

   По результатам инструментальной проверки будет определяться необходимость проведение защитного мероприятия, например установка рифленых стекол или зашумление стекол и пространства между ними.

В заключение первого этапа можно предложить установку стекол с рифленой поверхностью и кондиционера. Решение представляется оптимальным, т.к. акустический и визуально оптический каналы устраняются при минимальных финансовых затратах. Также, в дальнейшем, обеспечивается *удобство эксплуатации* объекта и исключается негативный *человеческий фактор*.

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

- скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с интенсивным движением затруднительно, т.к. подозрительные лица, транспортные средства и т.п. привлекают к себе внимание, легко визуально обнаруживаются;
- скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами расположенными напротив окон защищаемого помещения, вполне реализуемо.

Необходимо, если имеется такая возможность, проверить благонадежность (лояльность) жильцов в квартирах, потенциально пригодных для организации поста перехвата (сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица бывшие в конфликте с законом и т.п.). Возможности организации постов перехвата на технических этажах и т.п.

В случае получения в ходе проверки положительных данных можно заключить, что защитные мероприятия не требуются вообще. С точки зрения защиты от случайных утечек, например прослушивания, можно заключить, что улица с интенсивным автомобильным и пешеходным движением создает достаточно сильную акустическую помеху, за которой разговоры случайными

прохожими различаться не будут. При необходимости в этом можно убедиться экспериментально.

В случае получения в ходе проверки отрицательных или неоднозначных данных оптимальным остается вариант указанный в заключение первого этапа.

**Самостоятельная часть работы**

В самостоятельной части работы предлагается:

- выявить оставшиеся, потенциально возможные каналы утечки информации (с учетом исходных данных, используя, при необходимости оговорки);
- смоделировать возможные действия технических разведок, определить реальные каналы утечки информации;
- доказать целесообразность и предложить проведение тех или иных защитных мероприятий.

Примечание: При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допускается использовать оговорку типа " если.... то....".

## Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

### С.1. Лабораторная работа

Лабораторная работа № 1: Исследование широкополосного приемника AR8200

Порядок выполнения работы

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации приемника и меры безопасности при работе с ним.
2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.
4. Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями приѐмника.
5. Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера.
6. Составить отчет о проделанной работе, который должен включать:

– описание индикатора, принципа его действия, характеристик и основных приемы работы;
– данные, полученные при исследовании ЭМО в лаборатории;
– результаты идентификации контрольных образцов с подробным обоснованием принято решения.

7. Отчет составляется персонально каждым студентом, и полученные в нем результаты подлежат защите у преподавателя.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

1. Придерживаться рекомендаций, указанных в Лабораторном практикуме.
2. Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
3. Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
4. Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Лабораторная работа № 2: Поиск радиопередатчиков с помощью цифрового индикатора BLACK HUNTER.

Порядок выполнения работы

1. По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации цифрового индикатора BLACK HUNTER.
2. Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.
4. Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь возможностями цифрового индикатора BLACK HUNTER.
5. Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию.
6. Составить отчет о проделанной работе, который должен включать:
   - описание индикатора, принципа его действия, характеристик и основных приемы работы;
   - данные, полученные при исследовании ЭМО в лаборатории;
   - результаты идентификации контрольных образцов с подробным обоснованием принято решения.
7. Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

- Придерживаться рекомендаций, указанных в Лабораторном практикуме.
- Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

- Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
- Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

**Блок Д. Задания для использования в рамках промежуточной аттестации**

**Д1.Перечень контрольных вопросов**

16. Методы и средства поиска закладных устройств как электронных средств.
17. Методы и средства поиска закладных устройств как физических объектов.
18. Виды побочных электромагнитных излучений и наводок
19. Структура и классификация технических каналов утечки информации.
20. Каналы утечки речевой информации.
21. Каналы утечки информации при её передаче по каналам связи.
22. Закладные устройства: общие понятия и классификация.
23. Радиозакладные устройства.

## РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

Для студентов очно-заочной формы обучения применятся 4-балльная шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

| **уровни освоения компетенций** | продвинутый уровень | базовый уровень | пороговый уровень | допороговый уровень |
|---|---|---|---|---|
| **100 – балльная шкала** | 85 и ≥ | 70 – 84 | 51 – 69 | 0 – 50 |
| **4 – балльная шкала** | «отлично» | «хорошо» | «удовлетворительно» | «неудовлетворительно» |

**Шкала оценок при текущем контроле успеваемости по различным показателям**

| ***Показатели оценивания сформированности компетенций*** | ***Баллы*** | ***Оценка*** |
|---|---|---|
| Устный опрос | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Подготовка реферата | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Подготовка презентации | 0-5 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Тестирование | 0-30 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Выполнение практических заданий | 0-10 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |
| Выполнение лабораторной работы | 0-15 | «неудовлетворительно»<br>«удовлетворительно»<br>«хорошо»<br>«отлично» |

**Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости**

| ***Баллы*** | ***Оценка*** | ***Уровень освоения компетенций*** | ***Критерии оценивания*** |
|---|---|---|---|
| 0-50 | «неудовлетворительно» | Допороговый уровень | Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины |
| 51-69 | «удовлетворительно» | Пороговый уровень | Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок |
| 70-84 | «хорошо» | Базовый уровень | Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок |
| 85-100 | «отлично» | Продвинутый уровень | 100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами |

**Шкала оценок по промежуточной аттестации**

| ***Наименование формы промежуточной аттестации*** | ***Баллы*** | ***Оценка*** |
|---|---|---|
| Экзамен | 0-30 | «неудовлетворительно» «удовлетворительно» |

| | | |
|---|---|---|
| | | «хорошо»<br>«отлично» |

**Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся**

| ***Баллы*** | ***Оценка*** | ***Уровень освоения компетенций*** | ***Критерии оценивания*** |
|---|---|---|---|
| 0-9 | «неудовлетворительно» | Допороговый уровень | Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы |
| 10-16 | «удовлетворительно» | Пороговый уровень | Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме. |
| 17-23 | «хорошо» | Базовый уровень | Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания |
| 25-30 | «отлично» | Продвинутый уровень | Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой |

| | | | |
|---|---|---|---|
| | | | дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами |

## РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

### Методика оценивания ответов на устные вопросы

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 1. Полнота данных ответов;<br>2. Правильность ответов на вопросы. | Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, привести необходимые примеры. Изложение материала последовательно и правильно. |
| 3-4 | «хорошо» | | Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет. |
| 1-2 | «удовлетворительно» | | Студент обнаруживает знание и понимание основных положений данного задания, но:<br>1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил;<br>2) не умеет достаточно глубоко и доказательно |

| | | | |
|---|---|---|---|
| | | | обосновать свои суждения и привести свои примеры;<br>3) излагает материал непоследовательно и допускает ошибки. |
| 0 | «неудовле твори-тельно» | | Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал. |

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

**Методика оценивания выполнения тестов**

| Баллы | Оценка | Показатели | Критерии |
|---|---|---|---|
| 25-30 | «отлично» | 1. Полнота выполнения тестовых заданий;<br>2. Своевременность выполнения;<br>3. Правильность ответов на вопросы. | Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос |
| 19-24 | «хорошо» | | Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др. |
| 15-18 | «удовлетв орительно » | | Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками. |
| 0-14 | «неудовле твори-тельно» | | Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях). |

Тема реферата выбирается студентом самостоятельно из предложенного

списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

**Методика оценивания выполнения рефератов**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 1. Полнота выполнения рефератов;<br>2. Своевременность выполнения;<br>3. Четкость изложения идеи реферата во время защиты. | Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время защиты. |
| 3-4 | «хорошо» | | Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; выступление во время защиты требует дополнительных вопросов. |
| 1-2 | «удовлетворительно» | | Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы во время выступления. |
| 0 | «неудовлетвори-тельно» | | Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы, не проведена защита реферата. |

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На

подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

**Методика оценивания выполнения презентаций**

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 5 | «отлично» | 4. Полнота выполнения;<br>5. Своевременность выполнения;<br>6. Четкость изложения идеи презентации во время защиты. | Выполнены все требования к подготовке презентации: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, четкое и последовательное выступление во время демонстрации. |
| 3-4 | «хорошо» | | Основные требования к подготовке презентации выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации; имеются упущения в оформлении; выступление во время демонстрации требует дополнительных вопросов. |
| 1-2 | «удовлетворительно» | | Имеются существенные отступления от требований к презентации. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентации или при ответе на дополнительные вопросы во время выступления. |
| 0 | «неудовлетвори-тельно» | | Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы, не проведена демонстрация презентации. |

Практические задания выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или

оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента.

### Методика оценивания выполнения практических заданий

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 9-10 | «отлично» | 1. Полнота выполнения практического задания;<br>2. Своевременность выполнения задания;<br>3. Самостоятельность решения. | Основные требования к выполнению задания выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели |
| 6-8 | «хорошо» | | Основные требования к выполнению задания реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений |
| 3-5 | «удовлетворительно» | | Имеются существенные отступления от выполнения работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат |
| 1-2 | «неудовлетвори-тельно» | | Задача выполнения работы не раскрыта, обнаруживается существенное непонимание проблемы |

Лабораторные работы выполняются в специализированной аудитории во время лабораторных занятий. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

### Методика оценивания выполнения *лабораторных работ*

| ***Баллы*** | ***Оценка*** | ***Показатели*** | ***Критерии*** |
|---|---|---|---|
| 13-15 | «отлично» | 4. Полнота | Основные требования к выполнению задания лабораторной работы выполнены. |

| | | | |
|---|---|---|---|
| | | выполнения задания лабораторной работы; 5. Своевременность выполнения задания лабораторной работы; 6. Самостоятельность решения. | Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели |
| 9-12 | «хорошо» | | Основные требования к выполнению задания лабораторной работы реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений |
| 5-8 | «удовлетворительно» | | Имеются существенные отступления от выполнения лабораторной работы. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат |
| 0-4 | «неудовлетвори-тельно» | | Шаги выполнения лабораторной работы не выполнены, обнаруживается существенное непонимание проблемы. |

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной дисциплине, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

Время подготовки ответа при сдаче экзамена в устной форме должно составлять не менее 40 минут (по желанию обучающегося ответ может быть досрочным). Время ответа – не более 15 минут.

При подготовке к устному экзамену экзаменуемый, как правило, ведет записи в листе устного ответа, который затем (по окончании экзамена) сдается экзаменатору.

Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.

Оценка результатов устного аттестационного испытания объявляется обучающимся в день его проведения.

**Лист актуализации оценочных материалов по дисциплине «Противодействие техническим разведкам»**

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «_____»_____ 20___ г. №_____

Зав. кафедрой _____