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 **Защищенные информационные системы**

10.04.01 Информационная безопасность

Составитель(и): к.т.н., Доцент, Попов М.А.

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 Защищенные информационные системы

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 **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
контактная работа 104
самостоятельная работа 40
часов на контроль 36

Виды контроля в семестрах:
экзамены (семестр) 2
зачёты (семестр) 1
курсовые проекты 2

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семест р на курсе>)	**1 (1.1)**		**2 (1.2)**		Итого	
Недель	11 4/6		12 4/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные	16	16			16	16
Практические	16	16	32	32	48	48
Контроль самостоятельной работы	4	4	4	4	8	8
Итого ауд.	48	48	48	48	96	96
Контактная работа	52	52	52	52	104	104
Сам. работа	20	20	20	20	40	40
Часы на контроль			36	36	36	36
Итого	72	72	108	108	180	180

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Угрозы информационной безопасности. Технологии и средства обес-печения информационной безопасности. Автоматизированные системы (АС).. Автоматизированные системы в защищенном исполнении (АСЗИ). Разработка АСЗИ. Средства обеспечения надежности АСЗИ. Организация технического обслуживания АСЗИ. Сертификация средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.04
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Криптографические методы защиты информации
2.1.2	Методы проектирования защищенных информационных систем
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационные WEB-системы и их безопасность
2.2.2	Тестирование и верификация информационных систем

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;
Знать:
Основы математики; физики; дискретной математики; теории вероятностей и ма-тематической стати-стики; математиче-ского анализа; надежности инфор-мационных систем для применения в профессиональной деятельности.
Уметь:
Решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных зна-ний, методов матема-тического анализа и моделирования.
Владеть:
Навыками теорети-ческого и экспери-ментального ис-следования объек-тов профессио-нальной деятель-ности.
ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;
Знать:
Современные ин-формационные тех-нологии и программ-ные средства при решении задач обще-го курса железных дорог; мультимедиа технологии, в том числе отечественного производства.
Уметь:
Выбирать современные информационные технологии и про-граммные средства при решении задач общего курса железных дорог; мультимедиа техноло-гии, в том числе отече-ственного производ-ства.
Владеть:
Навыками приме-нения современных информационных технологий и про-граммных средств при решении задач общего курса же-лезных дорог; мультимедиа тех-нологии, в том чис-ле отечественного производства.

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 сем						
1.1	Угрозы информационной безопасности. Уязвимости и угрозы информационной безопасности операционных систем, компьютерных сетей, баз данных. Компьютерные вирусы. Угрозы информационной безопасности	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	

1.2	Технологии и средства обеспечения информационной безопасности. Технологии и средства защиты информации от несанкционированного доступа. Средства защиты информации от утечки по техническим каналам. Средства криптографической защиты информации. Антивирусное программное обеспечение. Организационные меры защиты информации. /Лек/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
1.3	Автоматизированные системы (АС). Основные компоненты АС. Свойства и показатели АС. Жизненный цикл АС. /Лек/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
1.4	Автоматизированные системы в защищенном исполнении (АСЗИ). Состав системы защиты информации (СЗИ) АСЗИ. Функции СЗИ АСЗИ. Основные требования к СЗИ АСЗИ. /Лек/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 2. Лекции 2 сем						
2.1	Разработка АСЗИ. Стадии и этапы создания АСЗИ. Формирование требований к структуре АСЗИ. Разработка концепции АСЗИ. Техническое задание. Эскизный проект. Технический проект. Рабочая документация. Ввод в действие АСЗИ. Сопровождение АС. /Лек/	2	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
2.2	Средства обеспечения надежности АСЗИ. Технологии создания отказоустойчивых систем. /Лек/	2	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
2.3	Организация технического обслуживания АСЗИ. Виды технического обслуживания АСЗИ. Средства диагностирования АСЗИ. Содержание и порядок ведения эксплуатационной документации. Организация восстановления системы защиты информации и защищаемой информации после воздействия угроз. /Лек/	2	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
2.4	Сертификация средств защиты информации. Сертификация технических средств защиты информации. Сертификация криптографических средств защиты информации. Сертификация антивирусных программ. Специальные исследования СВТ на ПЭМИН. Специальные технические проверки СВТ. /Лек/	2	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 3. Лабораторные 1 сем						
3.1	Установка и настройка программных средств защиты информации /Лаб/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
3.2	Установка и настройка программно-аппаратных средств защиты информации /Лаб/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	

3.3	Установка инастройка программного комплекса для обеспечения сетевой безопасности /Лаб/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
3.4	Контроль защищенности автоматизированной системы на соответствие требованиям защиты информации /Лаб/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 4. Практические 1 сем						
4.1	Составление технического задания на создание СЗИ АС /Пр/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
4.2	Проведение инструментального контроля СЗИ НСД в рамках аттестационных испытаний АС на базе СВТ. /Пр/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
4.3	Проведение инструментального контроля комплексной СЗИ НСД в рамках аттестационных испытаний распределенных вычислительных систем. /Пр/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
4.4	Базовые методы проектирования, разработки, внедрения в эксплуатацию автоматизированных систем в защищенном исполнении /Пр/	1	4	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 5. Практические 2 сем						
5.1	Модели защиты информации /Пр/	2	10	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
5.2	Реализация системы управления доступом /Пр/	2	10	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
5.3	Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации /Пр/	2	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
5.4	«Проведение инструментального контроля комплексной СЗИ НСД в рамках аттестационных испытаний распределенных вычислительных систем» /Пр/	2	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 6. Самостоятельная работа 1 сем						
6.1	Подготовка к лекциям /Ср/	1	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
6.2	Подготовка к лабораторным и практическим занятиям /Ср/	1	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
6.3	Подготовка к зачету /Ср/	1	8	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 7. Самостоятельная работа 2 сем						
7.1	Подготовка к лекциям /Ср/	2	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	

7.2	Подготовка к лабораторным и практическим занятиям /Ср/	2	6	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
7.3	Подготовка КП /Ср/	2	8	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	0	
	Раздел 8.						
8.1	/Экзамен/	2	36	ОПК-1 ОПК -2	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2 Э3 Э4	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	Хорев П.Б.	Методы и средства защиты информации в компьютерных системах: Учеб. пособие для вузов	Москва: Академия, 2007,
Л1.2	Бутакова Н.Г., Федоров Н.В.	Криптографические методы и средства защиты информации: учеб. пособие для вузов	Санкт-Петербург: Интермедия, 2017,
Л1.3	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

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации	М.|Берлин: Директ-Медиа, 2015, http://biblioclub.ru/index.php?page=book&id=276557

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Никитин В.Н.	Проведение анализа защищённости информации в информационной системе: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2020,

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

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

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

6.3.1 Перечень программного обеспечения

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

Windows 7 Pro - Операционная система, лиц. 60618367

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

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
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная
331	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория "Защита речевой информации"	комплект учебной мебели: столы, стулья, доска, системы виброакустического зашумления "Шорох-1", "Шорох-2", "Шорох-3", "Шорох-4"; вибропреобразователи КВП-2, КВП-6, КВП-7, КВП- 8,ПЭД-5, ПЭД-6, акустический излучатель; "OMS-2000", устройство дистанционного управления "ДУ-М", зашумляющая акустическая система "Хаос-4"

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 курсового проекта (самостоятельно).
Необходимый и достаточный для успешного выполнения практической работы объем теоретического материала изложен в методических указаниях или выдается преподавателем на занятиях. При выполнении задания должны соблюдаться все требования или условия, обозначенные в условиях практических заданий.
Практическая работа считается выполненной, если студент смог продемонстрировать на лабораторном стенде – ПК с соответствующим программным обеспечением правильный результат и пояснить ход выполнения работы.
При выполнении курсового проекта студент должен руководствоваться лекционным материалом, а также обязательно использовать другие литературные источники по своему усмотрению, в частности, приведенные в РПД дисциплины.
После завершения выполнения курсового проекта слушатель допускается к защите и демонстрации приложения. Защита курсового проекта проходит в форме собеседования по вопросам, касающихся причин применения и особенностей реализации предложенных программных решений.

Текущий контроль знаний студентов осуществляется на практических занятиях в соответствии с тематикой работ путем устного опроса, а также при защите курсового проекта. Кроме этого в середине семестра проводится промежуточная аттестация студентов дневной формы обучения, согласно рейтинговой системе ДВГУПС.
Студент, своевременно выполнивший все предусмотренные программой практические работы и защитивший РГР допускается к зачету. Выходной контроль знаний слушателей осуществляется на зачете в конце семестра в форме собеседования или тестирования.

Примерный перечень тем курсовых проектов

1. Разработка технического проекта на создание системы защиты информации автоматизированной системы
2. Создание защищенной мнфраструктуры на базе заданной операционной системы с использованием выбранных программных средств защиты информации

Вопросы
1. Порядок выборам мер защиты информации.
2. Порядок выбора СЗИ.
3. Обоснование выбора мер защиты.

4. Порядок выбора организационных мер защиты информации.

Отчет должен соответствовать следующим требованиям:
1. Отчет по курсовому проекту 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 курсовой проект, рецензии, содержания, разделов, выводов и списка литературных источников. В структуру отчета может входить Приложение.
3. Объем курсового проекта должен быть – 30 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 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»