



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.03 ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ
КАНАЛАМ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Доцент кафедры Информационно-измерительных систем, к.т.н.
Зубов А. А.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся способности решать задачи, связанные с инженерно-технической защитой информации, включая практическое применение знаний в конкретных условиях и использование системного подхода для анализа и обеспечения защиты информации.

Задачи изучения дисциплины:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных помещений от утечки акустической информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-11 Способен проводить эксперименты по заданной методике и обработку их результатов

ОПК-11.1 Знает фундаментальные основы и особенности применения методов, применяемых для защиты информации автоматизированных систем

Знать:

ОПК-11.1/Зн4 Компоненты систем защиты информации автоматизированных систем (основные понятия и терминологию, принятые в проектировании систем инженерно-технической защиты объектов)

Уметь:

ОПК-11.1/Ум2 Разрабатывать компоненты систем защиты информации автоматизированных систем (выбирать наиболее рациональные методы противодействия угрозам охраняемому объекту)

Владеть:

ОПК-11.1/Нв3 Навыками разработки компонентов систем защиты информации автоматизированных систем

ОПК-11.2 Проводит эксперименты в области информационной безопасности автоматизированных систем

Знать:

ОПК-11.2/Зн2 Технические средства и методы разведки, используемые для перехвата информации по техническим каналам, и способы противодействия таким средствам

Уметь:

ОПК-11.2/Ум3 Выявлять возможные технические каналы утечки информации на объектах информатизации и оценивать степень их опасности для конфиденциальной информации

Владеть:

ОПК-11.2/Нв2 Методикой категорирования объектов информатизации и выбора необходимых средств защиты в зависимости от класса защищаемой информации

ОПК-11.3 Обработывает результаты эксперимента в соответствии с фундаментальными закономерностями и с применением методом математической статистики

Знать:

ОПК-11.3/Зн2 Нормативные правовые акты и методические документы, регулирующие вопросы инженерно-технической защиты информации и требования к защите помещений и технических средств

Уметь:

ОПК-11.3/Ум2 Проводить инструментальный контроль эффективности принятых мер защиты и проверять защищаемые помещения на отсутствие закладных устройств

Владеть:

ОПК-11.3/Нв3 Способами организации инженерно-технической защиты информации на объекте, включая проектирование систем защиты и контроль их функционирования

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.О.19.03 «Защита информации от утечки по техническим каналам» относится к обязательной части образовательной программы и изучается в семестре(ах): 8.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
8 семестр	144	4	30	30	30	18	Экзамен (36)
Всего	144	4	30	30	30	18	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий (часы промежуточной аттестации не указываются)

Наименование раздела, темы	Лекционные занятия	Лабораторные занятия	Практические занятия	Самостоятельная работа	Учебные результаты, соответствующие результатам освоения программы
----------------------------	--------------------	----------------------	----------------------	------------------------	--

	Всего	Лабо ра	Лекци с	Практи с	Самост я	Планир обучен результ програ
Раздел 1. Технические каналы утечки информации	38	16	16		6	ОПК-11.1 ОПК-11.2
Тема 1.1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации	6		4		2	
Тема 1.2. Технические каналы утечки акустической (речевой) информации	16	8	6		2	
Тема 1.3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	16	8	6		2	
Раздел 2. Защита информации от утечки по техническим каналам	70	14	14	30	12	ОПК-11.1 ОПК-11.2 ОПК-11.3
Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	26	6	6	10	4	
Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам	26	6	4	12	4	
Тема 2.3. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	16	2	4	8	2	
Тема 2.4. Методы и средства выявления электронных устройств негласного получения информации	2				2	
Итого	108	30	30	30	18	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Технические каналы утечки информации

Тема 1.1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации). Нормативные документы по технической защите информации. Термины и определения в области технической защиты информации: объект информатизации, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка по техническому каналу, перехват информации, средство разведки, специальное техническое средство негласного получения информации, посторонние проводники, контролируемая зона, технический канал утечки информации.

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 1.2. Технические каналы утечки акустической (речевой) информации

Характеристики речевого сигнала. Общая характеристика и классификация технических каналов утечки акустической информации. Прямые акустические каналы утечки речевой информации. Акустовибрационные каналы утечки речевой информации. Акустооптический (оптикоэлектронный, лазерный) канал утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Акустоэлектромагнитные каналы утечки речевой информации. Средства акустической разведки и их технические характеристики.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Тема 1.3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки информации, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки информации, создаваемый путем «высокочастотного облучения» СВТ. Технический канал утечки информации создаваемый путем внедрения в СВТ электронных устройств негласного получения информации.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Защита информации от утечки по техническим каналам

Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Классификация способов и средств защиты объектов информатизации. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства вычислительной техники.

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата речевой информации (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

Текущий контроль
Вид (форма) контроля
Тестирование
Практическая работа

Тема 2.3. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Методика оценки возможностей средств акустической разведки по перехвату речевой информации. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

Текущий контроль
Вид (форма) контроля
Тестирование
Практическая работа

Тема 2.4. Методы и средства выявления электронных устройств негласного получения информации

Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 8 семестр.

Допуском к экзамену является сдача всех практических и лабораторных работ.

Экзамен оценивается по пятибальной шкале:

Оценка «отлично» (зачтено): студентом дан полный, в логической последовательности развернутый ответ на поставленные вопросы, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок.

Оценка «хорошо» (зачтено): студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускаются неточности в ответе. Решил предложенные практические задания с небольшими неточностями.

Оценка «удовлетворительно» (зачтено): студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.

Оценка «неудовлетворительно» (не зачтено): студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, неумением давать аргументированные ответы. Выводы поверхностны. Решение практических заданий не выполнено. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

7. Оценочные материалы текущего контроля

Раздел 1. Технические каналы утечки информации

Контролируемые ИДК: ОПК-11.1 ОПК-11.2

Тема 1.1. Место технической защиты информации в государственной системе защиты информации в Российской Федерации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Виды технических каналов утечки информации:

1. Каналы утечки, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации
2. (ТСПИ);
3. Каналы утечки речевой информации;
4. Утечка информации при ее передаче по каналам связи;
5. Технические каналы утечки видовой информации.

2. Технические каналы утечки информации при передаче по каналам связи:

1. Электромагнитные
2. Электрические
3. Индукционные
4. Градиентные

3. По информативности ТКУИ делятся на:

1. Информативные
2. Малоинформативные
3. Неинформативные
4. Бесполезные

4. По времени функционирования ТКУИ выделяют:

1. Постоянные
2. Эпизодические
3. Случайные
4. Редкие

5. Средства активной акустической и вибрационной защиты речевой информации – это:

1. Технические средства формирования маскирующих акустических и вибрационных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.
2. Помещение, предназначенное для проведения переговоров, содержащих конфиденциальную информацию, и прошедшее процедуру аттестации в соответствии с законодательством Российской Федерации.

6. Технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях:

1. Вспомогательные технические средства и системы
2. Средства применяемые для обеспечения жизнедеятельности сотрудников

7. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

8. Как называется попытка реализации угрозы?

9. Непосредственная причина возникновения угрозы называется

10. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?

11. Как называется неконтролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?

12. К какому техническому каналу утечки информации относится несанкционированное распространение за пределы контролируемой зоны вещественных носителей с защищаемой информацией?

13. Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?

14. Как называется пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения?

Тема 1.2. Технические каналы утечки акустической (речевой) информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Пространственное зашумление предполагает:
 1. Создание маскирующих помех в окружающем ОТСС пространстве
 2. Создание маскирующих помех в линиях передачи информации
2. В каком техническом канале утечки информации носителем является упругая акустическая волна?
3. В каких технических каналах утечки акустической информации средой распространения информативного сигнала являются конструкции зданий, стены, потолки и другие твердые тела?
4. В каких технических каналах утечки акустической информации основным средством съема информации является микрофон?
5. В каких технических каналах утечки акустической информации основным средством съема информации является лазер?
6. Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС есть элементы, обладающие "микрофонным эффектом"?
7. Верно ли определение: акустический сигнал - это возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности?
 1. Верно
 2. Не верно
8. Основными путями прохождения акустических волн из помещения являются:
 1. Воздушный перенос: прохождение через открытые окна, двери, щели, поры, вентиляционные воздуховоды
 2. Материальный перенос: прохождение через материал стены или по трубам отопления, газопровода, водопровода в виде продольных колебаний
 3. Мембранный перенос: передача колебаний посредством поперечных колебаний перегородки (стекла, стены и пр.)
9. Технические каналы утечки речевой информации делятся на:
 1. Воздушные
 2. Виброакустические
 3. Оптико-электронные
 4. Акустоэлектрические
 5. Параметрические
10. Верно ли утверждение, что в вибрационных технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела?
 1. Верное
 2. Не верно
11. В воздушных технических каналах утечки информации средой распространения акустических сигналов является:
 1. Провода
 2. Воздух
12. Спектр речи человека лежит в диапазоне:
 1. От 20Гц до 20кГц
 2. От 200Гц до 2000кГц

3. От 20Гц до 20МГц

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Исследование способов и принципов построения и работы технических средств подслушивания акустической (речевой) информации

Моделирование стетоскопа, исследование его характеристик и принципов работы

Тема 1.3. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Для персонального компьютера потенциально-информативными ПЭМИ являются излучения:

1. Цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате.

2. Цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора

3. IDE шлейф подключения DVDRom

2. В цепях, выполняющие вспомогательные функции, по которым никогда не будут передаваться сигналы, содержащие закрытую информацию, возникают излучения, порождаемые протеканием токов в таких цепях:

1. Неинформативные излучения

2. Слаботочные излучения

3. Наиболее опасным аналоговым видеотрактом является:

1. VGA

2. LPT

3. USB

4. SSD

4. Укажите основные функции селективного приемника сигналов:

1. Выбор (селекцию) носителя с нужной получателю информацией

2. Усиление принятого сигнала до значений, обеспечивающих съём информации

3. Съём информации с носителя (демодуляцию, декодирование)

4. Передачу информации в радиоканал

5. Линейное зашумление включает в себя:

1. Линейное зашумление линий электропитания и заземления;

2. Линейное зашумление посторонних проводников и соединительных линий ВТСС

6. Как называется технический канал утечки информации, при котором производится съём информации с линии связи контактного подключения аппаратуры злоумышленника?

7. Как называется технический канал утечки информации, заключающийся в перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи?

8. Как называется технический канал утечки информации, при котором производится бесконтактный съём информации с кабельных линий связи?

9. Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС под давлением звуковой волны может измениться взаимное расположение элементов схем, проводов и т.п.?

10. Как называются электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях?

11. Что значит буква "Н" в аббревиатуре ПЭМИН?

12. Назовите способы получения видовой информации:

13. Сосредоточенная случайная антенна:

1. Компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д
2. Способна принимать только узконаправленные сигналы

14. Причинами возникновения электрических каналов утечки информации могут быть:

1. наводки электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны
2. просачивание информационных сигналов в линии электропитания ОТСС
3. просачивание информационных сигналов в систему заземления ОТСС
4. использование закладных устройств

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Исследование сигнальных демаскирующих признаков радиоэлектронных средств

Определение вероятности обнаружения радиоэлектронного средства аппаратурой радиотехнической разведки. Моделирование и исследование сигнальных демаскирующих признаков работы радиопередатчиков.

2. Исследование источников опасных сигналов

Исследование побочных электрических сигналов, возникающих за счет эффекта акустоэлектрического преобразования. Моделирование и исследование физического эффекта паразитной генерации высокочастотных сигналов.

3. Моделирование и исследование технических каналов утечки информации, возникающих за счет побочных электромагнитных излучений и наводок

Моделирование и исследование электромагнитных каналов утечки информации, возникающих от технических средств передачи, хранения, обработки и отображения информации (ТСПИ). Моделирование и исследование электрических каналов утечки информации, наводимых в линиях электропитания и заземления ТСПИ, соединительных линиях ВТСС и посторонних проводниках.

Раздел 2. Защита информации от утечки по техническим каналам

Контролируемые ИДК: ОПК-11.1 ОПК-11.2 ОПК-11.3

Тема 2.1. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Пассивные методы защиты информации направлены на:

1. ослабление побочных электромагнитных излучений ОТСС на границе контролируемой зоны
2. ослабление наводок побочных электромагнитных излучений в посторонних проводниках, соединительных линиях цепях электропитания и заземления, выходящих за пределы контролируемой зоны;
3. исключение или ослабление просачивания информационных сигналов в цепи электропитания и заземления, выходящие за пределы контролируемой зоны

2. К пассивным методам защиты относятся:

1. Применение разделительных трансформаторов и помехоподавляющих фильтров
2. Экранирование
3. Заземление всех устройств, как необходимое условие эффективной защиты информации

Тема 2.2. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Звукоизоляция относится к:

1. Пассивные методы защиты акустической (речевой) информации
2. Методам повышения качества звучания

2. Для перехвата акустических колебаний используются:

1. Контактные микрофоны (стетоскопы)
2. Громофоны

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Высокочастотного навязывания

Моделирование и исследование процесса паразитной (несанкционированной) модуляции (интермодуляции). Моделирование и исследование принципов действия средств высокочастотного навязывания.

2. Исследование принципов построения и работы средств экранирования, фильтрации информационных сигналов и генерации шума для энергетического скрывания

Моделирование и исследование принципов работы средств экранирования ПЭМИН. Моделирование и исследование принципов построения и работы средств генерации шума для энергетического скрывания.

3. Исследование принципов построения и работы аналоговых скремблеров речевого сигнала

Преобразование речи в цифровую форму. Основные принципы построения систем закрытия речи. Ознакомление с принципом работы скремблера

Тема 2.3. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Помещение, предназначенное для проведения переговоров, содержащих конфиденциальную информацию, и прошедшее процедуру аттестации в соответствии с законодательством Российской Федерации.- это:

1. Защищаемое помещение
2. Бомбоубежище
3. Бункер

2. Для персонального компьютера неинформативными ПЭМИ являются излучения:

1. Цепи формирования и передачи сигналов синхронизации
2. Цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате

3. В процессе проведения оценки защищенности ОТСС от утечки по каналам ПЭМИН необходимо производить измерения следующих физических величин:

1. Напряженность электромагнитного поля по электрической составляющей (Е)
2. Напряженность магнитного поля (Н)
3. Напряжение в линиях и токоведущих конструкциях (U)
4. Плотность светового потока

4. Источниками ПЭМИ в АС являются:

1. Все линии и устройства, в которых присутствуют те или иные электрические сигналы
2. CD, DVD диски

5. Источниками информативных ПЭМИ в АС являются:

1. Клавиатура
2. Видео тракт (монитор, кабели, видеоадаптер)
3. CD, DVD диски

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Исследование принципов построения и работы средств выявления электронных устройств перехвата информации: детекторов поля, сканирующих приемников и нелинейных локаторов

Моделирование и исследование принципов построения и работы детекторов (индикаторов) поля. Моделирование и исследование принципов построения и работы сканирующих приемников. Моделирование и исследование принципов построения и работы нелинейных локаторов.

2. Документальное оформление результатов аттестационных испытаний объекта информатизации требованиям по безопасности информации

Решение практических задач по документальному оформлению результатов аттестационных испытаний

8. Оценочные материалы промежуточной аттестации

8 семестр, Экзамен

Контролируемые ИДК: ОПК-11.1 ОПК-11.2 ОПК-11.3

Вопросы/Задания:

1. Концепция безопасности и техническая защита информации

2. Теоретические основы технической защиты информации как конкретизация положений концепции безопасности, слабо формализуемые задачи (понятие)

3. Способ решения слабо формализуемых задач

4. Системный подход (понятие)

5. Свойства системы

6. Системное мышление (понятие)

7. Суть системного мышления применительно к технической защите информации

8. Системный анализ(понятие)

9. Содержание модели системы защиты информации

10. Общие принципы технической защиты информации

11. Профессиональные принципы технической защиты информации

12. Назовите каналы передачи речевой информации

13. Каналы утечки речевой информации

14. Воздушные, акустические каналы утечки речевой информации (понятие)

15. Вибрационные,виброакустические каналы утечки речевой информации (понятие)

16. Акустоэлектрические каналы утечки речевой информации (понятие)

17. Оптико-электронный (лазерный) канал утечки речевой информации (понятие)
18. Параметрические каналы утечки речевой информации (понятие)
19. Какие существуют характеристики речи?
20. Физические характеристики звуковых волн
21. Понятие структурного звука (акустовибрационные волны)
22. Чем характеризуется распространение структурных волн в инженерных конструкциях здания?
23. Понятия музыкального тона, созвучия, шума и взрыва (нарисовать графики)



24. Классификация методов оценки разборчивости речи
25. Понятие форманты
26. Понятие разборчивости речи
27. Что включает в себя понятие контроль выполнения норм защищенности речевой информации от акустической речевой разведки?
28. Как производится выбор опасных средств речевой разведки?
29. Чем характеризуется звукоизолирующая способность строительных конструкций?
30. Причины появления опасных сигналов в цепи электропитания

31. Типы и цели заземления
32. Пути попадания опасного сигнала в систему заземления
33. Основные термины и определения оценки эффективности защиты информации
34. Природа ПЭМИН (побочные электромагнитные излучения и наводки)
35. Классификация ПЭМИН, по способам возникновения

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие: учебное пособие / А. М. Голиков. - Защита информации от утечки по техническим каналам - Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/72090.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Основы защиты информации от утечки по техническим каналам: учебно-методическое пособие: учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.] - Основы защиты информации от утечки по техническим каналам - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019. - 267 с. - 978-5-9515-0426-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/101929.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
3. Киренберг А. Г. Защита информации от утечки по техническим каналам: учебное пособие: учебное пособие / А. Г. Киренберг, В. О. Коротин. - Защита информации от утечки по техническим каналам - Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. - 221 с. - 978-5-00137-407-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/135100.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Никифоров С. Н. Защита информации: учебное пособие / С. Н. Никифоров. - Защита информации - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015. - 384 с. - 978-5-9227-0585-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/74365.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Крахоткина Е. В. Архитектура ЭВМ: учебное пособие (лабораторный практикум): учебное пособие (лабораторный практикум) / Е. В. Крахоткина, В. И. Терехин. - Архитектура ЭВМ - Ставрополь: Северо-Кавказский федеральный университет, 2015. - 80 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/63074.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс

Ресурсы «Интернет»

1. <https://www.elibrary.ru/> - НЭБ eLIBRARY
2. <https://www.iprbookshop.ru/> - IPR BOOKS
3. <https://intuit.ru/> - Электронная образовательная среда "ИНТУИТ"
4. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
5. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

1. Microsoft Office;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Учебная аудитория

LED-экран - 1 шт.

Автоматизированное рабочее место (АРМ) - 1 шт.

Компьютерный класс

Автоматизированное рабочее место (АРМ) - 15 шт.

Доска настенная одноэлементная - 2 шт.

Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.