Приложение Л.РПД Б1.В.07

Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

УТВЕРЖДАЮ
Зам. директора
по учебно-методической работе
филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске
_____ В.В. Рожков
«11» 10 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01 Информационная безопасность

Магистерская программа: Безопасность автоматизированных систем

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Смоленск

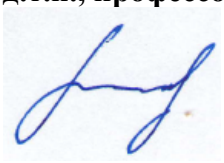
Программа составлена с учетом ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от «26» ноября 2020 г. № 1455

Программу составил:
к.т.н., доцент

К.И. Свириденков
«21» сентября 2021 г.

Программа обсуждена и одобрена на заседании кафедры «вычислительная техника»
«22» сентября 2021 г., протокол № 2

Заведующий кафедрой вычислительной техники
д.т.н., профессор



А.С. Федулов

«08» октября 2021 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

Е.В. Зуева

«08» октября 2021 г.

1. 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к проектной и научно-исследовательской деятельностям по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач.

2. 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Технические средства защиты информации» относится к вариативной части программы.

Данная дисциплина в траектории формирования профессиональной компетенции ПК-1 находится на заключительной стадии.

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

Б1.В.03	Проектирование программного обеспечения автоматизированных систем
Б1.В.05	Интеллектуальный анализ и моделирование информационных систем и процессов
Б1.В.06	Криптографические методы и средства защиты информации
Б1.В.ДВ.01.01	Цифровая обработка сигналов

Перечень последующих дисциплин, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:

Б2.В.02(П)	Проектно-технологическая практика
Б2.В.03(П)	Преддипломная практика
Б3.01	Подготовка к защите и защита выпускной квалификационной работе

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-3. Способен управлять безопасностью компьютерных систем и сетей (06.032-D/01.7-D/04.7) (06.033-C/01.7, C/06.7)	**ПК-3.1.** Проводит анализ безопасности компьютерных систем и сетей	**Знает:** - технические каналы "утечки" информации; - технические средства контроля эффективности мер защиты информации; - принципы построения средств защиты информации от "утечки" по техническим каналам - основные характеристики технических средств защиты информации от утечек по техническим каналам **Умеет:** - анализировать архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; - выполнять анализ безопасности компьютерных систем. **Владеет:** - навыками выявления основных угроз безопасности в автоматизированных система; - подбором инструментальных средств тестирования систем защиты информации автоматизированных систем; - основными методами управления информационной безопасностью.

	ПК-3.2. Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	**Знает**: - угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в автоматизированных системах; - организацию защиты информации от "утечки" по техническим каналам на объектах информатизации; - средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; - нормативные правовые акты в области защиты информации. **Умеет:** - формализовать задачу управления безопасностью компьютерных систем и сетей; - применять действующую нормативную базу в области обеспечения безопасности информации; - разрабатывать проекты нормативных документов, регламентирующих работу по защите информации. **Владеет:** - заданием требований к защите информации компьютерных систем и сетей; - разработкой проектов нормативных документов, регламентирующих работу по защите информации; - документированием программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Индекс	Наименование	Семестр 3										Итого за курс									
		Контроль	Академических часов								з.е.	Контроль	Академических часов								з.е.
			Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль			Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего
Б1.В.07	Технические средства защиты информации	Экз	**180**	86	34	34	18		58	36	5	Экз	**180**	86	34	34	18		58	36	5

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз – экзамен.

Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КР – курсовая работа;
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	**Лекционные занятия – 10 шт. по 2 час, 3 шт. по 4 часа:** **1. РАЗДЕЛ 1. Теоретические основы технической защиты информации** **Лекция 1. Введение в курс «Технические средства защиты информации». (2часа)** Место технической защиты информации в обеспечении информационной безопасности. Предмет, цели, задачи, содержание и структура дисциплины техническая защита информации (ТЗИ). Базовые знания, необходимые для изучения курса. Виды и формы отчетности. Рекомендуемые учебные пособия основной и дополнительной литературы по дисциплине. **Лекция 2. Общие положения технической защиты информации. (2 часа)** Особенности задач технической защиты информации. Основные параметры системы ТЗИ. Представление сил и средств технической защиты информации в виде системы технической защиты информации. Цели и задачи технической защиты информации. Понятие о безопасности информации. Затраты на информацию. Ресурсы системы. Меры технической защиты информации. Процесс преобразования входов в выходы. Критерии эффективности мер технической защиты информации. Основные направления организации технической защиты информации. **Лекция 3. Особенности информации, как предмета технической защиты. (2 часа)** Демаскирующие признаки объектов и их классификация. Информативность. Понятие признаковой структуры. Видовые, сигнальные и вещественные демаскирующие признаки. Демаскирующие объекты, сигналы и вещества. Носители информации. Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы как источники сигналов. Источники случайных опасных сигналов. Пути распространения опасных сигналов из помещения. Классификация побочных электромагнитных излучений и наводок. Виды акустоэлектрических преобразователей и их параметры. Побочные низкочастотные излучения и их источники. Источники высокочастотных побочных излучений. Условия возникновения паразитной генерации в усилителях. Способы высокочастотного навязывания. Сосредоточенные и распределенные источники электромагнитного поля. Понятие ближней и дальней зон. Характер распространения электромагнитных полей сосредоточенных источников в ближней и дальней зонах. Виды излучений распределенных источников электромагнитного поля. Понятие о цепях Пикара. Виды паразитных связей. Факторы, вызывающие проникновению опасных сигналов в цепи электропитания и заземления. **Лекция 4. «Аппаратные средства повышения отказоустойчивости и надежности информационных систем» (2 часа)** Понятие надежности и отказоустойчивости. Защита систем от проблем с питанием. Виды устройств защиты. Классификация источников бесперебойного питания, области защиты. Дублирование – как основной способ повышения отказоустойчивости.

РАЗДЕЛ 2. Технические каналы утечки информации

Лекция 5. Понятие, назначение и классификация технических каналов утечки информации. (4 часа)

Понятие технического канала утечки информации. Простые и составные каналы утечки информации. Структура и основные показатели технических каналов утечки информации (общая схема образования каналов утечки информации). Классификация технических каналов утечки информации в зависимости от источника конфиденциальной информации (объекта защиты). Характеристика первоочередных источников, образующих каналы утечки информации и воздействия на информацию. Каналы утечки информации из технических систем и средств передачи, обработки, хранения и отображения информации. Виды технических каналов утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Лекция 6. Технические каналы утечки речевой информации. (4 часа)

Характеристика акустических сигналов технических каналов утечки информации. Основные физические характеристики акустических волн. Параметры речевого сигнала (речевой информации). Понятность и разборчивость речи. Метод артикуляции. Акустический и виброакустический каналы утечки информации, принципы подслушивания речевой информации. Структура акустического канала утечки информации. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации. Особенности акустоэлектрических каналов утечки информации. Назначение, устройство и общая характеристика акустоэлектрических преобразователей. Технические характеристики акустоэлектрического канала утечки информации. Оптико-электронный технический канал утечки акустической информации. Параметрический технический канал утечки акустической информации.

Лекция 7. Технические каналы утечки информации при ее передаче по каналам связи. (4 часа)

Средства передачи электрических сигналов. Напряженность электрического и магнитного полей в пространстве. Электрическое поле. Магнитное поле. Электромагнитная волна. Проводные линии связи (симметричные, несимметричные, коаксиальные).

Электромагнитные каналы утечки информации. Электромагнитные излучения элементов ТСПИ. Электромагнитные излучения на частотах работы генераторов ВЧ ТСПИ и ВТСС. Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Побочные электромагнитные излучения персонального компьютера.

Электрические каналы утечки информации. Наводки электромагнитных излучений ТСПИ. Просачивание информационных сигналов в цепи электропитания. Паразитные связи через цепи питания. Просачивание информационных сигналов в цепи заземления. Индукционный съем информации с электрического каналам утечки информации. Параметрический канал утечки информации.

Лекция 8. Технические каналы утечки видовой информации. Материально-вещественный канал утечки информации. (2 часа)

Визуально-оптический канал утечки информации. Особенности визуально-оптических каналов утечки информации. Структура визуально-оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-

диапазонах в различные периоды времени. Варианты визуально-оптических каналов утечки информации для типовых контролируемых зон организации. Материально-вещественные каналы утечки информации. Особенности материально-вещественных каналов утечки информации. Структура материально-вещественных каналов утечки информации и характеристики ее элементов.

РАЗДЕЛ 3. Принципы, способы и средства добывания информации

Лекция 9. Способы и средства добывания информации техническими средствами. (2 часа)

Типовая структура средства добывания информации. Классификация технических средств добывания по видам носителя информации. Средства обеспечения дистанционного доступа к источникам информации без нарушения контролируемой зоны организации. Классификация и характеристика закладных устройств.

Лекция 10. Способы и средства наблюдения. (2 часа)

Структура и основные характеристики средств наблюдения. Основные показатели средств наблюдения. Виды и технические характеристики визуально-оптических приборов, фото- и киноаппаратов.

Лекция 11. Технические средства перехвата радио и электрических сигналов. (2 часа)

Способы и средства перехвата сигналов. Задачи решаемые при перехвате сигналов. Типовая структура комплекса средств перехвата радио и электрических сигналов. Виды и характеристики антенн и радиоприемников. Основные функции средств анализа сигналов. Особенности и основные характеристики сканирующих радиоприемников.

Лекция 12. Способы и средства подслушивания акустических сигналов. (2 часа)

Типовая структура средства подслушивания. Структура и характеристика технических средств подслушивания. Средства акустической разведки. Классификация и характеристика микрофонов Основные показатели средств подслушивания. Виды микрофонов. Остронаправленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Параметрические акустоэлектрические преобразователи. Способы и средства высокочастотного навязывания. Лазерные средства подслушивания. Контроль и прослушивание телефонных каналов связи. Средства снятия речевой информации с телефонной линии. Подслушивающие закладные устройства, их классификация и основные параметры функционирования.

РАЗДЕЛ 4. Системный подход к обеспечению защиты информации

Лекция 13. Основы системного подхода к защите информации. (2 часа)

Сущность системного подхода и системного анализа. Характеристики системы защиты информации. Характеристика системы защиты информации. Частные и глобальные критерии эффективности системы защиты. Понятие о моделировании как основном процессе системного анализа. Виды моделей и их возможности при исследовании проблем защиты информации.

	Лекция 14. Моделирование объектов защиты и каналов утечки информации. (2 часа) Сущность моделирования. Структурные, функциональные и информационные модели объектов защиты и каналов утечки информации. Принципы построения комплексных моделей объектов защиты и каналов утечки. Подходы к оценке угрозы каналов утечки безопасности конфиденциальной информации. Методические рекомендации по структурированию защищаемой информации. Выявление и описание источников информации. Формы представления моделей объектов информационной безопасности.
2	**Лабораторные занятия – 8 лабораторных работ (по 4 часа) и 1 занятие по защите выполненных лабораторных работ (2 часа)** 2.1. Вводное занятие. Знакомство с лабораторией технических средств защиты информации и организацией работы в ней. Проведение инструктажа по технике безопасности. (2 часа). 2.2. Лабораторная работа № 1. Тема: Исследование воздушного акустического канала утечки речевой конфиденциальной информации. (4 часа). 2.3 Лабораторная работа №2. Тема: Исследование виброакустического канала утечки речевой конфиденциальной информации. (4 часа). 2.4. Лабораторная работа №3. Тема: Обнаружение скрытых видеокамер (4 часа). 2.5. Лабораторная работа №4. Тема: Исследование электромагнитного канала утечки информации из средств вычислительной техники (4 часа). 2.6. Лабораторная работа №5. Тема: Исследование электромагнитного канала утечки информации за счет наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации. (4 часа). 2.7. Лабораторная работа №6. Тема: Подавление интернета и радиостанций. (4 часа). 2.8. Лабораторная работа №7. Тема: Поиск видеокамер с радиоканалом и радиомаяков систем слежения (4 часа). 2.9. Лабораторная работа № 8. Тема: Поиск и локализация подслушивающих устройств, передающих информацию в инфракрасном диапазоне (4 часа).
3	**Практические занятия – 9 семинаров по 2 часа** 3.1. Пути распространения опасных сигналов из помещения. Классификация побочных электромагнитных излучений и наводок. Виды акустоэлектрических преобразователей и их параметры. Побочные низкочастотные излучения и их источники. Источники высокочастотных побочных излучений. Условия возникновения паразитной генерации в усилителях. Способы высокочастотного навязывания. (Семинар – 2 часа). 3.2. Сосредоточенные и распределенные источники электромагнитного поля. Понятие ближней и дальней зон. Характер распространения электромагнитных полей сосредоточенных источников в ближней и дальней зонах. Виды излучений распределенных источников электромагнитного поля. Понятие о цепях Пикара. Виды паразитных связей. Факторы, вызывающие проникновению опасных сигналов в цепи электропитания и заземления (Семинар – 2 часа).

	3.3. Характеристика первоочередных источников, образующих каналы утечки информации и воздействия на информацию. Каналы утечки информации из технических систем и средств передачи, обработки, хранения и отображения информации. (Семинар – 4 часа). 3.4. Характеристика акустических и виброакустических каналов утечки информации. Структура акустического канала утечки информации. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации (Семинар – 4 часа). 3.5. Особенности акустоэлектрических каналов утечки информации. Назначение, устройство и общая характеристика акустоэлектрических преобразователей. Технические характеристики акустоэлектрического канала утечки информации (Семинар – 2 часа). 3.6. Характеристика технических средств подслушивания акустических сигналов. Классификация и характеристика микрофонов. Виды микрофонов. Остронаправленные микрофоны. Стетоскопы. Диктофоны. Средства снятия речевой информации с телефонной линии (Семинар – 2 часа). 3.7 Характеристика радиоэлектронных каналов утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации (Семинар – 2 часа). 3.8. Технические средства и способы добывания информации перехватом радио и электрических сигналов. Назначение, классификация и характеристика закладных устройств. Основное предназначение и характеристика технических способов и средств перехвата сигналов (Семинар – 2 часа). 3.9. Характеристика основных показателей оптоэлектронных линий связи и способы снятия с них информации. (Семинар – 2 часа)
4	**Курсовая работа –** не предусмотрена учебным планом
5	**Самостоятельная работа студентов:** 5.1. Тестирование после 6-й лекции (тест 1) и 12-й лекции (тест 2). 5.2. Подготовка к выполнению лабораторных работ и семинарским занятиям. 5.3. Выполнение курсовой работы – не предусмотрено учебным планом 5.4. Выполнение расчетно-графической работы – не предусмотрено учебным планом. 5.4. Подготовка к экзамену по дисциплине.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица - Образовательные технологии, используемые при реализации различных видов учебной занятий по дисциплине

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция
2	Лабораторная работа	Допуск к лабораторной работе.

		Технология выполнения лабораторных заданий индивидуально.
3	Практические занятия	Технология обучения на основе решения задач и выполнения упражнений
4	Консультации по курсовой работе	Индивидуальные и групповые консультации Информационно-коммуникационные технологии: технология взаимодействия со студентами в синхронном режиме связи — «offline»; технология взаимодействия со студентами в синхронном режиме связи —«online»
5	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
6	Контроль (промежуточная аттестация: экзамен)	Технология устного опроса

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ – ДЛЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает в себя: текущий контроль успеваемости (опрос по материалам лекции, выполнение лабораторных работ и их защита, оценка работы на семинарских занятиях, тестирование и т.п.) и промежуточную аттестацию.

Для текущего контроля результатов образования проводится тестирование:

1. Тест № 1. Общие положения технической защиты информации. Особенности информации, как предмета технической защиты
2. Тест № 2. Классификация и технические характеристики технических каналов утечки информации. Принципы, способы и средства добывания информации.

Вопросы по формированию и развитию теоретических знаний, предусмотренных компетенциями, закрепленными за дисциплиной (вопросы для самоконтроля):

Примеры вопросов к контрольному опросу после 1-й лекции:

1 Дайте определение понятию «информация».
2 Дайте определение понятию «информатизация».
3 Дайте определение понятию «защита информации».
4 Дайте определение понятию «целостность информации».
5 Что относится к техническим средствам защиты информации?
6 Простые и составные каналы утечки информации.

7 Виды технических каналов утечки информации.
8 Основные характеристики технических каналов утечки информации.

Примеры вопросов к контрольному опросу после 6-й лекции:

1. Как характеризуются акустические сигналы технических каналов утечки информации?
2. Какими параметрами оценивается речевая информация?
3. В чем отличие акустического и виброакустического каналов утечки информации?
4. Как влияет время реверберации на разборчивость речи?
5. С помощью каких способов можно увеличить протяженность акустического канала утечки информации?
6. Что понимается под акустоэлектрическим каналом утечки информации.
7. Какими характеристиками оценивается акустоэлектрический канал утечки информации.
8. Что понимается под оптоэлектронным техническим каналом утечки акустической информации.

Описание лабораторных работ представлены в методических указаниях для обучающихся по освоению дисциплины.

Вопросы к экзамену по дисциплине «Технические средства защиты информации»

1. Действия, приводящие к неправомерному овладении конфиденциальной информацией.
2. Демаскирующие признаки объектов. Классификация. Информативность
3. Технические каналы утечки информации. Подробная классификация технических каналов утечки информации. Краткая характеристика каналов
4. Каналы утечки информации обрабатываемой техническими средствами приёма, обработки хранения и передачи информации. Понятие: ВТСС, ОТСС, посторонние проводники, контролированная зона. Краткая характеристика каналов.
5. Каналы утечки информации при её передачи по каналам связи.
6. Материально-вещественный канал утечки информации. Способы восстановления информации на магнитных носителях. Пример программ для восстановления информации с магнитных носителей
7. Оптический канал утечки информации. Характеристика каналов
8. Каналы утечки речевой информации. Краткая характеристика каналов
9. Закладное устройство. Классификация закладных устройств. Типы закладных устройств. Закладные устройства с передачей информации по цепям питания.
10. Микрофоны. Типы микрофонов. Принцип работы. Основные характеристики микрофонов. Системы аудио-мониторинга помещений, основные характеристики данных систем.
11. Направленные микрофоны. Типы направленных микрофонов. Принцип работы. Основные характеристики. Назначение. Примеры направленных микрофонов.
12. Диктофоны. Типы. Классификация. Назначение диктофонов.
13. Лазерные системы акустической разведки. Принцип работы. Назначение. Примеры
14. Способы скрытого видеонаблюдения и съёмки. Основные характеристики современных скрытых камер, Возможности систем видеонаблюдения и съёмки.

15. Средства перехвата радиосигналов. Средства и методы пеленгации источника радиосигнала. Сканирующие радиоприёмники: назначение, основные характеристики.
16. Акустоэлектрические каналы утечки информации. Характеристика канала. Источники акустоэлектрических преобразований.
17. Мероприятия по выявлению и оценке свойств каналов утечки информации.
18. Перехват информации в каналах сотовой связи.
19. Утечка информации в волоконно-оптических линиях связи
20. Методы и средства выявления закладных устройств.
21. Технические средства подавления сигналов радио закладных устройств. Характеристика, примеры
22. Методы подавления записи речевой информации на диктофон. Способы подавления. Средства подавления.
23. Пассивные методы защиты речевой информации от её утечки через ограждающие конструкции. Рекомендации по выбору ограждающих конструкций.
24. Организация защиты речевой информации от утечки по техническим каналам в защищаемом помещение. Методы Зашита информации от направленных и лазерных микрофонов.
25. Структурное скрытие речевой информации.
26. Основные способы и методы защита информации от утечки по акустическим каналам
27. Защита от утечки в волоконно-оптическим линиях и системах связи
28. Активные методы и средства защиты речевой информации от утечки по техническим каналам, Характеристика генераторов шума.
29. Методы и средства защиты информации в телефонных линиях связи.
30. Защита речевой информации от утечки информации за счёт «микрофонного эффекта»
31. Защита речевой информации от утечки информации за счёт «ВЧ-навязывания»
32. Методы и способы защиты информации от утечки по каналу ПЭМИН от ПК.
33. Экранирование электромагнитных волн. Экранирование проводов и катушек индуктивности. Экранированные помещения.
34. Заземление технических средств и подавление информационных сигналов в цепях заземления.
35. Фильтрация информационных сигналов. Основные сведения о помехоподавляющих фильтрах. Выбор типа фильтра.
36. Пространственное и линейное зашумление, основные характеристики ГШ.
37. Скрытие речевой информации в телефонных системах с использованием криптографических методов.
38. Перехват информации в телефонных линиях связи
39. Организация защиты информации от утечки по цепям питания.
40. Методы, способы, средства защиты информации от утечки по материально-вещественному каналу

В филиале используется система с традиционной шкалой оценок – "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", "зачтено", "не зачтено" (далее - пятибалльная система).

Форма промежуточной аттестации по настоящей дисциплине – Экзамен **с оценкой**.

Применяемые критерии оценивания по дисциплинам (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23):

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «эталонный».
«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом непринципиальные ошибки. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «продвинутый».
«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «пороговый».
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут продолжить обуче-

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	ние по образовательной программе без дополнительных занятий по соответствующей дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная:

- специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное:

- специализированной мебелью; доской аудиторной; персональным компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

Программное обеспечение:

Операционная система OS Windows 10; офисный пакет Microsoft Office – для работы над РПД и методическим обеспечением к ней.

2.

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;
- 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;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

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 филиалом, 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.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1 Зайцев, А. П. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. — Москва : Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111057 (дата обращения: 21.04.2021). — Режим доступа: для авториз. пользователей.

2 Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная

система. — URL: https://e.lanbook.com/book/125739 (дата обращения: 21.04.2021). — Режим доступа: для авториз. пользователей.

Дополнительная литература.

1. Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=208661 (дата обращения: 21.04.2021). – Текст : электронный.

2. Креопалов, В.В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. – Москва : Евразийский открытый институт, 2011. – 278 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90753 (дата обращения: 21.04.2021). – ISBN 978-5-374-00507-3. – Текст : электронный.

Список авторских методических разработок.

1. Тест № 1. Общие положения технической защиты информации. Особенности информации, как предмета технической защиты

2. Тест № 2. Классификация и технические характеристики технических каналов утечки информации. Принципы, способы и средства добывания информации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10