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 **Технология защиты в корпоративных сетях передачи данных**

10.05.03 Информационная безопасность автоматизированных систем

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 Технология защиты в корпоративных сетях передачи данных

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 **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
контактная работа 62
самостоятельная работа 46
часов на контроль 36

Виды контроля в семестрах:
экзамены (семестр) 7
РГР 7 сем. (1)

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	62	62	62	62
Сам. работа	46	46	46	46
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Фильтрация сетевого трафика. Обеспечение качества обслуживания сетей передачи данных. Трансляция сетевых адресов. Групповое вещание. Протокол IPv6. Виртуальные частные сети.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.36.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Виртуальные частные сети и их безопасность
2.1.2	Безопасность сетей ЭВМ
2.1.3	Основы криптографии
2.1.4	Сети и системы передачи информации
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Моделирование защищенных автоматизированных систем
2.2.2	Информационные системы на железнодорожном транспорте
2.2.3	Тестирование средств защиты информации

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 (по видам);
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 систем защиты 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 (по видам) 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 транс-порте
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 автоматизи-рованных средств контроля защи-щенности 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	Фильтрация сетевого трафика. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
1.2	Обеспечение качества обслуживания сетей передачи данных. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
1.3	Трансляция сетевых адресов. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
1.4	Групповое вещание. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	2	Проблемная лекция
1.5	Протокол IPv6. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	2	Проблемная лекция
1.6	Виртуальные частные сети. /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
1.7	Особенности проектирования систем защиты информации корпоративных тетей передачи данных /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
1.8	Основные угрозы и уязвимости, методы контроля защищенности сетей передачи данных /Лек/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
	Раздел 2. Лабораторные						
2.1	Фильтрация /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.2	Файерволы. Файерволы с функцией NAT. Программные файерволы хоста. /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	

2.3	Прокси-серверы /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.4	Типовые архитектуры сетей, защищаемых файерволами /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.5	Анализаторы протоколов. Система мониторинга NetFlow /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.6	Система обнаружения вторжений /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.7	Архитектура сети с защитой параметра и разделением внутренних зон /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
2.8	Аудит событий безопасности /Лаб/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
	Раздел 3. Практики						
3.1	Атаки на транспортную инфраструктуру сети. TCP-атаки /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
3.2	ICMP атаки /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
3.3	UDP атаки /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
3.4	IP атаки /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	2	Метод проектов

3.5	Сетевая разведка /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	2	Метод проектов
3.6	Атаки на DNS /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
3.7	Безопасность маршрутизации /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
3.8	Технологии защищенного канала /Пр/	7	2	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
	Раздел 4. Самостоятельная работа						
4.1	Подготовка к лекциям /Ср/	7	14	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
4.2	Подготовка к практическим занятиям /Ср/	7	16	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
4.3	Подготовка РГР /Ср/	7	16	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	0	
	Раздел 5.						
5.1	/Экзамен/	7	36	ОПК-9.3. ОПК-9.2.	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3	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	Олифер В.Г., Олифер Н.А.	Компьютерные сети. Принципы, технологии, протоколы: учеб. пособие для вузов	Санкт-Петербург: Питер, 2009,
Л1.2	Дибров М. В.	Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: Учебник и практикум для вузов	Москва: Юрайт, 2021, https://urait.ru/bcode/471236

	Авторы, составители	Заглавие	Издательство, год
Л1.3	Дибров М. В.	Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: Учебник и практикум для вузов	Москва: Юрайт, 2021, https://urait.ru/bcode/471908
6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Олифер В.Г., Олифер Н.А.	Сетевые операционные системы: учеб. для вузов	Санкт-Петербург: Питер, 2008,
Л2.2	Олифер В.Г., Олифер Н.А.	Основы компьютерных сетей: учеб. пособие для вузов	Санкт-Петербург: Питер, 2009,
Л2.3	Гончарук С. В.	Администрирование ОС Linux	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=429014
Л2.4	Погонин В. А., Третьяков А. А., Елизаров И. А., Назаров В. Н.	Сети и системы телекоммуникаций: учебное электронное издание: учебное пособие	Тамбов: ФГБОУ ВПО "ТГТУ", 2018, http://biblioclub.ru/index.php?page=book&id=570531
6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Кадура Е.В.	Операционные системы: метод. указания для подготовки к лаб. работам	Хабаровск: Изд-во ДВГУПС, 2018,
Л3.2	Самуйлов К. Е., Василевский В. В., Васин Н. Н., Королькова А. В., Шалимов И. А., Кулябов Д. С.	Сети и телекоммуникации: Учебник и практикум для вузов	Москва: Юрайт, 2021, https://urait.ru/bcode/469090
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)			
Э1	Лаборатория радиосистем		ttp://radiosys.ksu.ru
Э2	Информационный портал по телекоммуникационным технологиям		http://book.itep.ru
Э3	Информационные и телекоммуникационные технологии		http://kunegin.com/
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 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

Аудитория	Назначение	Оснащение
		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 дипольная активная АИ5-0 Зав. № 1742,
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)

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 работ (в аудитории), а также расчетно-графических работ (самостоятельно) в течение одного семестра.
Необходимый и достаточный для успешного выполнения 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 заданий.
Работа считается выполненной, если студент смог продемонстрировать на стенде – ПК с соответствующим программным обеспечением правильный результат и пояснить ход выполнения работы.
При выполнении РГР студент должен руководствоваться лекционным материалом, а также обязательно использовать другие литературные источники по своему усмотрению, в частности, приведенные в РПД дисциплины. В ходе выполнения каждой РГР студент на изучаемых ранее языках и технологиях программирования должен создать несколько вариантов тематического (в соответствии с заданным вариантом) приложения, реализующего предусмотренные заданием функционал.
После завершения выполнения каждой РГР слушатель допускается к защите и демонстрации приложения. Защита РГР проходит в форме собеседования по вопросам, касающихся причин применения и особенностей реализации предложенных программных решений.

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

Темы РГР.

1. Система защиты информации корпоративной сети передачи данных.

Вопросы

1. Особенности проектирования систем защиты информации корпоративных сетей передачи данных
2. Особенности эксплуатации систем защиты информации корпоративных сетей передачи данных
3. Угрозы защищенности корпоративных сетей передачи данных
4. Уязвимости защищенности корпоративных сетей передачи данных
5. Методы контроля защищенности защищенности корпоративных сетей передачи данных

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 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»
Реализация дистанционных занятий проводится в соответствии со СТ 02-02-18 "Реализация образовательных программ с использованием электронного обучения и дистанционных образовательных технологий".