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

26.04.2024

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 24.04.2024г. № 4

Обсуждена на заседании методической комиссии по родственным направлениям и специальностям: Протокол

г. Хабаровск
2024 г.

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

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2028 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) 9

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		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	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.15
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	Аттестация на соответствие требованиям по защите информации
2.2.2	Информационная безопасность автоматизированных систем на транспорте

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/	9	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/	9	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/	9	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/	9	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/	9	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/	9	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/	9	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.2	Suricata —open source IPS/IDS система. /Лаб/	9	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.3	Сетевой анализатор Wireshark /Лаб/	9	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/	9	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
2.5	Инструмент анализа веб-безопасности Burp Suite Scanner /Лаб/	9	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/	9	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/	9	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2Л3.1 Э1 Э2	0	
3.2	Существующие технологии СОВ. Повышение эффективности систем. Характеристика направлений и групп методов обнаружения вторжений. Сравнительный анализ существующих СОВ. /Пр/	9	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2Л3.1	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/	9	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2Л3.1	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/	9	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2Л3.1 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/	9	4	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3Л3.1	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/	9	2	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2Л3.1 Э1	0	
	Раздел 4. Самостоятельная работа						
4.1	Подготовка к лекциям /Ср/	9	12	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.2	подготовка к лабораторным /Ср/	9	14	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.3	подготовка к практическим /Ср/	9	14	ПК-9.2	Л1.1 Л1.2 Л1.3Л2.2	0	
4.4	подготовка к зачету /Ср/	9	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., Ищейнов Вячеслав	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва, Берлин: Директ-Медиа, 2020, https://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

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Сырецкий Г. А.	Моделирование систем. Лабораторный практикум	Новосибирск: НГТУ, 2011, http://biblioclub.ru/index.php?page=book&id=229304

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	Учебная аудитория для проведения лабораторных и практических занятий. Лаборатория "Специальных информационных и автоматизированных систем".	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader- Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022. комплект учебной мебели, доска маркерная, проектор Windows 10 Pro Электронные ключи Контракт 1044 ДВГУПС от 25.11.2019 бессрочная Office Pro Plus 2007 Номера лицензий: 45525415 (ГК 111 от 22.04.2009, бессрочная), 46107380 (Счет 00000000002802 от 14.11.07, бессрочная)
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная лаборатория "Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях".	комплект учебной мебели, мультимедийный проектор, экран, автоматизированное рабочее место IZEC «Студент» в сборе, 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, 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. Лицензионное программное обеспечение: Microsoft Windows Professional 10 Russian 1 License, базовый пакет для сертифицированной версии ОС Windows 8.1 Профессиональная/Pro для использования на 1 АРМ, Microsoft Office Professional Plus 2019 Russian OLP 1 License, программа контроля сертифицированной версии ОС Windows 8.1 Профессиональная, Microsoft Windows Server CAL 2019 Russian OLP 1 License User CAL, Базовый пакет для сертифицированной версии ОС Microsoft Windows Server Datacenter 2012 R2 для использования на 2 процессора, ОС Astra Linux Special Edition (Box версия с установочным комплектом)- Контракт № 12724018158190000324/157 ДВГУПС от 15.03.2019 г. RedCheck Professional на 1 IP-адрес на 1 год , КриптоПро CSP версии 4.0, Dallas Lock 8.0-C с модулями «Межсетевой экран» и «Система обнаружения и предотвращения вторжений», Secret Net Studio 8 в редакции «Постоянная защита» (бессрочная) с модулями защиты от НСД, контроля устройств (СКН) и межсетевого экранирования (МЭ) , Антивирус Kaspersky Endpoint Security бизнеса – Расширенный Russian Edition. 1500-2499 Node 1 year Educational Renewal License -

Аудитория	Назначение	Оснащение
		Контракт №12724018158190000584/290 ДВГУПС от 08.05.2019 г. комплект учебной мебели, доска маркерная, проектор Windows 10 Pro Электронные ключи Контракт 1044 ДВГУПС от 25.11.2019 бессрочная Office 2019 Pro Электронные ключи Контракт 757 ДВГУПС от 16.12.2020
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы.	Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор. Лицензионное программное обеспечение: Windows 10 Pro - MS DreamSpark 700594875, 7-Zip 16.02 (x64) - Свободное ПО, Autodesk 3ds Max 2021, Autodesk AutoCAD 2021, Autodesk AutoCAD Architecture 2021, Autodesk Inventor 2021, Autodesk Revit 2021- Для учебных заведений предоставляется бесплатно, Foxit Reader- Свободное ПО, MATLAB R2013b - Контракт 410 от 10.08.2015, Microsoft Office Профессиональный плюс 2007 - 43107380, Microsoft Visio профессиональный 2013 - MS DreamSpark 700594875, Microsoft Visual Studio Enterprise 2017- MS DreamSpark 700594875, Mozilla Firefox 99.0.1 - Свободное ПО, Opera Stable 38.0.2220.41 - Свободное ПО, PTC Mathcad Prime 3.0 - Контракт 410 от 10.08.2015 лиц. 3A1874498, КОМПАС-3D V19 - КАД-19-0909, АСТ-Тест лиц. АСТ.РМ.А096.Л08018.04, Договор № Л-128/21 от 01.06.2021 с 01 июля 2021 по 30 июня 2022. ПЭВМ с возможностью выхода в интернет по расписанию Windows 10 Pro Контракт №235 ДВГУПС от 24.08.2021; Office Pro Plus 2019 Контракт №235 от 24.08.2021; Kaspersky Endpoint Security Контракт № 0322100012923000077 от 06.06.2023; КОМПАС-3D V19 Контракт № 995 от 09.10.2019; nanoCAD Номер лицензии: NC230P-81412 Срок действия: с 01.08.2023 по 31.07.2024;
304	Учебная аудитория для проведения занятий лекционного типа.	Интерактивная доска, мультимедийный проектор, персональный компьютер с программным обеспечением, комплект учебной мебели Windows XP Номер лицензии: 46107380 Счет 00000000002802 от 14.11.07, бессрочная; Office Pro Plus 2007 Номера лицензий: 45525415 (ГК 111 от 22.04.2009, бессрочная), 46107380(Счет 00000000002802 от 14.11.07, бессрочная); Visio Pro 2007 Номер лицензии: 45525415 ГК 111 от 22.04.2009, бессрочная.

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».

Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация: специализация N 9 "Безопасность автоматизированных систем на транспорте" (по видам)

Дисциплина: Моделирование защищенных автоматизированных систем

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительн	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено

Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям. Образец экзаменационного билета

Компетенция ПК-9.2:

1. Поясните отличия понятий множества и системы.
2. Обоснуйте мотивы формирования систем из множеств и наоборот.
3. Приведите базовые свойства системы.
4. Поясните сущность понятий угроза, уязвимость, ущерб и безопасность.
5. Поясните сущность информационно-кибернетических и информационно-психологических операций
6. Перечислите основные виды информационных операций
7. Приведите теоретико-множественную постановку задачи управления социотехническими системами
8. Поясните сущность функций чувствительности в приложении к оценке безопасности социотехнических систем
9. Приведите выражения для интегрального, усредненного, элементарного риска и защищенности социотехнических систем
10. Поясните мотивы соперничества и сотрудничества социотехнических систем?
11. Перечислите качества информации, существенные для ее безопасности, а также операции, нарушающие безопасность
12. Приведите классификацию сетевых угроз и атак
13. На моделях поясните сущность атак, основанных на подборе имени пароля посредством

перебора

14. Приведите модели атак, основанных на анализе сетевого трафика
15. На моделях поясните сущность атак, основанных на сканировании портов
16. Приведите модели атак, основанных на внедрении ложного доверенного объекта
17. На моделях поясните сущность атак, приводящих к отказу в обслуживании.
18. Поясните сущность интегрального усредненного риска и защищенности систем на примере различных законов дискретных распределений вероятностей успеха кибератаки
19. Приведите модели простейших операций информационно-психологического управления
20. Поясните сущность неформальных организаций
21. Приведите специфику информационных технологий деструктивных культов.
22. Покажите особенности информационных операций, реализуемых в рамках политических технологий
23. Перечислите средства противодействия деструктивным информационно-психологическим операциям
24. Приведите стохастические модели информационно-управляющего воздействия
25. Поясните стратегии информационно-управляющих воздействий
26. На основе теории конфликтов проведите анализ мотивов террористической деятельности
27. Поясните специфику информационных операций террористического характера
28. На моделях покажите сущность процессов последействия информационных операций террористического характера.
29. Приведите сценарные модели информационных операций террористического характера
30. Перечислите меры противодействия информационным операциям террористического характера
31. Перечислите приемы кибертерроризма
32. Опишите кризисный период, режим бифуркации и запас устойчивости социотехнических систем с учетом риска теракта
33. Поясните качественно динамику информационного противоборства на основе поверхности риска теракта
34. Обоснуйте сравнение теракта с детонатором информационной бомбы.
35. Табличные и диаграммные модели информационных атак
36. Формализованные модели информационных атак
37. Анализ существующих моделей процесса обнаружения информационных атак
38. Сигнатурные модели процесса обнаружения атак
39. Поведенческие модели процесса выявления атак
40. Модели процесса оценки рисков информационной безопасности АС
41. Математическая модель информационных атак на ресурсы автоматизированных систем

3. Тестовые задания. Оценка по результатам тестирования.

Примерные задания теста

Задание 1 (ПК-9.2)
Выберите правильный вариант ответа.
Условие задания:
Атака доступа направлена на:
А. уничтожение информации
Б. уничтожение компьютера
В. нарушение конфиденциальности информации

Задание 2 (ПК-9.2)
Выберите правильный вариант ответа.
Условие задания:
К основным категориям атак относятся:
А. атаки модификации
Б. атаки на отказ от обязательств
В. атаки прохода

Задание 3 (ПК-9.2)
Выберите правильный вариант ответа.
Условие задания:
1.К основным категориям атак относятся:
А. атаки на отказ в обслуживании

Б. атаки прохода
В. атаки трансформации

Задание 4 (ПК-9.2)
Выберите правильный вариант ответа.
Условие задания:
Наиболее надежный способ аутентификации:
А. парольная защита
Б. смарт-карты
В. биометрические методы

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).

Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительн	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.

Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.