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 **Информационная безопасность объектов критической информационной инфраструктуры**

10.05.03 Информационная безопасность автоматизированных систем

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

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 Информационная безопасность объектов критической информационной инфраструктуры

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
контактная работа 60
самостоятельная работа 48

Виды контроля в семестрах:
экзамены (семестр) 7
РГР 7 сем. (2)

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	16	16	16	16
Контроль самостоятельной работы	12	12	12	12
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	60	60	60	60
Сам. работа	48	48	48	48
Итого	108	108	108	108

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Вопросы обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации, согласно 187-ФЗ от 26.07.2017. Объекты критической информационной инфраструктуры. Субъекты критической информационной инфраструктуры. Права и обязанности субъектов критической информационной инфраструктуры. Система безопасности значимого объекта критической информационной инфраструктуры. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации ГосСОПКА. Оценка безопасности критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов
1.2	критической информационной инфраструктуры. Ответственность за нарушение требований 187-ФЗ и принятых в соответствии с ним иных нормативных правовых актов

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.В.ДВ.02.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Управление проектами в профессиональной деятельности
2.1.2	Организационное и правовое обеспечение информационной безопасности
2.1.3	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Метрология, стандартизация и сертификация в информационной безопасности
2.2.2	Защита электронного технологического документооборота
2.2.3	Информационная безопасность автоматизированных транспортных систем
2.2.4	Информационная безопасность информационно- управляющих и информационно-логистических систем транспорта
2.2.5	Разработка и эксплуатация автоматизированных систем в защищенном исполнении

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-9.4: Разработка программных и программно-аппаратных средств для системы защиты информации автоматизированных систем
Знать:
аппаратные средства защиты технологии защиты передачи данных; процессы управления ИБ, языки программирования, методами разработки и реализации алгоритмов
Уметь:
применять способы программно-аппаратной защиты; проводить анализ системы управления информационной безопасностью автоматизированной системы
Владеть:
методами разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения

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	Этапы проектирования систем защиты информации критически важных объектов. /Лек/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
1.2	Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры. /Лек/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	

1.3	Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование предприятия. /Лек/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
1.4	Криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры объектов. /Лек/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
1.5	Составные части АИСУ, жизненный цикл АСОИУ, виды проектов АСОИУ. /Лек/	7	4	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
1.6	Технические средства контроля эффективности мер защиты информации. /Лек/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
1.7	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации ГосСОПКА. /Лек/	7	2		Л1.1Л2.5Л3.1 Э1	0	
	Раздел 2. Практики						
2.1	Определение комплекса мер для защиты информации значимых объектов критической информационной инфораструктуры /Лаб/	7	6	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
2.2	Обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры /Лаб/	7	6	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
2.3	Устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры /Лаб/	7	4	ПК-9.4	Л1.1Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Э1	0	
2.4	Изучение модели угроз информационной безопасности на предприятии /Пр/	7	4	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
2.5	Изучение локальных нормативных актов и других документов, определяющих политику и правила обеспечения информационной безопасности на предприятии /Пр/	7	4	ПК-9.4	Л1.1Л2.5Л3.1 Э1	2	Метод проектов
2.6	Методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры /Пр/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	2	Метод проектов
2.7	Методические и руководящие документы по защите информации на значимых объектах критической информационной инфраструктуры /Пр/	7	2	ПК-9.4	Л1.1Л2.5Л3.1 Э1	2	Метод проектов
2.8	Методы организации и проведения технического обслуживания средств защиты информации /Пр/	7	4	ПК-9.4	Л1.1Л2.5Л3.1 Э1	2	Метод проектов
	Раздел 3. Самостоятельная работа						
3.1	Подготовка к лекциям /Ср/	7	10	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	

3.2	подготовка к практическим /Ср/	7	11	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
3.3	подготовка к лабораторным /Ср/	7	11	ПК-9.4	Л1.1Л2.5Л3.1 Э1	0	
3.4	подготовка расчетно графической работы /Ср/	7	16	ПК-9.4	Л1.1Л2.5Л3.1 Э1	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	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: ПГТУ, 2019, http://biblioclub.ru/index.php?page=book&id=562246

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Таненбаум Э.	Современные операционные системы	Санкт-Петербург: Питер, 2015,
Л2.2	Решетникова О.В.	Администрирование информационной структуры средствами MS Windows Server : методические указания	Хабаровск : Изд-во ДВГУПС, 2011,
Л2.3	Михеев М. О.	Администрирование VMware vSphere	Москва: ДМК Пресс, 2012, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=9124
Л2.4	Матвеев М. Д.	Администрирование Windows 7. Практическое руководство и справочник администратора.	Москва: Наука и Техника, 2013, http://e.lanbook.com/books/element.php?pl1_id=39611
Л2.5	Пакин А. И.	Информационная безопасность информационных систем управления предприятием	Москва: Альтаир|МГАВТ, 2009,

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Бабаш А.В., Баранова Е.К., Мельников Ю.Н.	Информационная безопасность. Лабораторный практикум + еПриложение: Учебное пособие	Москва: КноРус, 2021, https://www.book.ru/book/936566

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

Э1	Документы по обеспечению безопасности критической информационной инфраструктуры	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury

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 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
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
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)

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 расчетно-графических работ (самостоятельно) в течение одного семестра.
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 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 практических 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 практические работы и защитивший РГР допускается к экзамену. Выходной контроль знаний слушателей осуществляется на экзамене в конце семестра в форме собеседования или тестирования.

Темы РГР1

1. Категорирование объекта КИИ

Вопросы

1. Классификация АСУТП: требования, параметры, сроки.
2. Категорирование объектов критической информационной инфраструктуры

Темы РГР2

2. Составление эксплуатационной и проектной документации

Вопросы
1. Эксплуатационная и проектная документация на информационные системы
2. Эксплуатационная и проектная документация на информационно-телекоммуникационные сети
3. Эксплуатационная и проектная документация на автоматизированные системы управления

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»