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

Защита информации в распределенных информационных системах и центрах обработки данных

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.т.н., доцент, Ешенко Роман Анатольевич

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.

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 Защита информации в распределенных информационных системах и центрах обработки данных

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

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 **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:	
в том числе:		экзамены (семестр)	7
контактная работа	76	РГР	7 сем. (1)
самостоятельная работа	32		
часов на контроль	36		

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	32	32	32	32
Контроль самостоятельной работы	12	12	12	12
В том числе инт.	8	8	8	8
Итого ауд.	64	64	64	64
Контактная работа	76	76	76	76
Сам. работа	32	32	32	32
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Распределенные информационные системы. Распределенная обработка информации в автоматизированных системах. Архитектура распределенных информационных систем. Распределенные информационные ресурсы и сети. Распределенные файловые системы, базы и банки данных. Технология построения сетевого программного обеспечения. Управление обменом информацией в распределенных информационных системах. Телекоммуникационные среды. Методы, средства и протоколы доступа к среде и удаленным информационным ресурсам. Мультипроцессорные сетевые устройства. Интерфейсы и протоколы связи с объектом. Сетевые протоколы. Методы и средства формального описания протоколов. Методы анализа корректности и верификации протоколов. Тестирование протокольных реализаций. Информация как собственность и товар. Законы РФ об охране информации. Средства и методы защиты информации, механизмы обеспечения безопасности.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.36.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Организационное и правовое обеспечение информационной безопасности
2.1.2	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информации от утечки по техническим каналам
2.2.2	Моделирование защищенных автоматизированных систем
2.2.3	Защита электронного технологического документооборота
2.2.4	Информационная безопасность автоматизированных транспортных систем
2.2.5	Информационная безопасность информационно- управляющих и информационно-логистических систем транспорта
2.2.6	Основы программно-аппаратных средств защиты информации
2.2.7	Разработка и эксплуатация автоматизированных систем в защищенном исполнении
2.2.8	Надежность и оценка рисков

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-9.2.: Способен осуществлять внедрение и эксплуатацию систем защиты информации автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (железнодорожный транспорт);
Знать:
особенности эксплуатации систем защиты информации автоматизированных систем на транспорте особенности эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте
Уметь:
осуществлять внедрение системзащиты информации автоматизированных систем на транспорте осуществлять внедрение систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами
Владеть:
методами эксплуатации систем защиты информации автоматизированных систем на транспорте методами эксплуатации систем защиты информации информационно-управляющих и информационно-логистических систем на транспорте, в том числе автоматизированных систем управления технологическими процессами
ОПК-9.3.: Способен осуществлять контроль защищенности автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (железнодорожный транспорт) с учетом установленных требований безопасности;
Знать:
основные угрозы и уязвимости, методы контроля защищенности автоматизированных систем на транспорте и методы контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте
Уметь:
выявлять уязвимости в автоматизированных системах на транспорте и в информационно-управляющих и информационно-логистических системах на транспорте, в том числе в автоматизированных системах управления технологическими процессами; анализировать, прогнозировать и устранять угрозы информационной безопасности в течение всего времени их применения
Владеть:
навыками применения автоматизированных средств контроля защищенности автоматизированных систем на транспорте и

контроля защищенности информационно-управляющих и информационно-логистических систем на транспорте

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	Распределенные информационные системы. Распределенная обработка информации в автоматизированных системах. Архитектура распределенных информационных систем. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.3 Л1.6Л2.1	0	
1.2	Распределенные информационные ресурсы и сети. Распределенные файловые системы, базы и банки данных. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.6Л2.3	2	лекция-визуализация
1.3	Технология построения сетевого программного обеспечения. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.6	2	дискуссии
1.4	Управление обменом информацией в распределенных информационных системах.Телекоммуникационные среды. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.2 Л1.3 Л1.6 Э1	0	
1.5	Методы, средства и протоколы доступа к среде и удаленным информационным ресурсам. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.6Л2.2 Э2	0	
1.6	Мультипроцессорные сетевые устройства.Интерфейсы и протоколы связи с объектом.Сетевые протоколы. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.2 Л1.6Л2.3	0	
1.7	Методы и средства формального описания протоколов.Методы анализа корректности и верификации протоколов.Тестирование протокольных реализаций. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.6	0	
1.8	Информация как собственность и товар.Законы РФ об охране информации.Средства и методы защиты информации, механизмы обеспечения безопасности. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.2 Л1.6	0	
	Раздел 2. Практические работы						
2.1	Сущность и задачи комплексной системы защиты информации /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л2.3Л3.2 Э2	0	
2.2	Определения состава защищаемой информации /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.6Л3.2	0	
2.3	Разработка модели КСЗИ /Пр/	7	6	ОПК-9.3. ОПК-9.2.	Л1.6Л3.2	0	
2.4	Определение состава носителей защищаемой информации /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.5 Л1.6Л2.2Л3.3	0	
2.5	Выявление способов воздействия на информацию /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.5 Л1.6Л3.3	2	работа в малых группах
2.6	Определение компонентов комплексной системы защиты информации в распределенных информационных системах /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.5 Л1.6Л2.2Л3.2	0	
2.7	Сбор, обработка и изучение информации, необходимой для планирования ЦОД /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.2 Л1.6Л2.3Л3.2	0	
2.8	Анализ и использование результатов проведения контрольных мероприятий функционирования ЦОД /Пр/	7	4	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.6Л3.2	2	дискуссии

	Раздел 3. Лабораторные работы						
3.1	Файловые подсистемы Linux /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.4 Л1.6Л2.1Л3.1	0	
3.2	Обеспечение целостности и доступности данных /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.4 Л1.6Л2.1Л3.1	0	
3.3	Восстановление данных /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.4 Л1.6Л2.1Л3.1	0	
3.4	Нагрузочное тестирование веб- сервера /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л3.3	0	
3.5	DDoS - основные особенности их организации и защиты от них /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л3.3	0	
3.6	Антиспам /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л3.3	0	
3.7	Защита с помощью систем обнаружения и предотвращения вторжений (Snort) /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л3.3	0	
3.8	Получение навыков работы с SIEM /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.6Л3.3	0	
	Раздел 4. Самостоятельная работа						
4.1	Подготовка к лекциям /Ср/	7	4	ОПК-9.3. ОПК-9.2.	Л1.3 Л1.6Л2.2 Л2.3 Э1 Э2	0	
4.2	Работа с литературными и интернет-источниками /Ср/	7	6	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.2 Л2.3	0	
4.3	Подготовка к лабораторным занятиям /Ср/	7	6	ОПК-9.3. ОПК-9.2.	Л1.2 Л1.6Л2.2 Л2.3Л3.1 Л3.3	0	
4.4	Подготовка к практическим работам /Ср/	7	8	ОПК-9.3. ОПК-9.2.	Л1.6Л2.2 Л2.3Л3.1 Л3.3	0	
4.5	Выполнение РГР /Ср/	7	8	ОПК-9.3. ОПК-9.2.	Л1.6Л2.2 Л2.3Л3.1 Л3.3	0	
	Раздел 5. Контроль						
5.1	Подготовка к экзамену /Экзамен/	7	36	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.2 Л2.3	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	Сергеева Ю. С.	Защита информации: Конспект лекций	Москва: А-Приор, 2011, http://biblioclub.ru/index.php?page=book&id=72670
Л1.2	Спицын В. Г.	Информационная безопасность вычислительной техники	Томск: Эль Контент, 2011, http://biblioclub.ru/index.php?page=book&id=208694

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Артемов А. В.	Информационная безопасность	Орел: МАБИВ, 2014, http://biblioclub.ru/index.php?page=book&id=428605
Л1.4	Бражук А. И.	Сетевые средства Linux	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=428794
Л1.5	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
Л1.6	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Бэндл Д.	Защита и безопасность в сетях LINUX	Санкт-Петербург: Питер, 2002,
Л2.2	Некраха А.В., Шевцова Г.А.	Организация конфиденциального делопроизводства и защита информации: учеб. пособие для вузов	Москва: Академ. проект, 2007,
Л2.3	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

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Гончарук С. В.	Администрирование ОС Linux	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=429014
Л3.2	Петренко В.И., Мандрица И.В.	Защита персональных данных в информационных системах. Практикум: учеб. пособие	Санкт-Петербург: Лань, 2019,
Л3.3	Никифоров С.Н.	Методы защиты информации. Защита от внешних вторжений: учеб. пособие для вузов	Санкт-Петербург: Лань, 2020,

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

Э1	Поиск электронной учебной литературы	http://poiskknig.ru/
Э2	Все для студентов	http://www.studfiles.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 7 Pro - Операционная система, лиц. 60618367

Office Pro Plus 2007 - Пакет офисных программ, лиц.45525415

Free Conference Call (свободная лицензия)

Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

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

Аудитория	Назначение	Оснащение

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
108	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестаци, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-4670 CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23", проектор, экран для проектора
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
104/1	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23", доска
104/2	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23"

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

С целью эффективной организации учебного процесса студентам в начале семестра представляется учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе. В процессе обучения студенты должны, в соответствии с планом выполнения самостоятельных работ, изучать теоретические материалы по предстоящему занятию и формулировать вопросы, вызывающие у них затруднения для рассмотрения на лекционных или лабораторных занятиях. При выполнении самостоятельной работы необходимо руководствоваться литературой, предусмотренной рабочей программой и указанной преподавателем.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, практические занятия, самостоятельная работа.

Самостоятельная работа – изучение студентами теоретического материала, подготовка к лекциям, лабораторным работам, оформление конспектов лекций, выполнение РГР, написание рефератов, отчетов, работа в электронной образовательной среде и др. для приобретения новых теоретических и фактических знаний, теоретических и практических умений.

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов университета: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в Интернет; аудитории для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы.

Лабораторная работа является средством связи теоретического и практического обучения. Дидактической целью лабораторной работы является выработка умений решать практические задачи по обработке информации. Одновременно формируются профессиональные навыки владения методами и средствами обработки информации, в том числе графической.

При подготовке к лабораторным работам необходимо изучить рекомендованную учебную литературу, изучить указания к практическим работам, составленные преподавателем.

Лабораторные работы проводятся в компьютерных классах, на компьютерах которых установлено соответствующее программное обеспечение, позволяющее решать поставленные задачи обработки мультимедийной информации.

При подготовке к экзамену 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 экзамену.
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 экзамена.

Тема РГР: Защита информации в центрах обработки данных.
Вопросы:
1) Установка, настройка, разграничение прав доступа в ОС Linux.
2) Особенности ролевой модели доступа.
3) Виды атак и классы атак соответствующих уровням модели ISO OSI.
4) Межсетевые экраны. Приобретение навыков работы с Iptables и WAF.

Отчет должен соответствовать следующим требованиям:
1. Отчет результатов РГР 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 на РГР, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем РГР работы должен быть – 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.

Оформление и защита работ 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».