Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и системы

Попов М.А., канд. техн. наук, доцент

11.06.2021

РАБОЧАЯ ПРОГРАММА

дисциплины **Техническая защита информации и средства контроля**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): Ст. препод., Рак Е.В.

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 09.06.2021г. № 6

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 11.06.2021 г. № 6

г. Хабаровск
2022 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины Техническая защита информации и средства контроля

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1457

Квалификация **специалист по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
контактная работа 62
самостоятельная работа 46

Виды контроля в семестрах:
зачёты (семестр) 10

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	4	4	4	4
Итого ауд.	48	48	48	48
Контактная работа	62	62	62	62
Сам. работа	46	46	46	46
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Виды, источники и носители защищаемой информации; демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники; побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации; классификация технической разведки; основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки; концепция и методы инженерно-технической защиты информации; методы и средства инженерной защиты и технической охраны объектов; скрытие объектов наблюдения; скрытие речевой
1.2	информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств,
1.3	подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов; характеристика государственной системы противодействия технической разведке; нормативные документы по противодействию технической разведке; виды контроля эффективности защиты информации; основные положения методологии инженерно-технической защиты информации; методы расчета и инструментального контроля показателей защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.В.11
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Основы программно-аппаратных средств защиты информации
2.1.2	Управление информационной безопасностью
2.1.3	Защита информации от утечки по техническим каналам
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Научно-исследовательская работа
2.2.2	Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-9.1: Тестирование систем защиты информации автоматизированных систем
Знать:
нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации методы тестирования и отладки программного и аппаратного обеспечения
Уметь:
проводить комплексное тестирование и отладку аппаратных и программных систем защиты информации
Владеть:
навыками составления протоколов тестирования систем защиты информации автоматизированных систем и навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	Характеристика технической разведки. Основные этапы добывания информации. Технология добывания информации. Способы несанкционированного доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. Доступ к источникам информации без нарушения государственной границы. Показатели эффективности добывания информации. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	

1.2	Технические каналы утечки информации. Закладные устройства и за -щита от них. Построение и общие характеристики закладных устройств. Радиозакладные устройства. Радиозакладные переизлучающие устройства. Закладные устройства типа «длинное ухо». Сетевые закладные устройства. Направления защиты от закладных устройств. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	2	
1.3	Технические каналы утечки информации. Общая характеристика ТКУИ. Определение ТКУИ. Место ТКУИ в общей системе угроз безопасности информации. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.4	Технические каналы утечки информации. ТКУИ, обрабатываемой ТСПИ. Электромагнитные каналы. Электрические каналы. Параметрические каналы. Вибрационные каналы. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
1.5	Технические каналы утечки информации. ТКУИ речевой информации. Акустические каналы. Виброакустические каналы. Акустоэлектрические каналы. Оптико-электронные каналы. Параметрические каналы. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.6	Технические каналы утечки информации. ТКУИ при ее передаче по каналам связи. Электромагнитные каналы. Электрические каналы. Индукционные каналы. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
1.7	Технические каналы утечки информации. ТКУИ при ее передаче по каналам связи. Технические каналы утечки видовой информации. Наблюдение за объектами. Съемка объектов. Съемка документов. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
1.8	Технические каналы утечки информации. Несанкционированный доступ к информации обрабатываемой средствами вычислительной техники. Атаки на уровне систем управления базами данных. Атаки на уровне операционной системы. Атаки на уровне сетевого программного обеспечения. Программные закладки. /Лек/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 2.						
2.1	Оптимизация системы активной защиты двери и стены по акустическому и виброакустическому каналам и оценка её эффективности /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.2	Оптимизация системы защиты окон по виброаку-стическому каналу и оценка ее эффективности /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.3	Оценка эффективности генератора шума для защиты по каналу ПЭМИ /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	

2.4	Оптимизация системы активной защиты вентиля-ции и батареи водяного отопления по акустиче-скому и виброакустическому каналам и оценка её эффективности /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
2.5	Измерение затухания электромагнитных сигналов /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.6	Оценка защищенности окон от утечки информации по акустическому и виброакустическому каналам /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
2.7	Оценка защищенности двери и стены от утечки информации по акустическому и виброакустическому каналам /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
2.8	Освоение практических приёмов работы с системой «Шепот» /Лаб/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
	Раздел 3.						
3.1	Оптимизация системы активной защиты двери и стены по акустическому и виброакустическому каналам и оценка её эффективности /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.2	Оптимизация системы защиты окон по виброаку-стическому каналу и оценка ее эффективности /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
3.3	Оптимизация системы активной защиты вентиля-ции и батареи водяного отопления по акустиче-скому и виброакустическому каналам и оценка её эффективности /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.4	Измерение затухания электромагнитных сигналов /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.5	Оценка защищенности окон от утечки информации по акустическому и виброакустическому каналам /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.6	Оценка защищенности двери и стены от утечки информации по акустическому и виброакустическому каналам /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
3.7	Освоение практических приёмов работы с системой «Шепот» /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
3.8	Оценка эффективности генератора шума для защиты по каналу ПЭМИ /Пр/	10	2	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 4.						

4.1	Изучение теоретического материала по лекциям, учебной литературе и интернет-ресурсам /Ср/	10	14	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
4.2	Оформление отчетов по лабораторным работам и подготовка к их защите /Ср/	10	10	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	0	
4.3	Изучение технической документации и функционала технических средств защиты информации /Ср/	10	10	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	
	Раздел 5.						
5.1	Подготовка к зачету /Зачёт/	10	12	ПК-9.1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э3 Э4 Э5	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Степанов Е. А., Корнеев И. К.	Информационная безопасность и защита информации: Учеб. пособие	Москва: ИНФРА-М, 2001,
Л1.2	Яковлев В. В., Корниенко А. А.	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учеб. для вузов жд тр-та	Москва: УМК МПС России, 2002,
Л1.3	Н.А. Свинарев	Инструментальный контроль и защита информации	Воронеж: Воронежский государственный университет инженерных технологий, 2013, http://biblioclub.ru/index.php?page=book&id=255905
Л1.4	Прохорова О. В.	Информационная безопасность и защита информации: Учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014, http://biblioclub.ru/index.php?page=book&id=438331

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Титов А. А.	Инженерно-техническая защита информации	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010, http://biblioclub.ru/index.php?page=book&id=208567
Л2.2	Аверченков В. И., Рытов М. Ю.	Организационная защита информации	Москва: Флинта, 2011, http://biblioclub.ru/index.php?page=book&id=93343

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	ФСТЭК России	http://www.fstec.ru
Э2	Компания Код безопасности	http://www.securitycode.ru
Э3	ФСБ России	http://www.fsb.ru
Э4	Национальный отрытый институт	http://www.intuit.ru

Э5	Группа компаний МАСКОМ	http://www.mascom.ru/

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

Office Pro Plus 2007 - Пакет офисных программ, лиц.45525415
Windows 7 Pro - Операционная система, лиц. 60618367
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

Информационно-правовой портал Гарант.ру - http://www.garant.ru
Информационно-правовой портал КонсультантПлюс - http://www.consultant.ru
Профессиональные справочные системы Техэксперт - http://www.cntd.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

С целью эффективной организации учебного процесса учащимся в начале семестра предоставляется учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе.
В процессе обучения студенты должны, в соответствии с календарным планом, самостоятельно изучать теоретический материал по предстоящему занятию и формулировать вопросы, вызывающие у них затруднение для рассмотрения на лекционном, практическом или лабораторном занятии.
В назначенные дни студент имеет возможность получить консультации у ведущего преподавателя.
При проведении лабораторных (практических) работ от студента требуется выполнять все требования преподавателя. По результатам выполнения каждой лабораторной (практической) работы формируется отчет, который подлежит последующей защите. Правила оформления отчета и требования к содержанию находятся в методических указаниях к лабораторным (практическим) работам.
Перед осуществлением защиты лабораторной (практической) работы студенту необходимо освоить весь теоретический материал, имеющий отношение к данной лабораторной работе. Подготовка к защите лабораторной (практической) работы включает в себя самоподготовку и консультации.
После получения задания студенту предоставляется возможность подготовиться к ответу в течение не более академического часа. Аттестация в письменной форме проводится для всех студентов академической группы одновременно. При аттестации в форме собеседования преподаватель обсуждает со студентом один или несколько вопросов из учебной программы. При необходимости преподаватель может предложить дополнительные вопросы, задачи и

примеры. Для проведения аттестации в письменной форме используется перечень вопросов, утвержденный заведующим кафедрой. В перечень включаются вопросы из различных разделов курса, позволяющие проверить и оценить теоретические знания студентов и умение применять их для решения практических задач.
По окончании ответа студента на вопросы преподаватель проставляет результаты сдачи. Лабораторная (практическая) работа остаются у преподавателя.
Для подготовки к промежуточной аттестации студенту рекомендуется ознакомиться со списком вопросов и успешно ответить на содержащиеся в них вопросы.
Для повышения качества подготовки и самопроверки знаний студентам рекомендуется систематически изучать учебные материалы, и отвечать на контрольные вопросы.