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 **Технологии и средства обеспечения информационной безопасности**

10.04.01 Информационная безопасность

Составитель(и): доцент, Никитин В.Н.

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 Технологии и средства обеспечения информационной безопасности

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1455

Квалификация **магистр**

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 76
самостоятельная работа 32

Виды контроля в семестрах:
зачёты с оценкой 2
РГР 2 сем. (1)

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семест р на курсе>)	**2 (1.2)**		Итого	
Недель	12 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	48	48	48	48
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
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации и технологиям защиты информации, принципы работы и устройства технических средств защиты информации. Требования, предъявляемые к процессам защите информации в современных ГИС, МИС, КИИ. Принципы выбора средств и технологий защиты при организации системы информационной безопасности. Классификация технологий обеспечения ИБ: обнаружения вторжений, защиты от НСД, антивирусное программное обеспечение, проактивной защиты инфор-мации в корпоративных системах, аудита информационной безопасно-сти. Проблемы развития технологий обеспечения безопасности. Техно-логии разработки документов при создании системы информационной безопасности (политик, концепций, планов, описаний, технических заданий и процедур).

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.В.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Компьютерные, сетевые и информационные технологии
2.1.2	Современные технологии и методы разработки и реализации программных проектов
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика
2.2.2	Информационные WEB-системы и их безопасность

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-2: Способен применять знания в области технологий и методов защиты информации при моделировании, разработке и документации систем защиты информации в автоматизированных системах
Знать:
технологии и методы обеспечения информационной безопасности; методы анализа и синтеза информационных систем при моделировании; разработку документации систем защиты информации в автоматизированных системах
Уметь:
технологии и методы обеспечения информационной безопасности; моделировать системы и разрабатывать документацию защиты автоматизиро-ванных систем
Владеть:
технологиями и методами обеспечения информационной безопасности; моделировать системы и разрабатывать документацию защиты 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	Требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации и технологиям защиты информации, принципы работы и устройства технических средств защиты информации. /Лек/	2	2	ПК-2	Л1.8Л2.3 Л2.5 Э1 Э2 Э3	0	
1.2	Требования, предъявляемые к процессам защите информации в современных ГИС, МИС, КИИ.	2	2	ПК-2	Л1.7Л2.2 Э1 Э2	0	визуализация
1.3	Принципы выбора средств и технологий защиты при организации системы информационной безопасности. /Лек/	2	4	ПК-2	Л1.1Л2.5 Э1 Э2 Э3	0	визуализация

1.4	Классификация технологий обеспечения ИБ: обнаружения вторжений, защиты от НСД, антивирусное программное обеспечение, проактивной защиты информации в корпоративных системах, аудита информационной безопасности. /Лек/	2	6	ПК-2	Л1.2 Э1 Э2 Э3	0	
1.5	Проблемы развития технологий обеспечения безопасности. Технологии разработки документов при создании системы информационной безопасности (политик, концепций, планов, описаний, технических заданий и процедур). /Лек/	2	2	ПК-2	Л1.3Л3.1 Э1 Э2 Э3	0	
	Раздел 2. Практические работы						
2.1	Защита операционных систем /Пр/	2	4	ПК-2	Л2.1 Л2.6 Э1 Э2 Э3	0	
2.2	Защита от программных закладок. Политика безопасности. /Пр/	2	4	ПК-2	Л1.8 Э1 Э2 Э3	1	работа в группах
2.3	Автоматизация процесса обработки конфиденциальной Информации. /Пр/	2	4	ПК-2	Л1.4Л2.4 Э1 Э2 Э3	1	работа в группах
2.4	Безопасное взаимодействие в компьютерных системах /Пр/	2	4	ПК-2	Л1.9 Э1 Э2 Э3	1	работа в группах
2.5	Безопасное взаимодействие в компьютерных системах /Пр/	2	2	ПК-2	Л1.4Л2.6 Э1 Э2 Э3	1	работа в группах
2.6	Механизмы управления доступом и защиты ресурсов. /Пр/	2	2	ПК-2	Л3.1 Э3	1	работа в группах
2.7	Механизм полномочного управления доступом. /Пр/	2	4	ПК-2	Л3.1 Э1 Э2 Э3	1	работа в группах
2.8	Методы обеспечения информационной безопасности компьютерных систем /Пр/	2	6	ПК-2	Л1.7 Э1 Э2 Э3	2	работа в группах
2.9	Механизм избирательного управления доступом. /Пр/	2	4	ПК-2	Л2.6 Э1 Э2 Э3	0	
2.10	Механизм контроля целостности.Контроль аппаратной конфигурации компьютера. /Пр/	2	6	ПК-2	Л1.1 Э1 Э2 Э3	0	
2.11	Порядок аттестации автоматизированных систем обработки информации. /Пр/	2	4	ПК-2	Л1.6 Э1 Э2	0	
2.12	Аппаратные средства защиты от несанкционированного входа. /Пр/	2	4	ПК-2	Л1.9 Э1 Э2 Э3	0	
	Раздел 3. Самостоятельная работа						
3.1	Подготовка к лекциям /Ср/	2	8	ПК-2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6 Л1.7 Л1.8Л2.1Л3.1	0	
3.2	Подготовка к практическим занятиям /Ср/	2	16	ПК-2	Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1Л3.1	0	
3.3	Выполнение РГР /Ср/	2	8			0	
	Раздел 3.						

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	Цилькер Б.Я., Орлов С.А.	Организация ЭВМ и систем: Учеб. для вузов	Санкт-Петербург: Питер, 2007,
Л1.2	Таненбаум Э.	Современные операционные системы	Санкт-Петербург: Питер, 2015,
Л1.3	Ситнов А. А.	Аудит информационной инфраструктуры	Москва: Евразийский открытый институт, 2011, http://biblioclub.ru/index.php?page=book&id=90796
Л1.4	Фефилов А. Д.	Методы и средства защиты информации в сетях	Москва: Лаборатория книги, 2011, http://biblioclub.ru/index.php?page=book&id=140796
Л1.5	Титов А. А.	Технические средства защиты информации	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010, http://biblioclub.ru/index.php?page=book&id=208661
Л1.6	Н.А. Свинарев	Инструментальный контроль и защита информации	Воронеж: Воронежский государственный университет инженерных технологий, 2013, http://biblioclub.ru/index.php?page=book&id=255905
Л1.7	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
Л1.8	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,
Л1.9	Ададуров С.Е.	Информационная безопасность и защита информации на железнодорожном транспорте. в 2 - ч.: Учеб.	Москва: ФГБОУ, 2014,
6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Хорев П.Б.	Методы и средства защиты информации в компьютерных системах: Учеб. пособие для вузов	Москва: Академия, 2007,
Л2.2	Лашук Н. В., Раевская П. Е.	Информационные технологии: учеб. пособие	Чита: ЗабИЖТ, 2015,
Л2.3	Голицына О.Л., Максимов Н. В., Попов И. И.	Информационные системы и технологии: учеб. пособие для вузов	Москва: Форум : Инфра-М, 2016,
Л2.4	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
Л2.5	Нестеров С. А.	Основы информационной безопасности	Санкт-Петербург: Издательство Политехнического университета, 2014, http://biblioclub.ru/index.php?page=book&id=363040
Л2.6	Аверченков В. И., Рытов М. Ю.	Организационная защита информации	Москва: Флинта, 2011, http://biblioclub.ru/index.php?page=book&id=93343
6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)			

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Крат Ю.Г.	Современные компьютерные технологии обработки информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2011,

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

Э1	ФСТЭК России	http://www.fstec.ru
Э2	ООО "Центр безопасности информации"	http://www.cbi-info.ru/
Э3	Холдинг МАСКОМ Восток	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

Windows 7 Pro - Операционная система, лиц. 60618367

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

Антивирус Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition - Антивирусная защита, контракт 469 ДВГУПС

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

Free Conference Call (свободная лицензия)

Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

1) http://www.securitycode.ru/;

2) http://fstec.ru/;

3) http://www.anti-malware.ru/news;

4) http://www.itsec.ru/forum.php.

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

Аудитория	Назначение	Оснащение
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
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
3519	Лаборатория "Защита информации в локальных вычислительных сетях"	комплект учебной мебели, система оценки защищенности технических средств от утечки информации по техническим каналам "ТАЛИС-НЧ" в специальной комплектации, система оценки защищенности технических средств от утечки информации по техническим каналам "Сигурд" специальная комплектация, автоматизированная система измерения реального затухания электрических и электромагнитных сигналов "СТЕНТОР" в расширенной комплектации
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)

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, практические занятия, самостоятельная работа.

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите сетей и систем передачи информации. В процессе изучения учебной дисциплины упор делается на изучение действующей нормативной правовой базы в области защиты сетей и систем передачи информации, системы стандартизации Российской Федерации и системы документов ФСТЭК России.
Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия с указанием отрабатываемых учебных вопросов, методических пособий по их отработке и литературы. Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала; подготовка к практическим занятиям. В ходе самостоятельной работы обучающиеся получают консультации у преподавателей.
Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программно-аппаратных средств защиты сетей и систем передачи данных, проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла практических занятий выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении практических занятий отрабатываются задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению.
Практические занятия по установке и настройке средств защиты проводятся по циклам на шести-восьми рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе). На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля, подключенное к локальной вычислительной сети.
Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями сетей передачи данных, и набором конкретных действий, существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.
Самостоятельные занятия проводятся под руководством преподавателя. Для обеспечения занятий используются автоматизированные обучающие системы, электронные учебники, виртуальные автоматизированные системы и компьютерные сети, а также программные средства имитации несанкционированных действий.

1) РГР №1: Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет
Вопросы к защите:
1. Виды угроз
2. Организационные меры защиты информации
3. Технические меры защиты информации
4. Программные меры защиты информации
5. Аппаратно-программные средства защиты информации

2)РГР №2: Использование защищенных компьютерных систем
Вопросы к защите:
1. Аппаратно-программные средства защиты информации от несанкционированного использования
2. Стандарт сетевой аутентификации IEEE 802.1x 18
3. Протоколы аутентификации
4. Комплект протоколов IP-Security (IP-Sec)

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.

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.

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.

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».