МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»,

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
Рабочая программа дисциплины

Составитель(и):
Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин
……..
Ответственный редактор
Кандидат технических наук, доцент, и.о. зав. кафедрой КЗИ Д.А. Митюшин
……

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 14.03.2024 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка студентов, необходимая для освоения методов и технологий обеспечения безопасности информации от её утечки по техническим каналам.

Задачи дисциплины:

– получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности информации от утечки по техническим каналам;

– изучение теоретических основ информационной безопасности на объектах информатизации;

– формирование умений использовать основные достижения в области защиты информации от утечки по техническим каналам при реализации своей профессиональной деятельности;

– владение практическими навыками защиты информации на объектах информатизации;

– развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей её достижения.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Уметь: • анализировать параметры электрической цепи и ее электронных компонентов
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Владеть: • навыками использования положений техники безопасности при разработке, настройке и эксплуатации электронных устройств
ОПК-9 *Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;*	*ОПК-9.1* *Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации*	*Знать:* • *основные понятия, принципы и модели технической защиты информации;* • *состав и порядок разработки нормативных документов по обеспечению безопасности объектов информатизации;* • *назначение и виды, подлежащих защите информационных ресурсов, моделей и процессов жизненного цикла системы защиты информации;* • *основные демаскирующие признаки объектов защиты.*

	ОПК-9.2 *Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации*	*Уметь:* • *применять физический подход при решении задач технической защиты информации;* • *разрабатывать нормативные документы по обеспечению безопасности объектов информатизации от утечки информации по техническим каналам;* • *организовать работу по обеспечению безопасности объектов информатизации от воздействия источников угроз и угроз.*
	ОПК-9.3 *Владеет методами и средствами криптографической и технической защиты информации*	*Владеть:* • *физической терминологией, физическими понятиями и теориями, используемыми при технической защите информации;* • *навыками использования стандартов и руководящих документов по защите объектов информатизации;* • *навыками по моделированию источников угроз и угроз безопасности объектов информатизации.*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства защиты информации от утечки по техническим каналам» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Физика», «Математические основы защиты информации», «Физические основы защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексная защита объектов информатизации. Организационное проектирование систем защиты информации», «Комплексная защита объектов информатизации. Управление службой защиты информации», «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _4_ з.е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
6	Лекции	**28**
6	Практические работы	**32**

Всего:	**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _84_ академических часа.

3. Содержание дисциплины

Раздел 1. Теоретические основы технической защиты информации

Тема 1. Введение в дисциплину. Системный подход к технической защите информации

Предмет, цели, задачи и содержание курса технической защиты информации (ТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Место дисциплины среди других курсов.

Термины и определения, основные нормативные и правовые документы по инженерно-технической защите информации.

Основные положения системного подхода к технической защите информации. Понятие системного подхода, основные методы при моделировании системы защиты информации, сущность системного подхода. Понятие системы защиты информации, её свойства, параметры, цели и задачи системы защиты информации,

Принципы технической защиты информации, основные понятия принципов, таких как: надёжность, непрерывность, скрытность, целеустремлённость, рациональность, активность, гибкость защиты информации, многообразие способов защиты, комплексное использование различных способов и средств защиты информации.

Тема 2. Объекты защиты, угрозы безопасности информации

Источники и носители конфиденциальной информации. Понятие об источниках, носителях и получателях информации. Классификация источников информации. Способы записи информации на различные виды носителей и принципы съёма информации.
Понятие об опасных сигналах и их источниках.

Источники угроз, угрозы информационной безопасности. Виды угроз безопасности информации. Преднамеренные, несанкционированные и случайные воздействия на источники информации, носители информации. Утечка информации и её особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

Тема 3. Побочные электромагнитные излучения и наводки

Методы и способы защиты информации от утечки за счёт побочных электромагнитных излучений и наводок. Классификация способов и средств защиты информации. Защита информации от утечки за счёт ПЭМИН. Мероприятия организационной защиты. Пассивные методы защиты от утечки за счёт ПЭМИН. Активные меры защиты информации от утечки за счёт ПЭМИН. Защита информации от утечки по цепям питания и заземления. Защита информации от утечки за счёт паразитной генерации и ВЧ воздействия. Защита каналов и линий связи.

Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки. Требования к средствам подавления сигналов побочных электромагнитных излучений и наводок. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных и электромагнитных полей.

Раздел 2 Методы и средства добывания (перехвата) защищаемой информации

Тема 4. Демаскирующие признаки объектов защиты

Видовые демаскирующие признаки. Сигнальные демаскирующие признаки. Демаскирующие признаки веществ. Состав и характеристики видовых, сигнальных признаков, признаков веществ.

Классификация демаскирующих признаков. Видовые демаскирующие признаки в оптическом диапазоне, ИК-диапазоне, радиодиапазоне. В радиодиапазоне по форме, физической природе сигнала, виду информативности, регулярности появления. Понятие спектр сигнала, прямое и обратное преобразование Фурье. Признаков веществ6 простые вещества, химические соединения, смеси веществ.

Понятие и параметры демаскирующего признака объекта защита, оценка величины информативности объекта защиты.

Тема 5. Технические каналы утечки информации

Технические каналы утечки информации. Классификация и структура технических каналов утечки информации. Характеристики каналов утечки информации. Структура и виды технических каналов утечки информации. Основные характеристики технических каналов утечки информации.

Акустические каналы утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Физические преобразователи. Излучатели электромагнитных колебаний. Паразитные связи и наводки. Комплексирование каналов утечки информации. Характеристика технических каналов утечки информации, обрабатываемой техническими средствами приёма, обработки, хранения и передачи информации. Характеристика технических каналов утечки информации при её передаче по каналам связи.

Тема 6. Технические средства разведки, методы и средства добывания информации

Органы добывания информации. Классификация технической разведки. Принципы ведения разведки. Технология добывания информации. Способы доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. Показатели эффективности разведки.

Способы несанкционированного доступа к источникам информации. Понятие о разведывательном контакте и его условиях. Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации без физического проникновения в контролируемую зону. Классификация и характеристики наземных средств дистанционного съёма информации с носителей. Возможности зарубежной космической, воздушной и морской разведки в мирное время.

Раздел 3. Методы и средства защиты информации от её утечки по техническим каналам

Тема 7. Основные положения по технической защите информации

Факторы обеспечения защиты информации от угроз утечки информации, перечень факторов, которые влияют на эффективность защиты информации от утечки влияют следующие факторы, такие как условия образования технического канала утечки информации, время и затраты на поиск носителя с защищаемой информацией, вероятность обнаружения и распознавания носителя информации, отношение сигнал/шум на входе приёмника.

Классификация методов технической защиты информации, предотвращение и нейтрализацию преднамеренных и случайных воздействий на источник информации и скрытие информации и её носителей от органа разведки (злоумышленника) на всех этапах добывания информации.

Состав, назначение основных методов технической защиты информации по скрытию информации (пространственное скрытие, структурное скрытие (маскировка, дезинформация), временное скрытие, энергетическое скрытие (уменьшение энергии сигнала, зашумление), маскировка признаков веществ), нейтрализации источника опасных сигналов.

Тема 8. Методы и средства защиты информации от её утечки по техническим каналам

Способы и средства защиты акустической (речевой) информации. Звукоизоляция акустического сигнала. Звукопоглощение акустической волны. Основные способы энергетического

срытия акустической (речевой) информации. Основные способы информационного скрытия речевых сообщений.

Способы средства защиты от наблюдения в видимом, ИК-диапазоне, в радиодиапазоне. Пассивные и активные методы и средства защиты видовых признаков сигнала.
Способы средства защиты от перехвата опасного сигнала за счёт ПЭМИН. Пассивные и активные методы и средства защиты от утечки информации по техническому каналу за счёт ПЭМИН.

Классификация средств обнаружения, локализации и подавления закладных устройств. Демаскирующие признаки закладных устройств. Типы и параметры сканирующих приёмников, автоматизированных комплексов радиоконтроля помещений. Технические средства обнаружители пустот, поиска наличия полупроводниковых элементов. Способы контроля телефонных линий и цепей электропитания. Способы подавления сигналов закладных устройств в телефонных и иных слаботочных линиях, цепях электропитания.

Раздел. 4 Создание системы защиты информации от утечки по техническим каналам на объектах информатизации

Тема 9. Основные требования и порядок построения системы защиты информации на объектах информатизации

Задачи и структура государственной системы технической защиты информации. Концепция технической защиты информации. Классификационная структура технической защиты информации.

Системный и комплексный подход к построению системы защите информации. Основные этапы и алгоритм проектирования системы. Основные этапы проектирования системы защиты информации.

Организация и порядок проведения работ по защите информации от утечки по техническим каналам на объектах информатизации. Лицензирование и сертификация в области защиты информации.

Тема 10. Методические рекомендации по построению системы защиты информации на объектах информатизации

Принципы моделирования объектов защиты, источников угроз, угроз безопасности информации. Модель поведения нарушителя. Основные факторы, влияющие на защиту информации от её утечки по техническим каналам.

Организационные и технические меры по обеспечению технической защиты информации. Способы и методы оценки состояния безопасности информации, методика расчёта расходов на техническую защиту информации и остаточного риска от реализации угроз на объекте информатизации.

4. Образовательные технологии

№ п/п	*Наименование раздела*	*Виды учебной работы*	*Образовательные технологии*
	Раздел 1. Теоретические основы технической защиты информации		
1	**Тема 1.** Введение в дисциплину, Системный подход к технической защите информации	*Лекция 1.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием электронной почты (ЭП).*
2	**Тема 2.** Объекты защиты, угрозы	*Лекция 2.*	*Традиционная с использованием видеоматериалов и презентаций.*

	безопасности информации	*Самостоятельная работа*	*Изучение материала по теме.* *Консультация с использованием ЭП.*
3	**Тема 3.** Побочные электромагнитные излучения и наводки	*Лекция 3.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
	Раздел 2. Методы и средства добывания (перехвата) защищаемой информации		
4	**Тема 4** Демаскирующие признаки объектов защиты	*Лекция 4.1.* *Лекция 4.2.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
5	**Тема 5.** Технические каналы утечки информации	*Лекция 5.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
6	**Тема 6.** ТСР, методы и средства добывания информации	*Лекция 6.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
	Раздел 3. Методы и средства защиты информации от её утечки по техническим каналам		
7	**Тема 7.** Основные положения по технической защите информации	*Лекция 7.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
8	**Тема 8.** Методы и средства защиты информации от её утечки по техническим каналам	*Лекция 8.1* *Лекция 8.2* *Лекция 8.3* *Лекция 8.4* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
	Раздел 4. Создание системы защиты информации от утечки по техническим каналам на объектах информатизации		
9	**Тема 9.** Основные требования и порядок построения системы защиты информа-	*Лекция 9.1.* *Лекция 9.2* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.*

	ции на объектах информатизации		*Консультация с использованием ЭП.*
10.	**Тема 10.** Методические рекомендации по построению системы защиты информации на объектах информатизации	*Лекция 10.1.* *Лекция 10.2.* *Самостоятельная работа*	*Традиционная с использованием видеоматериалов и презентаций.* *Изучение материала по теме.* *Консультация с использованием ЭП.*
	Раздел 5. Лабораторные работы		
12	Лабораторная работа 1	*Лабораторная работа 1*	*Выполнение и защита лабораторной работы.* *Консультация с использованием ЭП*
13	Лабораторная работа 2.	*Лабораторная работа 2.*	*Выполнение и защита лабораторной работы.* *Консультация с использованием ЭП*
14	Лабораторная работа 3.	*Лабораторная работа 3.*	*Выполнение и защита лабораторной работы.* *Консультация с использованием ЭП*
15	Лабораторная работа 4.	*Лабораторная работа 4.*	*Выполнение и защита лабораторной работы.* *Консультация с использованием ЭП*

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- опрос	*2 балла*	*12 баллов*
- лабораторная работа 1…4	*12 баллов*	*48 баллов*
Промежуточная аттестация – экзамен В традиционной форме по билетам		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Роль и значение технической защиты информации в системе обеспечении безопасности информации.	ОПК-9
2.	Определение опасного сигнала, источники и носители опасного сигнала.	ОПК-9
3.	Современная концепция защиты объектов информатизации, комплексный и системный подход к построению системы защиты информации.	ОПК-9
4.	Лицензирование деятельности и сертификация средств защиты информации.	ОПК-9
5.	Структура технического канала утечки информации, особенности утечки информации, утечки информации по техническим каналам.	ОПК-9
6.	Характеристики составных элементов технического канала утечки информации (носители информации, средства передачи, приёма сигналов, среда передачи сигнала).	ОПК-9
7.	Случайные антенны, понятия, технические характеристики, виды излучателей электромагнитных колебаний.	ОПК-9
8.	Преобразователи акустического сигнала в радиоэлектронный, физические основы, активные и пассивные преобразователи акустического сигнала	ОПК-9
9.	Физические основы возникновение паразитных связей и наводок в электрических цепях.	ОПК-9
10.	Виды технических разведок, преимущества технических разведок в сравнении с иными видами разведок по добыванию информации.	ОПК-9
11.	Эффективность ведения технической разведки, принципы ведения (активность, целеустремлённость скрытность, безопасность и т.п.), показатели технической разведки по добыванию защищаемой информации (достоверность, полнота, безопасность и материальные затраты).	ОПК-9
12.	Методы доступа («заходовый», «беззаходовый» на объект защиты) к	ОПК-9

	защищаемой информации, понятие и образование разведывательного контакта.	
13.	Цели и задачи специальной проверки технических средств, специального обследования предметов мебели и интерьера, технических средств.	ОПК-9
14.	Цели и задачи специального исследования технических средств, предназначенных для обработки защищаемой информации.	ОПК-9
15.	Классификация методов, способов, технических средств защиты информации от её утечки по техническим каналам.	ОПК-9
16.	Методы и средства пассивной (звукоизоляция и звукопоглощение) и активной (энергетического) защиты акустической (речевой) информации.	ОПК-9
17.	Методы и средства структурного скрытия информации (речевых сообщений).	ОПК-9
18.	Методы и средства противодействия наблюдению в оптическом диапазоне, ИК-диапазоне, радиодиапазоне.	ОПК-9
19.	Методы и средства защиты информации от утечки информации за счёт побочных электромагнитных излучений и наводок (ПЭМИН).	ОПК-9
20.	Методы и средства защиты информации от утечки информации по цепям питания и заземления.	ОПК-9
21.	Методы и средства защиты информации от утечки за счёт паразитной генерации и ВЧ воздействия (навязывания) на объект защиты.	ОПК-9
22.	Демаскирующие признаки закладных устройств, Методы и средства обнаружения (поиска) закладных подслушивающих устройств.	ОПК-9
23.	Цели, задачи и принципы построения системы защиты информации от её утечки по техническим каналам.	ОПК-9
24.	Основные правовые, организационные, технические мероприятия и требования нормативных документов по защите объектов информатизации.	ОПК-9
25.	Основные этапы и перечень работ при проектировании создании системы защиты информации от её утечки по техническим каналам.	ОПК-9
26.	Методы и принципы моделирования объекта защиты от реализации угроз безопасности информации.	ОПК-9
27.	Порядок проведения контроля и оценка эффективности организационных мероприятий и технических средств защиты от утечки информации по техническим каналам.	ОПК-9
28.	Цели, задачи и порядок проведения аттестации (аттестационных испытаний) объектов информатизации.	ОПК-9

Промежуточная аттестация (примерные вопросы к экзамену)

№	Вопрос	Реализуемая компетенция
1.	Основные положения концепции технической защиты информации. Системный подход при построении системы защиты информации. Цели и задачи системы защиты информации.	ОПК-9
2.	Понятие, свойства, ценность информации. Виды защищаемой информации, классификация информации в зависимости от порядка её предоставления и распространения.	ОПК-9
3.	Носители и источники информации. Запись и съем информация с одного носителя информации к другому.	ОПК-9

4.	Видовые демаскирующие признаки объектов. Видовые признаки электромагнитных волн в ИК – диапазоне, в радиодиапазоне.	ОПК-9
5.	Демаскирующие признаки сигналов. Классификация сигналов по форме, по физической природе, параметры сигналов.	ОПК-9
6.	Демаскирующие признаки веществ. Демаскирующие признаки деятельности.	ОПК-9
7.	Источники угроз, угрозы безопасности информации, определение, понятие. Особенности утечки информации.	ОПК-9
8.	Опасные сигналы, определение, понятие, виды опасных сигналов и их источники.	ОПК-9
9.	Преобразование акустических сигналов в акустоэлектрические сигналы. Физические явления, способствующие преобразованию акустического сигнала в электрический.	ОПК-9
10.	Паразитные связи и наводки в цепях радиоэлектронных средств и электрических приборов, виды паразитных связей и наводок.	ОПК-9
11.	Низкочастотные и высокочастотные излучения технических средств, источники побочных электромагнитных излучений и наводок.	ОПК-9
12.	Электромагнитные излучения сосредоточенных и распределённых источников, источники побочных электромагнитных излучений.	ОПК-9
13.	Утечка информации по цепям электропитания и заземления, причины появления опасных сигналов в цепях электропитания и заземления.	ОПК-9
14.	Особенности утечки информации по техническим каналам, типовая структура технических каналов утечки информации по видам носителей информации. Основные показатели технических каналов утечки информации, комплексное использование технических каналов утечки информации нарушителем.	ОПК-9
15.	Акустические и виброакустические каналы утечки информации, источники акустических сигналов, среда распространения сигнала, приёмники и их характеристики.	ОПК-9
16.	Оптические каналы утечки информации, источники излучения, среда передачи оптические приёмники и их характеристики.	ОПК-9
17.	Радиоэлектронные каналы утечки информации, источники сигналов, среда распространения сигналов, приёмники и их характеристики.	ОПК-9
18.	Вещественные каналы утечки информации, характеристика вещественного канала утечки информации.	ОПК-9
19.	Основные принципы разведки, Виды разведок и сфера их деятельности, разведка иностранных государств, коммерческая разведка. Технология, способы и методы добывания информации органами разведки. Показатели эффективности добывания информации.	ОПК-9
20.	Классификация технических средств добывания информации. Виды и возможности средств технической разведки по добыванию информации.	ОПК-9
21.	Закладные устройства. Назначение, классификация, состав и технические характеристики закладных устройств.	ОПК-9
22.	Акустические приёмники, виды, состав, технические показатели акустических приёмников.	ОПК-9
23.	Диктофоны, назначение, виды, технические характеристики диктофонов.	ОПК-9
24.	Средства высокочастотного навязывания, принцип работы, область применения и возможности средства высокочастотного навязывания. Технические средства защиты от высокочастотного навязывания.	ОПК-9

25.	Лазерные средства подслушивания, назначение, принцип работы, состав технических средств, технические характеристики лазерных устройств подслушивания. Средства защиты от лазерных средств подслушивания.	ОПК-9
26.	Средства наблюдения в оптическом диапазоне, оптические, визуально-оптические, фото и киноаппараты, виды, состав, технические характеристики средств наблюдения.	ОПК-9
27.	Средства наблюдения в инфракрасном диапазоне виды, состав, технические характеристики средств наблюдения.	ОПК-9
28.	Средства наблюдения в радиодиапазоне, виды, технические характеристики средств наблюдениям в радиодиапазоне.	ОПК-9
29.	Средства перехвата радиосигналов, задачи и цели, решаемые аппаратурой перехвата сигналов, состав и технические характеристики.	ОПК-9
30.	Средства перехвата оптических и электрических сигналов, возможности и способы подключения (снятия) информации с использованием оптических и оптоэлектронных средств наблюдения.	ОПК-9
31.	Факторы обеспечения защиты информации от угроз воздействия и от угроз утечки информации.	ОПК-9
32.	Классификация методов технической защиты информации на объекте информатизации. Структура системы технической защиты информации на объекте информатизации.	ОПК-9
33.	Подсистема технической защиты информации от её утечки по техническим каналам. Структура, цели и задачи системы безопасности объекта защиты от утечки информации по техническим каналам.	ОПК-9
34.	Подсистема защиты информации от утечки по вещественному каналу. Методы предотвращения утечки информации по вещественному каналу, требования и технические средства по уничтожению (утилизации) отходов производства.	ОПК-9
35.	Методы и средства противодействия наблюдению в оптическом диапазоне: пространственное, временное, структурное скрытие, типы оптических маскировочных масок, экранирование объектов наблюдения.	ОПК-9
36.	Методы и средства противодействия радиолокационному и гидроакустическому наблюдению: структурное, и энергетическое скрытие, принципы работ конструкции уголковых, линзовых, дипольных отражателей и переизлучающих антенных решёток.	ОПК-9
37.	Структурное скрытие речевой информации в каналах связи, шифрование, скремблирование, виды преобразования и режимы скрытия информации.	ОПК-9
38.	Энергетическое скрытие акустического сигнала, методы и способы звукоизоляции и звукопоглощения, Средства звукоизоляции и звукопоглощения акустического сигнала, виды поглощающих материалов, способы их применения.	ОПК-9
39.	Активные способы противодействия от подслушивания технических средств, глушения акустического сигнала.	ОПК-9
40.	Методы и средства пассивной защиты от предотвращения утечки опасного сигнала за счёт ПЭМИН. Методы и средства экранирования магнитного, электромагнитного поля, электрических проводов.	ОПК-9
41.	Методы и средства активной защиты от предотвращения утечки опасного сигнала за счёт ПЭМИН, шумовые заградительные помехи, радиотехническая маскировка сигнала.	ОПК-9
42.	Пассивные средства подавления опасных сигналов	ОПК-9

	акустоэлектрических преобразователей. Электрические фильтры, назначение, типы, технические характеристики.	
43.	Активные средства подавления опасных сигналов акустоэлектрических преобразователей. Генераторы шума, назначение, типы, технические характеристики.	ОПК-9
44.	Предотвращение утечки информации по цепям электропитания и заземления. Меры и средства по предотвращению утечки информации по цепям электропитания и заземления.	ОПК-9
45.	Демаскирующие признаки закладных устройств: (видовые, сигнальные, наличие полупроводниковых элементов).	ОПК-9
46.	Классификация средств обнаружения и локализации и подавления закладных устройств, радиоизлучающих, неизлучающих, радиоконтроля, подавления закладных устройств.	ОПК-9
47.	Назначение и основные характеристики средств обнаружения закладных устройств: индикаторы и детекторы, аппаратура нелинейной локации, обнаружители пустот, металлодетекторы, тепловизоры. сканирующие приёмники, аппаратура радиоконтроля, автоматизированные аппаратно-программные комплексы.	ОПК-9
48.	Принципы контроля линий связи и электрических цепей, виды, назначение и технические характеристики устройств контроля линий связи и электрических цепей.	ОПК-9
49.	Классификация технических средств подавления сигналов от закладных устройств. Способы и средства зашумления сигналов от закладных устройств, нарушения режима работы и уничтожение закладных устройств.	ОПК-9
50.	Способы и средства контроля помещений на отсутствие закладных устройств, виды «чистки», порядок проведения защитно-поисковых работ.	ОПК-9
51.	Назначение специсследования, спецпроверки технических средств, спецобследования, инструментального контроля помещений, когда и в каких случаях они проводятся.	ОПК-9
52.	Цели, задачи и принципы инженерно-технической защиты информации.	ОПК-9
53.	Методы и средства инженерно-технической защиты информации.	ОПК-9
54.	Моделирование объекта защиты от утечки информации по техническим каналам, несанкционированного доступа к информации, обрабатываемой на СВТ (АС).	ОПК-9
55.	Моделирование угроз безопасности информации, возможных методов и способов реализации угроз.	ОПК-9
56.	Порядок построения системы защиты информации на объектах информатизации в соответствии с требованиями нормативных документов.	ОПК-9
57.	Аттестационные испытания, аттестация объектов информатизации, назначение, задачи, основные требования к объекту информатизации.	ОПК-9
58.	Контроль эффективности защиты информации на объектах информатизации. Организационные, организационно-технические, технические методы контроля.	ОПК-9

Примерные тестовые задания – проверка сформированности компетенций – ОПК-9

1. Наличие радиоизлучения от пластиковой мусорной корзины на частоте 433 МГц говорит о:

а) браке при изготовлении корзины

б) наличии в корзине замаскированного радиозакладочного устройства

в) о том, что материал, использкемый при изготовлении корзины подвергся радиоактивному облучению

г) ни о чём не говорит

2. Как классифицируются закладные устройства по способу установки в помещении?

а) заходовые

б) беззаходовые

в) замаскированные

г) незамаскированные

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс] : Режим доступа : https:// http://www.consultant.ru/document/cons_doc_LAW_28399/ свободный. – Загл. с экрана.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=313796&fld=134&dst=1000000001,0&rnd=0.7796813329290967#010430102452128731 свободный. – Загл. с экрана.
3. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» (с изм. и доп., вступ. в силу с 31.12.2017) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220806&fld=134&dst=1000000001,0&rnd=0.6847213910250977#07452052248516211 свободный. – Загл. с экрана.
4. Указ Президента Российской Федерации от 10.01.2000 г. № 24 «О Концепции национальной безопасности Российской Федерации» [Электронный ресурс] : Режим доступа : http://www.kremlin.ru/acts/bank/14927 свободный. – Загл. с экрана.
5. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=208191&fld=134&dst=1000000001,0&rnd=0.9298403217707603#018712754822027167 свободный. – Загл. с экрана.
6. Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (утв. Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51). Режим доступа : http://www.rfcmd.ru/sphider/docs/InfoSec/Postan_pravit_N_912_ot_15_09_93.htm свободный. – Загл. с экрана.
7. Постановление Правительства РФ от 21.11.2011 № 957 (ред. от 10.11.2018) «Об организации лицензирования отдельных видов деятельности». Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_122062/ свободный. – Загл. с экрана..

Дополнительные

8. Положение о системе сертификации средств защиты информации, утверждённое приказом ФСТЭК России от 3 апреля 2018 г. № 55 Режим доступа : https://fstec.ru/component/attachments/download/1883 свободный. – Загл. с экрана.
9. Постановление Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». Режим доступа : https://fstec.ru/component/attachments/download/148 свободный. – Загл. с экрана.
10. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утв. Решением Коллегии Гостехкомиссии России № 7.2/02.03.2001 г. Режим доступа : http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm свободный. – Загл. с экрана.
11. Типовое положение о подразделении по защите информации от иностранных технических разведок и от её утечки по техническим каналам на предприятии (в учреждении, организации), одоб. решением Гостехкомиссии России от 14 марта 1995 года № 32. Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?base=EXP&dst=100259&n=376976&req=doc#0851 5518016040791. – Загл. с экрана.
12. Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте (одобрено решением от 03.10.95 г. № 42 Гостехкомиссии России). Режим доступа : http http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=381868&dst=100536#0827 0169448516825. (Приложение № 12) – Загл. с экрана.
13. ПУЭ-76 «Правила устройства электроустановок» (утв. Минэнерго СССР) (6-ое издание) Режим доступа : https://base.garant.ru/3923095/. – Загл. с экрана.
14. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Режим доступа : http://www.rfcmd.ru/sphider/docs/InfoSec/GOST_R_50922-96.htm. – Загл. с экрана.

Литература

Основная

1. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
2. *Титов, А. А.* Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.

Дополнительная

1. *Рагозин, Ю. Н.* Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.

6.2 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Информационный бюллетень Jet Info [Электронный ресурс]. – Электрон. дан. - [М., 2023]. - Режим доступа свобод.: http://www.jetinfo.ru/

2. Официальный сайт Российской государственной библиотеки [Электронный ресурс]. – Электрон. дан. - [М., 2023]. – Режим доступа свобод : http://www.rsl.ru/
3. Официальный сайт Российской национальной библиотеки [Электронный ресурс]. – Электрон. дан. - [М., 2023]. – Режим доступа свобод : http://www.nlr.ru/
4. Glossary Commander. Служба тематических толковых словарей [Электронный ресурс]. – Электрон. дан. - [М., 2023]. – Режим доступа свобод : http://glossary.ru/

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное

2) для оформления отчёта по лабораторным работам – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлены:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное

3) специализированный класс или лаборатория, оборудованный следующими техническими средствами:

– исследуемый акустопреобразовательный элемент;
– генератор сигналов типа Г3-111, ГЗ-33;
– шумомер типа AR-814, AR-844 (ШМ);
– акустический излучатель из комплекта либо экранированный датчик акустического поля;
– селективный нановольтметр типа Unipan-237;
– генератор низкочастотного сигнала типа SFG-2010, ГЗ-111, ГЗ-33 (ЗГ);
– активный акустический излучатель (громкоговоритель или звуковая колонка);
– шумомер типа AR-814, AR-844 (ШМ);
– комплект индикаторов поля типа ST-007, ST-032;
– макет закладного устройства;
– имитатор закладного устройства типа ST-121;
– сканирующие приёмники носимый и стационарный;
– активные имитаторы радиосигналов типа Шиповник 2 «Ш»
– комплекс радиомониторинга типа «Омега М5»
– нелинейный локатор (НЛ) типа «NR – μ».
– устройство предотвращения утечки информации «Терминатор 200».

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы лабораторных занятий

Лабораторные работы занятия проводятся в учебных группах (подгруппах) и имеют своей целью:
1) закрепление теоретических основ дисциплины, излагаемых в лекционном курсе, а также самостоятельно изучаемых студентами;
2) формирование практических навыков по использованию технических средств защиты информации;
3) научить студентов использовать техники экспериментальных исследований и анализа полученных результатов;
4) привитие навыков работы с лабораторным оборудованием, контрольно-измерительными приборами и вычислительной техникой.
К выполнению лабораторных работ допускаются обучаемые, уяснившие тему, цель, содержание работы, правила техники безопасности и эксплуатации ПЭВМ и знающие теоретический материал по теме лабораторной работы.
Для материально-технического обеспечения дисциплины «Техническая защита информации» необходимы:
При подготовке к лабораторной работе необходимо:
1. Изучить правила техники безопасности и правила технической эксплуатации ПЭВМ, инструкции по эксплуатации и правила безопасности при работе с соответствующим оборудованием.
2. Подготовить бланк отчёта по лабораторной работе, куда занести тему, цель работы, её содержание, состав и назначение применяемых для измерений приборов, а также таблицы наблюдений измеряемых величин.
3. Подготовиться к индивидуальному собеседованию по теме лабораторной работы.

Правила техники безопасности при работе на ПЭВМ.

Каждый обучаемый обязан знать и неукоснительно выполнять основные требования правил техники безопасности и расписаться за их изучение.
К самостоятельной работе в классе ПЭВМ допускаются лица, прошедшие инструктаж по технике безопасности.
Общие требования:
1. К работе на ПЭВМ, не связанной с их обслуживанием, допускаются лица, обученные безопасным методам работы с ПЭВМ, а также прошедшие проверку знаний и периодический инструктаж.
2. ПЭВМ должны удовлетворять следующим основным требованиям:
а) быстро включаться и отключаться от электросети (но не самопроизвольно);
б) быть безопасными в работе и иметь недоступные для случайного прикосновения токоведущие части;
в) подключаться к розетке, оборудованной дополнительной заземляющей жилой или иметь заземлённый корпус.
Перед началом работы на ПЭВМ необходимо проверить:
1. Состояние сетевого кабеля, целостность изоляции, отсутствие излома жил, надёжность крепления сетевой вилки.
2. Исправность заземления, защитных отключающих устройств.
При обнаружении каких-либо неисправностей работа на ПЭВМ должна быть немедленно прекращена и об этом доложено преподавателю или инженеру (технику) лаборатории.

Во время работы на ПЭВМ запрещается:

1. Начинать работу на ПЭВМ без прохождения инструктажа по мерам безопасности при работе с ПЭВМ.
2. Включать ПЭВМ без разрешения преподавателя.
3. Самостоятельно (без указания преподавателя) изменять что-либо в схеме или удалять какие-либо файлы в директории с установленной программой.
4. Без разрешения заведующего лабораторией, инженера или техника переносить с места на место системные блоки, мониторы, другие комплектующие ПЭВМ и периферийные устройства.
5. Снимать защитный кожух системного блока и монитора и производить самим какой-либо ремонт (как ПЭВМ, так и другого оборудования, разного рода кабелей и т.п.).
6. Держать сетевой кабель, касаться открытых токонесущих элементов, касаться одновременно корпуса ПЭВМ (металлических частей периферийных устройств) и заземляющего провода.
7. Подключать к работающей ПЭВМ и отключать от неё периферийные устройства, проверять надёжность подключённых кабелей.
8. Касаться сетевых терминаторов и коннекторов, вынимать их из разъёмов сетевых карт.
9. Разбирать силовые розетки, помещать в них посторонние предметы.

Лабораторная работа № 1 (12 ч.) Акустоэлектрические преобразовательные элементы, как источник технического канала утечки информации – проверка сформированности компетенций – УК-2, ОПК-9

Тема занятия: Определение эффективного значения коэффициента акустического преобразования элементов ВТСС и широкополосности акустопреобразовательных элементов.

1.1. Учебные вопросы

Учебные вопросы:

1. Измерение эффективного значения коэффициента акустического преобразования ВТСС.
2. Построение графика частотной зависимости коэффициента акустического преобразования исследуемого ВТСС (вспомогательные технические средства и системы).
3. Расчёт допустимого давления акустического поля в местах установки ВТСС, обладающих микрофонным эффектом.
4. Определение возможных способов защиты акустопреобразовательных технических каналов утечки информации (ТКУИ) от утечки речевой конфиденциальной информации.

1.2. Порядок выполнения работы

1. По заданию преподавателя собрать схему измерения.
2. К выходу генератора тест-сигнала подключить акустический источник.
Излучатель акустического поля представляет собой динамический громкоговоритель, который с целью снижения величины магнитного поля рассеяния помещается в двойной экран, выполненный из металла, обладающего высокой относительной магнитной проницаемостью.
3. В целях определения направления максимального воздействия акустического тест-сигнала на исследуемое преобразующее устройство перед измерениями необходимо произвести взаимную ориентацию АПЭ и измеряемого устройства. Для этого при фиксированном уровне звукового давления (контролируется по шкале шумомера) необходимо добиться за счёт изменения положения АПЭ максимального показания СНВ.
4. Используя шумовой тест-сигнал, произвести проверку АПЭ, подключив их к селективному нановольтметру. Замерить напряжение помех ($U_п$). АПЭ располагается на расстоянии от исследуемого устройства, гарантирующего наличие преобразованного электрического сигнала. (50 и 100 см)
5. Включить генератор низкочастотного сигнала, частота f = 250 Гц, установить ***уровень звукового давления D (в децибелах) в пределах 60-70*** **дБ.** Величина излучаемой мощности определяется с помощью ШМ или задаётся.

6. Снять показания шумомера в линейном режиме и по полученному значению уровня акустического давления L_p (дБ) определить шумовое давление Р, руководствуясь соотношением (13)[1] и таблицей 1.1 с указаниями к ней. Занести найденное значение Р в таблицу 1.1 (Приложение 1).
7. Замерить величины преобразованного электрического сигнала по СНВ (или по экрану осциллографа).
8. Изменяя плавно частоту генератора низких частот от 250 до 4000 Гц найти максимальное значение $U_{с+п}$ и занести значение в таблицу 1.1. (Приложение 1.1).
9. Провести повторные измерения по п.п. 5-8 на частотах 500, 1000 2000, 4000 Гц. Результаты записать в табл. 2.2, 2.3, 2.4, 2.5 (Приложение 1.1.).
10. Рассчитать по формуле (19) значение напряжения сигнала $U_{вых}$ для каждого исследуемого ВТСС и внести его в таблицу 1.1- 1.5 (Приложение 1.1.)
11. Определить полосу преобразованных частот и коэффициент преобразования по формуле 18. В заключении отметить степень опасности преобразования речевых сигналов.
Расчёт допустимой величины давления акустического поля в месте расположения ВТСС проводится в соответствии с формулой 13 или табл. 1.1.

Примечание:
Специальные электроакустические измерения в условиях эксплуатации желательно проводить при максимально низком уровне посторонних акустических шумов, выбирая для этого наиболее подходящее время суток.

1.3. Оформление отчёта

Отчёт по лабораторной работе выполняется в отдельной тетради или в лабораторном журнале (на отдельных листах) в рукописном или печатном вариантах согласно приложения 1.1. и включает следующие разделы:

- наименование лабораторной работы и учебные вопросы;
- описание и схема лабораторной установки;
- таблицы с измеряемыми параметрами;
- расчёты;
- график зависимости $U_{вых}$ от f (Гц) для каждого исследуемого АПЭ;
- разработанные предложения;
- выводы по работе.

Форма отчёта лабораторной работы представлена в приложении 1.1. Лабораторный практикум по учебной дисциплине «Техническая защита информации»

1.4. Защита полученных результатов

Оформленный отчёт по лабораторной работе представляется преподавателю.
Студент должен быть готовым к ответу на вопросы преподавателя по теоретическим материалам данной лабораторной работы, по порядку выполнения и оформления лабораторной работы.

Контрольные вопросы

1. Какие типы акустопреобразовательных элементов Вы знаете?
2. Что такое "коэффициент акустоэлектрического преобразования"?
3. Какие физические эффекты приводят к появлению прямого АПЭ?

Список литературы

1. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.

[1] Формулы, абюлицы и приложения указаны из лабораторного практикума.

2. *Титов, А. А.* Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
3. *Рагозин, Ю. Н.* Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
4. Материалы лекций по дисциплине.
5. Описание технических средств, используемых в лабораторной работе.

Материально-техническое обеспечение занятия:

- исследуемый акустопреобразовательный элемент (АПЭ);
- генератор сигналов типа Г3 –111, ГЗ-33 (ГЗ);
- шумомер типа AR-814, AR-844 (ШМ);
- акустический излучатель из комплекта либо экранированный датчик акустического поля (АИ);
- селективный нановольтметр Unipan - 237;
- бокс для акустических измерений.

Лабораторная работа № 2 (12 ч.) Методы защиты речевой конфиденциальной информации от утечки по воздушному акустическому каналу– проверка сформированности компетенций – УК-2, ОПК-9

Тема занятия: Использование пассивных методов защиты от утечки речевой информации из защищаемого помещения.

2.1. Учебные вопросы

Учебные вопросы:

1. Исследование условий образования акустических каналов утечки речевой информации за пределы защищаемого помещения.
2. Критерии защищённости ЗП от утечки речевой информации по воздушному акустическому каналу.
3. Методы и способы защиты речевой информации от утечки по акустическому каналу.

2.2. Описание лабораторного комплекса

1. В состав лабораторного комплекса входят:

- генератор низкочастотного сигнала типа ГЗ-111, ГЗ-33 (**ЗГ**);
- акустический излучатель (с усилителем мощности - **УМ**);
- шумомер типа AR-814. AR-844 (**ШМ**).

2.3. Методика выполнения лабораторной работы

2.3.1. Подготовительные работы

Перед выполнением лабораторной работы каждый студент ***ОБЯЗАН*** ознакомиться с правилами поведения в лаборатории и мерами безопасности при выполнении заданий лабораторного практикума под роспись в журнале ознакомления с мерами безопасности. При невыполнении этого требования, студент к выполнению лабораторной работы ***не допускается***, о чем преподавателем делается отметка в журнале посещаемости.

Примечание:

До начала измерений необходимо выполнить следующее:

а) провести внешний осмотр и анализ защищаемого помещения, обращая внимание на конструктивные особенности ограждающих конструкций и дверных проёмов, наличие вентиляционных отверстий и других конструктивных элементов, влияющих на звукоизоляцию помещений;
б) составить план защищаемого помещения с указанием возможных мест утечки речевой информации по акустическому каналу и вычертить его в отчёте по лабораторной работе;
в) определить, совместно с преподавателем, местоположение контрольных точек для последующих измерений;
г) ответить на контрольные вопросы по знанию инструкции по работе с приборами и, после разрешения преподавателя, продолжить выполнение лабораторной работы.

2.3.2. Порядок проведения инструментальных измерений

Инструментальные измерения проводятся в следующей последовательности:
1) собрать лабораторную установку под руководством преподавателя;
2) включить электропитание;
3) установить на шумомере режим измерения «Длительно» (1 с) и в точке, указанной преподавателем, замерить значение внешнего шумового сигнала ($L_{шум}$);
4) полученное значение $L_{шум}$ занести в таблицу 2.1. 2.2. 2.3. 2.4., приложения 2.1 отчёта по лабораторной работе;
5) включить электропитание генератора низкочастотного сигнала, а также активных акустических излучателей, установленных в комнате.
Выбор местоположения контрольных точек при акустических измерениях.
В зависимости от особенностей ограждающих конструкций и их состояния контрольные точки должны располагаться следующим образом.
За сплошной однородной конструкцией (например, за стеной, окном, дверью) контрольные точки располагаются в соответствии с рис. 2.3. Измерение в каждой точке выполняется в соответствии с рис. 2.4. или по указания преподавателя;

- за сплошной неоднородной конструкцией, например, за стеной, отдельные участки которой имеют различную толщину или выполнены из различных материалов, контрольные точки располагаются в соответствии с рис. 2.3 для каждого характерного участка;
- в случае наличия явных нарушений целостности ограждающих конструкций (отверстий, щелей) дополнительная контрольная точка располагается напротив места каждого нарушения на расстоянии 1-1.5 м.;
- в случае наличия вентиляционного канала, подводимого к проверяемому помещению, контрольная точка располагается в центральной области сечения воздушного канала

6) первое измерение ($L_{с1}$) на частотах 250, 500, 1000, 2000, 4000 Гц произвести в комнате на расстоянии 0,5-1м от акустического излучателя. Перед измерением в контрольной точке 1 регулятором выходного уровня сигнала генератора установить величину акустического давления по данным таблицы 2.5 (нормальный разговор), контролируя его значение по шкале шумомера. Результаты измерения записать в таблицу 2.1. приложения 2.1. отчёта по лабораторной работе;
7) измерения ($L_{2(сигн.+шум)}$) произвести в помещении при закрытой двери в соответствии со схемой приведённой, на рис. 2.3. Результаты измерения записать в таблицу 2.1 приложения 2.1. отчёта по лабораторной работе;

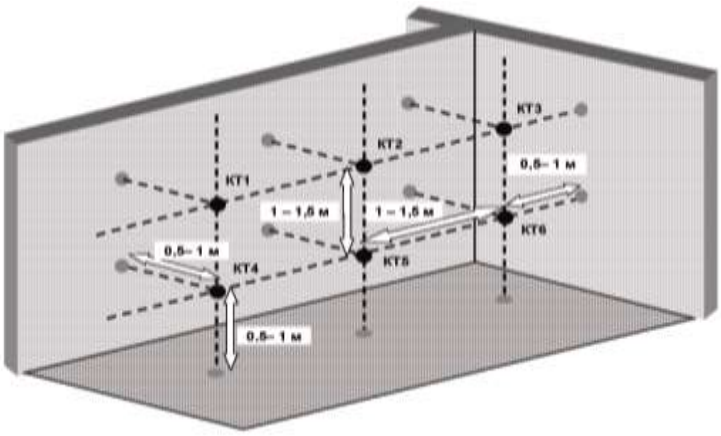


Рис. 2.3. Схема расположения контрольных точек за однородным ограждением.

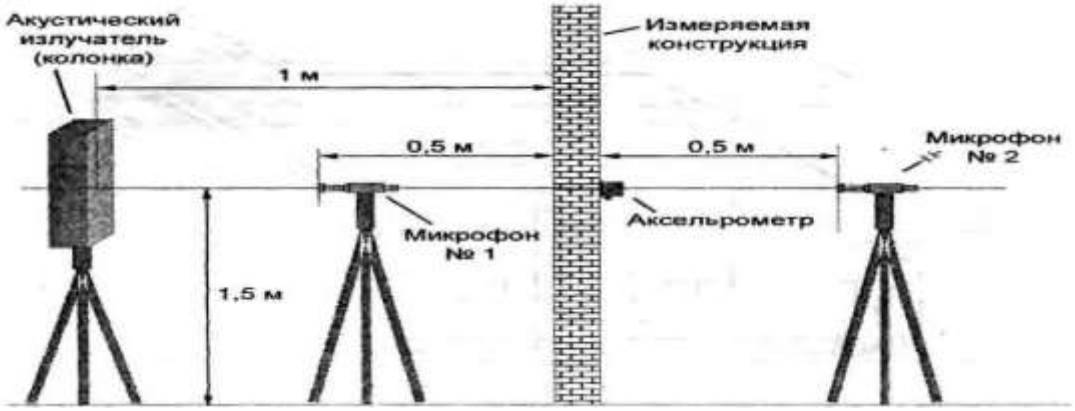


Рис. 2.4. Схема расположения приборов для измерения в контрольных точках за однородным ограждением

8) закрыть двери в помещения и произвести аналогичные трёхкратные измерения давления акустического поля ($L2_{сигн.+шум}$) для каждой из контрольных точек (К.т.2 – К.т.6), указанных на рис 2.3, на каждой среднегеометрической частоте октавных полос (250; 500; 1000; 2000 и 4000 Гц). Каждое измерение проводится после стабилизации показателя на шкале шумомера (3-5 сек) результаты измерений записать в таблицу 2.1. 2.2. 2.3. 2.4. приложения 2.1. отчета по лабораторной работе

9) повторить измерения для контрольных точек согласно рис. 2.3. или по указанию преподавателя, с п.п. 4 – 8, результаты измерений для каждой контрольной точки записать в соответствующие таблицы 2.2. 2.3. 2.4. приложения 2.1 к отчёту лабораторной работе;

10) закончив измерения, сообщить об этом преподавателю и отключить генератор и шумомер.

2.3.3. Порядок выполнения расчётов

Сущность проводимых расчётов заключается в определении величины звукоизоляции несущих конструкций выделенного помещения.

а) для измеренных величин $L_{с2+шум}$ уточняется значение акустического давления измеренного звукового сигнала $L_{сигн.}$, исходя из следующих условий:

если $L_{2(сигн.+шум)} - L_{шум} \geq 10$дБ, то $L_{сигн.2} = L_{2(сигн.+шум)}$, (1);

если $L_{2(сигн.+шум)} - L_{шум} < 10$дБ, то $L_{сигн.} = L_{2(сигн.+шум)} - \Delta$ (2);

величина Δ определяется из таблицы 1.3;

б) полученное в результате уточнения значение $L_{сигн2}$ записать в таблицы 2.1, 2.2, 2.3, 2.4. приложения 2.1. отчёта по лабораторной работе;

в) рассчитать параметр акустической защищённости помещения для каждой октавной полосы (250, 500, 1000, 2000, 4000 Гц), используя соотношение:

$Q_{расчi} = L_{сигн.i} - L_{сигн.2}$, (19)

где: $L_{сигн.i}$ – акустическое давление внутри защищаемого помещения;

$L_{сигн.2}$ - акустическое давление вне помещения.

Полученные в результате расчётов значения величины $Q_{измі.}$ записать в таблицы 2.1. 2.2. 2.3. 2.4. приложения 2.1. (отчёта по лабораторной работе);

г) определить разность между рассчитанным ($Q_{расчі}$) и нормативным ($Q_{нормі}$) значениями акустической защищённости помещения. Результаты записать в таблицы приложения 2.1 (отчёта по лабораторной работе);

Примечание: Величину $Q_{нормі}$ выбрать из таблицы 2.4 (раздел 2.2.3.) для условий проведения лабораторной работы.

д) по величине акустической защищённости помещения сделать выводы о степени соответствия данного параметра требованиям, определяемым следующими выражениями:

если $Q_{расчі} - Q_{нормі} \geq 0$,- соответствует; (3)

если $Q_{расчі} - Q_{нормі} < 0$, - не соответствует. (4)

В случае несоответствия параметра установленным требованиям необходимо разработать меры по улучшению акустической защищённости помещения;

е) выводы письменно отобразить в графе «Соответствие» таблиц 2 приложения 2.1. (отчёта по лабораторной работе);

ж) провести расчёт средней арифметической величины давления акустического поля для всех контрольных точек на каждой из октавных полос в соответствии со следующим выражением:

$L_{ср} = \sum F_i / n$, при i = {1..n}. (5)

полученные результаты записать в таблицы 2 приложения 2.1. (отчёта по лабораторной работе);

2.3.4. Разработка предложений по улучшению акустической защищённости помещения

а) разработку предложений по улучшению акустической защищённости помещения провести с использованием следующих способов:

первый – улучшение звукоизоляционных свойств несущих конструкций (таблица 2.7 и 2.8) с использованием «плиты на относе» и звукопоглощающих материалов;

второй – улучшение звукоизоляционных свойств дверей (таблица 2.8);

Таблица 2.7 Звукоизоляция ограждения, дБ

Материал конструкции	Толщина, мм	Поверхностная плотность	**9.1.1.1.1.1 Среднегеометрическая частота октавной полосы**							
			63	125	250	500	1000	2000	4000	8000
Кирпичная кладка, штукатуренная с двух сторон	½ кирпича 1 кирпич 1,5 кирпича 2 кирпича 2,5 кирпича	220 420 620 820 1000	32 36 41 45 45	39 41 44 45 47	40 44 48 52 55	42 51 55 59 60	48 58 61 65 67	54 64 65 70 70	60 65 65 70 70	60 65 65 70 70
Железобетонные плиты	40 50 100 160 200 300 400 800	100 125 250 400 500 750 1000 2000	- 28 34 - 40 44 45 47,5	32 34 40 43 42 44,5 47,5 55	36 35 40 47 44 50 55 61	35 35 44 51 51 58 61 67,5	38 41 50 60 59 65 67,5 70	47 48 55 63 65 69 70 70	53 55 60 - 65 69 70 70	- 55 60 - 65 69 70 70
Гипсобетонные плиты	95	135	-	32	37	37	42	48	53	-
Шлакоблоки, штукатуренные с двух сторон	220	360	-	42	42	48	54	60	63	-

Материал конструкции	Толщина,	Поверхностная	**9.1.1.1.1.1 Среднегеометрическая частота октавной полосы**							
Древесно-стружечная плита	20	12	23	26	26	26	26	26	26	33
Две железобетонные плиты на общем фундаменте	40-40-40	180	-	36	43	42	46	55	57	-
Две гипсобетонные плиты на общем основании	95-100-95	270	-	41	43	42	48	56	62	-

Таблица 2.8 Звукоизоляции дверей различных конструкций

№ п.п	Конструкция	Примечание	Значение Q_f (дБ) для частоты f (Гц)				
			250	500	1000	2000	4000
1	Стандартное дверное полотно толщиной 40мм (обыкновенная дверь)	Без уплотняющих прокладок	14	16	22	22	20
2		С уплотняющими прокладками из пористой резины	25	25	26	26	23
3	Стандартное дверное полотно толщиной 40 мм с обивкой дерматином по минеральному войлоку	Уплотняющий валик на дверной коробке	26	29	32	35	36
4	Глухая щитовая дверь толщиной 40 мм, облицованная с двух сторон фанерой толщиной 4 мм	Без уплотняющих прокладок	23	24	24	24	23
5		С уплотняющими прокладками	27	32	35	34	35
6	Щитовая дверь из древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой	Без уплотняющих прокладок	26	30	31	28	29
7		С уплотняющими прокладками	30	33	36	32	30
8	Дверное полотно толщиной 84 мм из двух наружных листов фанеры и одного асбоцементного листа по 6 мм каждый с двумя промежуточными слоями стекловолокна толщиной 16 и 50 мм	Два ряда прокладок из пористой резины	25	31	37	39	35

№	Конструкция	Примечание	Значение Q_f (дБ) для частоты f (Гц)				
9	Двойная дверь предыдущей конструкции с тамбуром шириной 300 мм	Два ряда прокладок из пористой резины	29	36	46	49	42
10	Дверь звукоизолирующая облегчённая	Прокладки из пористой резины	30	39	42	45	42
11	Двойная дверь звукоизолирующая облегчённая с тамбуром шириной 200 мм	Прокладки из пористой резины	42	55	58	60	60
12	Дверь звукоизолирующая тяжёлая двойная с тамбуром шириной 300 мм	Прокладки из пористой резины	46	60	65	65	65
13	Дверь звукоизолирующая тяжёлая. Прокладки из пористой резины	Одинарная	36	45	51	50	49
14		Двойная с тамбуром шириной 300 мм	46	60	65	65	65
15		Двойная с облицованным тамбуром шириной 300 мм.	58	65	70	70	70

б) сделать вывод о достаточности звукоизоляции несущих конструкций и двери для обеспечения требуемой акустической защищённости. Вывод оформить в отчёте по лабораторной работе.
в) при недостаточности акустической защищённости помещения разработать предложения по ее повышению.

При использовании звукопоглощающих материалов значение ослабления звука ограждениями, выполненными из различных материалов, может быть определено из соотношения:

$$R_{ог} = R_c + 6 + 10 \lg S_{ог} - К_{ог} \text{ (Дб)}, \quad (6)$$

где: $R_{ог}$ - уровень речевого сигнала за преградой, Дб;
R_c - уровень речевого сигнала в помещении, Дб;
$S_{ог}$ - площадь ограждения, $м^2$;
$К_{ог}$ - коэффициент поглощения материала ограждения, Дб (таблица 2.9.).

Таблица 2.9. Коэффициент поглощения материала ограждения

Тип ограждения	Коэффициент поглощения ($K_{ог}$) на частотах (Гц)					
	125	250	500	1000	2000	4000
Деревянная обивка	0,1	0,11	0,11	0,08	0,082	0,11
Войлок (25мм)	0,18	0,36	0,71	0,8	0,82	0,85
Ковёр с ворсом	0,09	0,08	0,21	0,27	0,27	0,37
Стеклянная вата (9мм)	0,32	0,4	0,51	0,6	0,65	0,8

2.4. Оформление отчёта

Отчёт по лабораторной работе выполняется в отдельной тетради или в лабораторном журнале (на отдельных листах) в рукописном или печатном вариантах и включает следующие разделы:

- наименование лабораторной работы и учебные вопросы;
- описание и схема лабораторной установки;
- таблицы с измеряемыми параметрами;
- расчёты;
- разработанные предложения;
- выводы по работе.

Форма отчёта лабораторной работы №2 представлена в приложении 2.1. Лабораторный практикум по учебной дисциплине «Техническая защита информации»

2.5. Защита полученных результатов

Оформленный отчёт по лабораторной работе представляется преподавателю.
Студент должен быть готовым к ответу на вопросы преподавателя по теоретическим материалам данной лабораторной работы, по порядку выполнения и оформления лабораторной работы.

Контрольные вопросы

1. Характеристика акустического воздушного канала утечки информации.
2. Критерии защищённости ЗП от утечки конфиденциальной речевой информации.
3. Пассивные методы защиты ЗП от утечки конфиденциальной речевой информации.
4. Использование звукоизолирующих материалов. Особенности защиты.
5. Применение гибкой плиты на «относе». Общая характеристика метода.
6. Октавные полосы речевого сигнала и их характеристика.

Литература:

1. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
2. *Титов, А. А.* Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
3. *Рагозин, Ю. Н.* Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
4. Материалы лекций по дисциплине.
5. Описание технических средств, используемых в лабораторной работе.

Материально-техническое обеспечение занятия:

1. генератор низкочастотного сигнала типа SFG-2010, ГЗ-111, ГЗ-33 (ЗГ);
2. активный акустический излучатель (громкоговоритель или звуковая колонка);
3. шумомер типа AR-814, AR-844 (ШМ);

Лабораторная работа № 3 (12 ч.) Организация радиомониторинга объекта защиты с помощью индикаторов поля – проверка сформированности компетенций – УК-2, ОПК-9

Тема занятия*: *Радиомониторинг объекта защиты - деятельность по изучению и контролю радиоэлектронной обстановки, поиску и обнаружению источников несанкционированного перехвата информации (НСИ) в районе объекта специальной проверки.

3.1. Учебные вопросы:

Учебные вопросы:

1. Определение демаскирующих признаков радиозакладочных устройств;
2. Изучение основных характеристик радиозакладочныхых устройств;

3. Изучение основных характеристик индикаторов поля (радиоприёмных устройств), используемых для радиомониторинга объекта защиты.
4. Организация спецпроверки защищаемого помещения с помощью индикаторов поля.

3.2. Порядок проведения лабораторной работы:

1. Изучить основные характеристики используемых индикаторов поля и их возможности при проведении спецобследования (радиомониторинга) объекта защиты.
2. Определить зону обнаружения радиозакладного устройства индикатором поля, используемым при проведении работ.
3. По заданию преподавателя произвести поиск закладного устройства в реальных условиях.
4. Провести проверку индикатора поля в сторожевом режиме.

3.2.1. Порядок проведения измерений.

1. Изучить схему, устройства управления, индикаторную панель и инструкцию по эксплуатации прибора ST-007, ST-032 (ИП).
2. Изучить инструкцию по эксплуатации комплекса радиомониторинга «Омега М5»
3. Изучить схему, устройства управления, индикаторную панель и инструкцию по эксплуатации НЛ «NR – μ»).
4. Подготовить приборы к эксплуатации согласно техническому описанию или в соответствии указаниям преподавателя.

3.2.2. Определения зоны обнаружения радиозакладки.

Для выполнения этой части работы необходимо определить расстояния, на которых происходит обнаружение радиозакладки при подходе к ней с настроенным индикатором с разных сторон - слева, справа, сверху, снизу.
Для выполнения этой части работы руководитель устанавливает телефонную радиозакладку и активизирует ее.
Студент осуществляет определение зоны обнаружения в соответствии с разделом «эксплуатация».

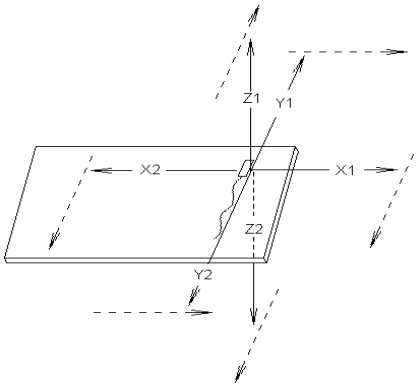


Рис. 1. Зона обнаружения стандартной радиозакладки (горизонтальная поляризация)

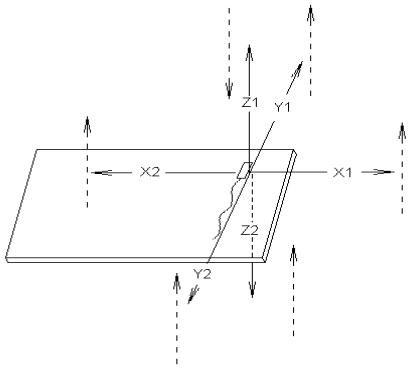
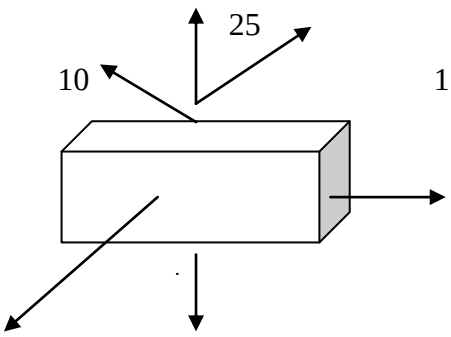


Рис. 2. Диаграмма направленности излучения ЗУ (вертикальная поляризация)

ИПШ – 12

- с выдвинутой антенной



- с задвинутой антенной

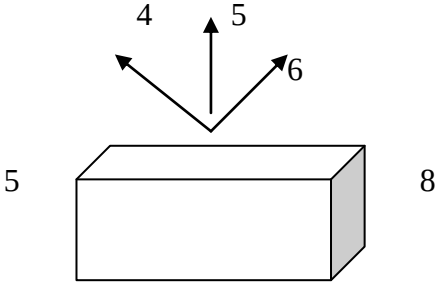


Рис. 3. Измерение зоны обнаружения телефонной радиозакладки.

3.2.3. Поиск радиозакладок.

Преподаватель устанавливает *радиозакладку* в защищаемом помещении. Студент входит в помещение и в соответствии с разделом «эксплуатация» осуществляет настройку индикатора и проводит поиск радиозакладки.

При проведении поиска радиозакладных устройств на объекте проверяющий обходит все возможные места установки последних, проводя антенной прибора на минимально возможном расстоянии от поверхности мебели и других устройств, расположенных в этом помещении.

Для более уверенного нахождения радиозакладок при поиске на исследуемой поверхности следует изменять ориентацию антенны вертикальную и горизонтальную плоскость.

Увеличение количества одновременно горящих светодиодов индикатора и повышение тона звукового сигнала свидетельствуют о возможном наличии закладки.

- для идентификации радиозакладки включить систему АОС, для чего установить переключатель в положение “Выкл” переключатель в положение «Демод». Сориентировать индикатор динамиком в сторону размещения источника радиоизлучений. Если в этом месте расположена радиозакладка будет слышен характерный свист акустической «завязки»;
- для увеличения точности место определения радиозакладки можно уменьшать чувствительность ИП поворотом регулятора против часовой стрелки. Если сигнал достаточно сильный и при максимальном загрублении чувствительности ИП (регулятор повернут против часовой стрелки до упора) на индикаторе все светодиоды горят, загрубите чувствительность путём включения аттенюатора поставьте переключатель в положение «Атт».

Студент перед началом работы составляет схему исследуемого помещения. Поиск проводится по схеме по или против часовой стрелки (это позволит избежать пропуск в поиске). В процессе поиска радиозакладки учитываются возможные переизлучения сигнала радиозакладки расположенными в помещении устройствами и на схеме помещения отмечаются все места, где имеется превышение электромагнитного поля над фоном (отмечается количество засвеченных секторов индикатора).

Результаты измерений заносятся в таблицу и отмечаются на плане помещения.

3.2.4. Определение начала работы радиозакладки в сторожевом режиме.

Студент производит настройку индикатора поля на нулевой уровень – на *усреднённый уровень электромагнитного поля в помещении.*

С учётом определённой ранее зоны обнаружения индикатора поля устанавливается и включается имитатор РЗУ. Определяется факт включения радиозакладки.

3.3. Обработка и представление результатов.

По разделу “Определение зоны обнаружения радиозакладки”:

- рассчитать и построить зоны обнаружения радиозакладки индикатором поля;
- построить диаграмму зоны обнаружения телефонной радиозакладки.

По разделу “Поиск радиозакладки в защищаемом помещении”:

- представить план защищаемого помещения с нанесёнными результатами полученных измерений.

3.4 Оформление отчёта

Отчёт по выполненной лабораторной работе выполняется в отдельной тетради или в лабораторном журнале (на отдельных листах) в рукописном или печатном вариантах и включает следующие разделы:

- наименование лабораторной работы и ее учебные вопросы;
- описание и схема лабораторной установки;
- зоны обнаружения радиозакладки индикатором поля;
- диаграмма зоны обнаружения телефонной радиозакладки;
- план защищаемого помещения с нанесёнными результатами полученных измерений.
- предложения по поиску закладных устройств;
- выводы.

Форма отчёта по лабораторной работе № 3 представлена в приложении 3.1. Лабораторный практикум по учебной дисциплине «Техническая защита информации»

3.5. Защита полученных результатов

Оформленный отчёт по лабораторной работе представляется преподавателю.
Студент должен быть готовым к ответу на вопросы преподавателя по теоретическим материалам данной лабораторной работы, по порядку выполнения и оформления лабораторной работы.

Контрольные вопросы:

1. Основные характеристики индикаторов поля.
2. Что такое «дифференциальный индикатор поля».
3. Чем определяется необходимый диапазон работы индикатора поля.
4. Чувствительность индикатора поля.
5. Поисковые индикаторы поля.
6. Сторожевые индикаторы поля.
7. Комбинированные индикаторы поля.

Литература:

1. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
2. *Титов, А. А.* Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
3. *Рагозин, Ю. Н.* Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
4. Материалы лекций по дисциплине.
5. Описание технических средств, используемых в лабораторной работе.

Материально-техническое обеспечение занятия:

– комплект индикаторов поля типа ST-007, ST-032;
– сканирующие приёмники;
– активные имитаторы радиосигналов типа Шиповник 2 «Ш»
– комплекс радиомониторинга типа «Омега М5»
– нелинейный локатор (НЛ) типа «NR – μ».

Лабораторная работа № 4 (12 ч.) Использование устройств, преднамеренного воздействия на информацию в защите информации– проверка сформированности компетенций – УК-2, ОПК-9

Тема занятия: Определение возможной зоны блокирования сотовых телефонов в зависимости от используемых типов блокираторов.

4.1. Учебные вопросы:

Учебные вопросы:

1. Определение эффективности аппаратуры преднамеренного воздействия (**ПДВ**) на решение вопроса защиты информации от ее утечки из систем сотовой связи и записанной на различные носители конфиденциальной информации. Определить условия проявления акустоэлектрического преобразования на представленном устройстве.
2. Определить зону блокирования сотового телефона в зависимости от вида используемого блокиратора.

4.2. Порядок выполнения лабораторной работы

1) получить блокиратор;
2) изучить инструкцию по эксплуатации «Терминатор 200»;
3) по заданию преподавателя определить место расположения блокиратора «Терминатор 200»;
- включив сотовые телефоны определить зону их подавления.

4.3 Оформление отчёта

Отчёт по выполненной лабораторной работе выполняется в отдельной тетради или в лабораторном журнале (на отдельных листах) в рукописном или печатном вариантах и включает следующие разделы:

- наименование лабораторной работы и ее учебные вопросы;
- описание и схема лабораторной установки;
- таблицы с измеряемыми параметрами
- разработанные предложения;
- выводы.

Форма отчёта лабораторной работы № 4 представлена в приложении 4.1. Лабораторный практикум по учебной дисциплине «Техническая защита информации»

4.4. Защита полученных результатов

Оформленный отчёт по лабораторной работе представляется преподавателю.
Студент должен быть готовым к ответу на вопросы преподавателя по теоретическим материалам данной лабораторной работы, по порядку выполнения и оформления лабораторной работы.

Контрольные вопросы:

1. Дайте определение несанкционированному воздействию на информацию.
2. Дайте определение преднамеренного воздействия (ПДВ).
3. Методы и способы несанкционированного воздействия на носители информации.
4. Методы и способы преднамеренного воздействия на носители информации.
5. Цели и задачи преднамеренного воздействия на носители информации.
6. Принцип работы блокиратора сотовых телефонов.

Литература:

1. *Данилов, А. Н.* Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. – Пермь : ПНИПУ, 2007. – 340 с. – ISBN 978-5-88151-821-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/160366 (дата обращения: 04.04.2023). – Режим доступа: для авториз. пользователей.

2. *Титов, А. А.* Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
3. *Рагозин, Ю. Н.* Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161337 (дата обращения: 04.04.2023). — Режим доступа: для авториз. пользователей.
4. Материалы лекций по дисциплине.
5. Описание технических средств, используемых в лабораторной работе.

Материально-техническое обеспечение занятия:

1. устройство предотвращения утечки информации «Терминатор 200».

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Методы и средства защиты информации от утечки по техническим каналам» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий обеспечения безопасности информации от ее утечки по техническим каналам.

Задачи: получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности информации от утечки по техническим каналам; изучение теоретических основ информационной безопасности на объектах информатизации; формирование умений использовать основные достижения в области защиты информации от утечки по техническим каналам при реализации своей профессиональной деятельности; владение практическими навыками защиты информации на объектах информатизации; развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения..

Дисциплина направлена на формирование следующих компетенций:

- УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ОПК-9 – Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

Знать: основные понятия, принципы и модели технической защиты информации; состав и порядок разработки нормативных документов по обеспечению безопасности объектов информатизации; назначение и виды, подлежащих защите информационных ресурсов, моделей и процессов жизненного цикла системы защиты информации; основные демаскирующие признаки объектов защиты.

Уметь: применять физический подход при решении задач технической защиты информации; разрабатывать нормативные документы по обеспечению безопасности объектов информатизации от утечки информации по техническим каналам; организовать работу по обеспечению безопасности объектов информатизации от воздействия источников угроз и угроз.

Владеть: физической терминологией, физическими понятиями и теориями, используемыми при технической защите информации; навыками использования стандартов и руководящих документов по защите объектов информатизации; навыками по моделированию источников угроз и угроз безопасности объектов информатизации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.