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

27.05.2022

РАБОЧАЯ ПРОГРАММА

дисциплины **Моделирование защищенных автоматизированных систем**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.ф.м.н, Доцент, Карачанская Е.В.

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

Протокол от 18.05.2022г. № 5

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 27.05.2022 г. № 7

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 Моделирование защищенных автоматизированных систем

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 60
самостоятельная работа 48

Виды контроля в семестрах:
зачёты (семестр) 8

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	16 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	12	12	12	12
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	60	60	60	60
Сам. работа	48	48	48	48
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Угрозы и их источники безопасности информационно - телекоммуникационным системам. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах. Основные задачи обеспечения безопасности информации в информационных системах. Математические метода моделирования угроз. Методы исследования угроз информационной безопасности автоматизированных систем. Использования инструментальных средств для анализа защищенности объектов информатизации. Требования нормативно-методических документов по защите информации. Классический подход. Официальный подход. Организация контроля эффективности защиты объектов информатизации. Формирование модели угроз информационной системе. Определение актуальности угроз. Математические способы анализа защищенности объектов информатизации и информационных систем. Анализ защищенности информационных систем на основе моделирования угроз. Критерии оценки эффективности. Требования к средствам контроля эффективности защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.В.14
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Теория автоматов
2.1.2	Математическая логика и теория алгоритмов
2.1.3	Теория информации и кодирования
2.1.4	Теория вероятностей и математическая статистика
2.1.5	Дискретная математика
2.1.6	Основы информационной безопасности
2.1.7	Алгебра и геометрия
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационные системы на железнодорожном транспорте
2.2.2	Тестирование средств защиты информации

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ПК-9.2: Разработка проектных решений по защите информации в автоматизированных системах

Знать:

нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации;
основы построения информационных систем и формирования информационных ресурсов;
меры и методы обеспечения информационной безопасности

Уметь:

работать с действующей нормативной правовой и методической базой в области защиты информации;
определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации;
разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗКИ, а также оформлять результаты аттестации объектов информатизации по требованиям безопасности информации;
пользоваться средствами обеспечения информационной безопасности

Владеть:

навыками организации деятельности подразделений и специалистов в области ТЗКИ в органах государственной власти и организациях
навыками работы с действующей нормативной правовой и методической базой в области защиты информации;
способностью разрабатывать системы обеспечения информационной безопасности

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	Угрозы и их источники безопасности информационно - телекоммуникационным системам. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах. /Лек/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	0	

1.2	Основные задачи обеспечения безопасности информации в информационных системах. Математические метода моделирования угроз. /Лек/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	0	
1.3	Методы исследования угроз информационной безопасности автоматизированных систем. Использование инструментальных средств для анализа защищенности объектов информатизации. /Лек/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
1.4	Требования нормативно-методических документов по защите информации. Классический подход. Официальный подход. Организация контроля эффективности защиты объектов информатизации. /Лек/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	0	
1.5	Формирование модели угроз информационной системе. Определение актуальности угроз. Математические способы анализа защищенности объектов информатизации и информационных систем. /Лек/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	0	
1.6	Анализ защищенности информационных систем на основе моделирования угроз. Критерии оценки эффективности. Требования к средствам контроля эффективности защиты информации. /Лек/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
	Раздел 2. Лабораторные						
2.1	Свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом IDS/IPS Snort /Лаб/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.2	Suricata —open source IPS/IDS система. /Лаб/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.3	Сетевой анализатор Wireshark /Лаб/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.4	Среда тестирования на проникновение Metsploit Framework. Анализ уязвимостей, тестирование известных эксплойтов и полная оценка безопасности /Лаб/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.5	Инструмент анализа веб-безопасности Burp Suite Scanner /Лаб/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.6	Тестер на проникновение для оценки безопасности веб-браузера. BeEF (Browser Exploitation Framework) /Лаб/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
	Раздел 3. Практические						
3.1	Понятие «атака» и «операция» в информационном аспекте. Классификация атак. Этапы реализации атак: сбор информации, основные механизмы реализации атак, реализация атак, завершение атаки. Принципы построения СОВ. Классификация и архитектура. /Пр/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1 Э2	0	
3.2	Существующие технологии СОВ. Повышение эффективности систем. Характеристика направлений и групп методов обнаружения вторжений. Сравнительный анализ существующих СОВ. /Пр/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	

3.3	Табличные и диаграммные модели информационных атак Формализованные модели информационных атак Анализ существующих моделей процесса обнаружения информационных атак Сигнатурные модели процесса обнаружения атак Поведенческие модели процесса выявления атак Модели процесса оценки рисков информационной безопасности АС /Пр/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
3.4	Программа и методика испытаний разработанного прототипа системы обнаружения атак, построенного на основе поведенческой модели Объект и цель испытаний Функциональные требования к прототипу системы обнаружения атак. Технические и программные средства проведения испытаний Порядок проведения испытаний Результаты проведённых испытаний Описание системы обнаружения атак, предназначенной для промышленной реализации Хостовые датчики системы обнаружения атак Сетевые датчики системы обнаружения атак Агенты системы обнаружения атак Модуль реагирования системы обнаружения атак Информационный фонд системы обнаружения атак Консоль администратора системы обнаружения атак Модуль координации потоков информации системы обнаружения атак /Пр/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	4	метод проектов
3.5	Математическая модель информационных атак на ресурсы автоматизированных систем Формальное описание модели информационных атак Особенности использования разработанной математической модели информационных атак Математическая модель процесса обнаружения информационных атак Математическая модель процесса оценки рисков информационной безопасности автоматизированных систем.Описание модели процесса оценки рисков информационной безопасности.Особенности использования модели оценки рисков безопасности. Методика разработки рекомендаций по повышению уровня защиты автоматизированных систем на основе модели оценки рисков безопасности /Пр/	8	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3	4	метод проектов

3.6	Анализ террористической деятельности. Сценарные модели наиболее масштабных террористических операций в информационном аспекте. Вероятностные и энтропийные модели террористических атак. Вероятностные модели информационно-психологических последствий террористических актов /Пр/	8	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2 Э1	0	
	Раздел 4. Самостоятельная работа						
4.1	Подготовка к лекциям /Ср/	8	12	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.2	подготовка к лабораторным /Ср/	8	14	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.3	подготовка к практическим /Ср/	8	14	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.4	подготовка к зачету /Ср/	8	8	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	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	Ададуров С.Е.	Информационная безопасность и защита информации на железнодорожном транспорте. в 2 - ч.: Учеб.	Москва: ФГБОУ, 2014,
Л1.2	Корниенко А.А.	Информационная безопасность и защита информации на железнодорожном транспорте. в 2- х ч. Ч -2	Москва: ФГБОУ, 2014,
Л1.3	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва|Берлин: Директ- Медиа, 2019, http://biblioclub.ru/index.php?page=book&id=499170

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: ПГТУ, 2019, http://biblioclub.ru/index.php?page=book&id=562246
Л2.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва|Берлин: Директ- Медиа, 2020, http://biblioclub.ru/index.php?page=book&id=571485
Л2.3	Бабаш А.В., Баранова Е.К., Мельников Ю.Н.	Информационная безопасность. Лабораторный практикум + еПриложение: Учебное пособие	Москва: КноРус, 2021, https://www.book.ru/book/936566

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

Э1	Национальный открытый университет	http://www.intuit.ru/catalog/
Э2	Открытое образование	https://openedu.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

Windows 10 - Операционная система, лиц.1203984220 ((ИУАТ)

Free Conference Call (свободная лицензия)

Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

Техэксперт - Профессиональная справочная система
КонсультантПлюс - Справочно-правовая система
do.dvgups.ru - Электронная образовательная среда ДВГУПС

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

Аудитория	Назначение	Оснащение
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)
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
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

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

Занятия по дисциплине реализуются с использованием как активных, так и интерактивных форм обучения, позволяющих взаимодействовать в процессе обучения не только преподавателю и студенту, но и студентам между собой.
В соответствии с учебным планом для слушателей дневного отделения изучение курса предполагает выполнение установленного комплекса практических работ (в аудитории), а также расчетно-графических работ (самостоятельно) в течение одного семестра.
Необходимый и достаточный для успешного выполнения практической работы объем теоретического материала изложен в методических указаниях или на практических занятиях. При выполнении задания должны соблюдаться все требования, изложенные в методических указаниях.
Практическая работа считается выполненной, если студент смог продемонстрировать на лабораторном стенде – ПК с соответствующим программным обеспечением правильный результат и пояснить ход выполнения работы.

Отчет должен соответствовать следующим требованиям:
1. Отчет результатов оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
2. Изложение материала в отчете должно быть последовательным и логичным. Отчет состоит из задания, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем работы должен быть не более – 10-15 страниц.
4. Отчет должен быть отпечатан на компьютере через 1-1,5 интервала, номер шрифта – 12-14 пт Times New Roman.
Расположение текста должно обеспечивать соблюдение следующих полей:
− левое 20 мм.
− правое 15 мм.
− верхнее 20 мм.
− нижнее 25 мм.
5. Все страницы отчета, включая иллюстрации и приложения, имеют сквозную нумерацию без пропусков, повторений, литературных добавлений. Первой страницей считается титульный лист, на которой номер страницы не ставится.
6. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
7. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
8. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.

9. Ссылки на литературный источник в тексте сопровождаются порядковым номером, под которым этот источник включен в список используемой литературы. Перекрестная ссылка заключается в квадратные скобки. Допускаются постраничные сноски с фиксированием источника в нижнем поле листа.
10. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

При подготовке к зачету с оценкой необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, образовательные Интернет - ресурсы. Студенту рекомендуется также в начале учебного курса познакомиться со следующей учебно-методической документацией:
- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами практических занятий;
- учебниками, пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету с оценкой.

После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть в процессе освоения дисциплины. Систематическое выполнение учебной работы на практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета с оценкой.

Оформление и защита производится в соответствии со стандартом ДВГУПС СТ 02-11-17 «Учебные студенческие работы. Общие положения»
Оценка знаний по дисциплине производится в соответствии со стандартом ДВГУПС СТ 02-28-14 «Формы, периодичность и порядок текущего контроля успеваемости и промежуточной аттестации».