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

дисциплины **Разработка и эксплуатация автоматизированных систем в защищенном исполнении**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): доцент, Никитин В.Н.

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.

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 Разработка и эксплуатация автоматизированных систем в защищенном исполнении 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 **7 ЗЕТ**

Часов по учебному плану 252
в том числе:
контактная работа 120
самостоятельная работа 96
часов на контроль 36

Виды контроля в семестрах:
экзамены (семестр) 10
зачёты (семестр) 9
курсовые работы 10

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		**10 (5.2)**		Итого	
Недель	17 1/6		18			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные	16	16	16	16	32	32
Практические	16	16	16	16	32	32
Контроль самостоятельной работы	12	12	12	12	24	24
В том числе инт.	8	8	8	8	16	16
Итого ауд.	48	48	48	48	96	96
Контактная работа	60	60	60	60	120	120
Сам. работа	48	48	48	48	96	96
Часы на контроль			36	36	36	36
Итого	108	108	144	144	252	252

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Компоненты комплексной системы информационной безопасности. Системный подход к защите информации. Методология формирования задач защиты, интеграция средств информационной безопасности в технологическую среду. Проектирование системы информационной. Основные этапы проектирования СИБ, требования к ним. Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ. Управление системой информационной безопасности. Мониторинг окружающей среды, выявление каналов несанкционированного доступа. Методика построения административного управления СИБ. Методика построения административного управления СИБ. Оценка качества системы информационной безопасности
1.2	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.31
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Организационное и правовое обеспечение информационной безопасности
2.1.2	Основы информационной безопасности
2.1.3	Управлениеинформационной безопасностью
2.1.4	Техническая защита информации и средства контроля
2.1.5	Информатика и основы программирования
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита электронного технологического документооборота
2.2.2	Информационная безопасность автоматизированных транспортных систем
2.2.3	Программно-аппаратные средства защиты информации
2.2.4	Основы программно-аппаратных средств защиты информации

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
Знать:
содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации; правовые и организационные меры защиты информации, в том числе информации ограниченного доступа, в автоматизированных системах
Уметь:
разрабатывать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах
Владеть:
способами применения действую-щуей нормативной базы в области защиты информации ограниченного доступа в автоматизированных системах
ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;
Знать:
основы диагностики и тестирования систем защиты информации автоматизированных систем; базовые методы анализа уязвимостей систем защиты информации и моделирования угроз информационной безопасности автоматизированных систем
Уметь:
проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем
Владеть:
базовыми навыками проведения диагностики и тестирования систем защиты информации автоматизированных систем

ОПК-14: Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;
Знать:
основные методы управления проектами в области информационной безопасности
Уметь:
разрабатывать, внедрять в эксплуатацию, оценивать качество автоматизированных систем; проводить подготовку исходных данных для технико-экономического обоснования про-ектных решений
Владеть:
базовыми методами проектирования, разработки, внедрения в эксплуатацию автоматизированных систем в защищенном исполнении

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. Теоретические занятия						
1.1	Компоненты комплексной системы информационной безопасности. Системный подход к защите информации. /Лек/	9	4	ОПК-13 ОПК-14 ОПК-6	Л1.7Л2.5 Э1 Э3	0	
1.2	Методология формирования задач защиты, интеграция средств информационной безопасности в технологическую среду. /Лек/	9	6	ОПК-13 ОПК-14 ОПК-6	Л1.2 Э1 Э3	0	
1.3	Проектирование системы информационной. Основные этапы проектирования СИБ, требования к ним. /Лек/	9	6	ОПК-13 ОПК-14 ОПК-6	Л1.10Л3.1 Э1 Э2 Э4	0	
1.4	Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ. Управление системой информационной безопасности. /Лек/	10	4	ОПК-13 ОПК-14 ОПК-6	Л1.10 Э1 Э3 Э4	4	визуализация
1.5	Мониторинг окружающей среды, выявление каналов несанкционированного доступа. Методика построения административного управления СИБ. /Лек/	10	6	ОПК-13 ОПК-14 ОПК-6	Л1.9 Э1 Э2 Э3 Э4	0	
1.6	Методика построения административного управления СИБ. Оценка качества системы информационной безопасности. /Лек/	10	6	ОПК-13 ОПК-14 ОПК-6	Л1.9 Э1 Э4	0	
	Раздел 2. Практические занятия						
2.1	Составление технического задания на создание СЗИ АС /Лаб/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.10Л2.4 Э3	0	
2.2	Проведение инструментального контроля СЗИ НСД в рамках аттестационных испытаний АС на базе СВТ. /Лаб/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.6Л2.5 Э1 Э2	0	
2.3	Проведение инструментального контроля комплексной СЗИ НСД в рамках аттестационных испытаний распределенных вычислительных систем. /Лаб/	10	8	ОПК-13 ОПК-14 ОПК-6	Л2.4 Э1 Э2 Э3	0	
2.4	Базовые методы проектирования, разработки, внедрения в эксплуатацию автоматизированных систем в защищенном исполнении /Лаб/	10	8	ОПК-13 ОПК-14 ОПК-6	Э1 Э4	0	

2.5	Модели защиты информации /Пр/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.10Л2.1 Э1 Э3	4	Работа в малых группах
2.6	Реализация системы управления доступом /Пр/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.11Л2.2 Э1 Э3	4	Работа в малых группах
2.7	Установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации /Пр/	10	8	ОПК-13 ОПК-14 ОПК-6	Л1.8Л2.2 Э2	4	Работа в малых групах
2.8	«Проведение инструментального контроля комплексной СЗИ НСД в рамках аттестационных испытаний распределенных вычислительных систем» /Пр/	10	8	ОПК-13 ОПК-14 ОПК-6	Э1 Э4	0	
	Раздел 3. Самостоятельная работа						
3.1	Изучение нормативно-правовых актов в области разработки защищенных информационных систем /Ср/	9	16	ОПК-13 ОПК-14 ОПК-6	Л1.4Л2.6 Э1 Э4	0	
3.2	Сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации /Ср/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.10Л2.3 Э1 Э2 Э4	0	
3.3	Методы и методики проектирования КСИБ от НСД /Ср/	9	8	ОПК-13 ОПК-14 ОПК-6	Л1.3 Э1 Э3	0	
3.4	Этапы подготовки конфиденциальных документов. Учет, изготовление и издание документов. Технология контроля исполнения документов и поручений. Порядок работы персонала с конфиденциальными документами и материалами. Обработка изданных документов. /Ср/	10	8	ОПК-13 ОПК-14 ОПК-6	Л1.5Л2.4 Э1 Э3	0	
3.5	Защита информации при проведении совещаний и переговоров. Защита информации при работе с посетителями. Защита информации в работе кадровой службы. Нормативно- методические документы по обеспечению безопасности информации. /Ср/	10	8	ОПК-13 ОПК-14 ОПК-6	Л1.1 Л1.11 Э1 Э2 Э4	0	
3.6	Словарь-справочник терминов. Основные операционные технологические схемы обработки конфиденциальных документов. /Ср/	10	8	ОПК-13 ОПК-14 ОПК-6	Л1.6Л3.1 Э3	0	
3.7	Подготовка к зачету /Ср/	9	16	ОПК-13 ОПК-14 ОПК-6	Л1.1 Л1.10Л2.2 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4	0	
3.8	Выполнение курсовой работы /Ср/	10	24	ОПК-13 ОПК-14 ОПК-6	Л1.2Л2.3 Л2.6 Э1 Э2 Э3 Э4	0	
	Раздел 4. Контроль						
4.1	Подготовка к экзамену /Экзамен/	10	36	ОПК-13 ОПК-14 ОПК-6	Л1.1 Л1.10 Л1.11Л2.1 Л2.6Л3.1 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	Березюк Л.П.	Организационное обеспечение информационной безопасности: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,
Л1.3	Таненбаум Э.	Современные операционные системы	Санкт-Петербург: Питер, 2015,
Л1.4	Киселева И. А.	Моделирование рисковых ситуаций	Москва: Евразийский открытый институт, 2011, http://biblioclub.ru/index.php?page=book&id=90413
Л1.5	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
Л1.6	Загинайлов Ю. Н.	Теория информационной безопасности и методология защиты информации	М.|Берлин: Директ-Медиа, 2015, http://biblioclub.ru/index.php?page=book&id=276557
Л1.7	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций	М.|Берлин: Директ-Медиа, 2015, http://biblioclub.ru/index.php?page=book&id=362895
Л1.8	Волкова В. Н.	Системный анализ информационных комплексов	Санкт-Петербург: Издательство Политехнического университета, 2014, http://biblioclub.ru/index.php?page=book&id=363065
Л1.9	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
Л1.10	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,
Л1.11	Советов Б.Я., Яковлев С.А.	Моделирование систем: учеб. для академ. бакалавриата	Москва: Юрайт, 2016,

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Анфилатов В. С., Емельянов А. А.	Системный анализ в управлении: Учеб. пособие для вузов	Москва: Финансы и статистика, 2002,
Л2.2		Математические основы моделирования систем	, 2006,
Л2.3	Подоба В.А., Баландина О.В.	Экономико-математические методы и модели: учеб. пособие: практикум	Хабаровск: Изд-во ДВГУПС, 2011,
Л2.4	Ю.Ю. Громов	Организация безопасной работы информационных систем	Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014, http://biblioclub.ru/index.php?page=book&id=277794

	Авторы, составители	Заглавие	Издательство, год
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	Латфуллин Г.Р., Громова О.Н.	Организационное поведение: учеб. для вузов	Санкт-Петербург: Питер, 2008,

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

Windows 7 Pro - Операционная система, лиц. 60618367
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 Гарант - http://www.garant.ru
Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru
Профессиональная база данных, информационно-справочная система Техэксперт - https://cntd.ru/

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 дипольная активная АИ5-0 Зав. № 1742, мультимедийный проектор,
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
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор

Аудитория	Назначение	Оснащение
	для самостоятельной работы	
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, лабораторные работы, практические занятия, самостоятельная работа.

Теоретическая часть материала учебной дисциплины отрабатывается на лекциях. На лекциях излагаются теоретические положения учебной дисциплины и раскрываются основы нормативного правового обеспечения технической защиты информации. В процессе изучения учебной дисциплины упор делается на изучение нормативной правовой базы в области защиты информации, системы стандартизации Российской Федерации и системы документов ФСТЭК России.
Семинарские занятия проводятся с целью углубления и закрепления знаний, привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам защиты информации, а также с целью обсуждения других, наиболее важных вопросов учебной дисциплины и контроля успеваемости обучающихся.
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 групповым и семинарским занятиям. В ходе самостоятельной работы обучающиеся получают консультации у преподавателей.
Практическая часть учебной дисциплины отрабатывается на практических занятиях. На практических занятиях развиваются умения работать с действующей нормативной правовой и методической базой в области защиты информации; работать с правовыми базами данных, базами данных, а также формируются навыки реализации в органах государственной власти и организациях требований нормативных и методических документов, а также действующего законодательства по вопросам защиты конфиденциальной информации.

Основные задачи дисциплины предусматривают предоставление знаний по вопросам:
- общие принципы проектирования АС;
- особенности построения ЗАС;
- типовая структура комплексной системы защиты информации от несанкционированного доступа;
- аттестация АС по требованиям безопасности;
- основные модели защиты информации.

Тема курсовой работы: Разработка проекта системы защиты информации в автоматизированной (информационной) системе.
Вопросы к курсовой работе "Разработка проекта системы защиты информации в автоматизированной (информационной) системе":
1. Порядок выборам мер защиты информации.
2. Порядок выбора СЗИ.
3. Обоснование выбора мер защиты.
4. Порядок выбора организационных мер защиты информации.

КР должна соответствовать следующим требованиям:
1. Пояснительная записка оформляется в текстовом редакторе MS Word на листах формата А4 (297х210).
2. 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.
3. 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.
4. Таблицы и диаграммы, созданные в MS Excel, вставляются в текст в виде динамической ссылки на источник через специальную вставку.
5. Основной текст делится на главы и параграфы. Главы нумеруются арабскими цифрами в пределах всей работы и начинаются с новой страницы.
6. Подчеркивать, переносить слова в заголовках и тексте нельзя. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.

7. 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.
8. Составление библиографического списка используемой литературы осуществляется в соответствии с ГОСТ.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу. Основное в подготовке к сдаче зачета - это повторение всего материала дисциплины, по которому необходимо сдавать зачет. При подготовке к сдаче зачета студент весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнение намеченной работы. В период подготовки к зачету студент вновь обращается к уже изученному (пройденному) учебному материалу.

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»