Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к910) Вычислительная техника и компьютерная графика

Фалеева Е.В., канд. тех. наук

16.06.2021

РАБОЧАЯ ПРОГРАММА

дисциплины **Защита информации**

для направления подготовки 09.03.01 Информатика и вычислительная техника

Составитель(и): к.ф.м.н., доцент, Пономарчук Ю.В.

Обсуждена на заседании кафедры: (к910) Вычислительная техника и компьютерная графика

Протокол от 16.06.2021г. № 8

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 16.06.2021 г. № 10

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 (к910) Вычислительная техника и компьютерная графика

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Фалеева Е.В., канд. тех. наук

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 (к910) Вычислительная техника и компьютерная графика

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Фалеева Е.В., канд. тех. наук

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 (к910) Вычислительная техника и компьютерная графика

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Фалеева Е.В., канд. тех. наук

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 (к910) Вычислительная техника и компьютерная графика

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Фалеева Е.В., канд. тех. наук

Рабочая программа дисциплины Защита информации

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 929

Квалификация **бакалавр**

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 68
самостоятельная работа 76
часов на контроль 36

Виды контроля в семестрах:
экзамены (семестр) 7

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	4	4	4	4
В том числе инт.	16	16	16	16
Итого ауд.	64	64	64	64
Контактная работа	68	68	68	68
Сам. работа	76	76	76	76
Часы на контроль	36	36	36	36
Итого	180	180	180	180

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Основные понятия и определения криптографии и криптологии. Источники, риски и формы атак на информацию. Политика безопасности. Стандарты безопасности. Криптографические модели. Алгоритмы симметричного и асимметричного шифрования. Алгоритмы вычисления цифровой подписи и аутентификационного кода сообщений. Алгоритмы защиты мультимедийных данных. Встраивание цифровой подписи в изображение, аудио- и видеопотоки. Визуальная криптография. Модели безопасности основных ОС. Администрирование сетей. Алгоритмы аутентификации пользователей. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Требования к системам защиты информации

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.16
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	ЭВМ и периферийные устройства
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Изучение дисциплины является завершающим этапом освоения соответствующих знаний, умений и навыков.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Знать:

Виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность.

Уметь:

Проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.

Владеть:

Методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией.

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Знать:

Принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Уметь:

Решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Владеть:

Навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Знать:

1. Действующее законодательство и правовые нормы, регулирующие профессиональную деятельность
2. Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы

Уметь:

1. Использовать нормативно-правовую документацию в сфере профессиональной деятельности
2. Применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы

Владеть:

1. Навыками работы с нормативно-правовой документацией.
2. Навыками составления технической документации на различных стадиях жизненного цикла информационной системы

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	Модуль 1 – Основные понятия защиты информации Основные понятия информационной безопасности. Свойства информации. Классификация информации по уровню доступа /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.2Л3.1 Э1 Э2	0	
1.2	Классификация уязвимостей, угроз и злоумышленников. Методы аутентификации пользователей. Защита паролей /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.2Л3.1 Э1 Э2	2	Диспуты
1.3	Модуль 2 – Основные криптографические схемы Блочный шифр DES: алгоритм, характеристики, особенности применения /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.4	Блочный шифр AES: алгоритм, характеристики, особенности применения /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.5	Модуль 3 – Основные атаки и уязвимости, управление доступом Классификация атак информационных систем изнутри. Виды вредоносного ПО, последствия атак.	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.2Л3.1 Э1 Э2	0	
1.6	Классификация вирусных программ. Антивирусные программы и антивирусная технология. Политика безопасности и механизмы защиты: домены защиты, списки управления доступом, перечни возможностей. Надежные системы /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.2Л3.1 Э1 Э2	2	Диспуты
1.7	Дискреционное и принудительное управление доступом. Модели многоуровневой защиты: Белла-Ла Падулы и Биба. Критерии безопасности. /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.2Л3.1 Э1 Э2	0	
1.8	Схемы идентификации. Применение "водяных знаков" и "отпечатков пальцев" для защиты информации. Основы визуальной криптографии /Лек/	7	4	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
	Раздел 2. Лабораторные занятия						
2.1	Криптосхемы классической криптографии: шифры сдвига, подстановки, перестановки, Виженера, Хилла, линейный шифр	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.2	ЛР 1. Криптосхемы классической криптографии: шифры сдвига, подстановки, перестановки, Виженера, Хилла, линейный шифр	7	2			0	
2.3	Потоковые шифры: с автоматическим выбором ключей, LFSR. Выдача тем рефератов /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.4	ЛР 2. Потоковые шифры: с автоматическим выбором ключей, LFSR /Лаб/	7	2			0	

2.5	ЛР 3. Криптоанализ потоковых и простейших блочных шифров /Лаб/	7	0	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.6	Программная реализация алгоритма DES /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.7	ЛР 4. Программная реализация алгоритма DES /Лаб/	7	2			2	Работа в малых группах
2.8	Программная реализация элементов алгоритма AES /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.9	ЛР 5. Программная реализация элементов алгоритма AES /Лаб/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.10	Криптосхемы асимметричной криптографии: шифры RSA и Эль-Гамаля /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.11	ЛР 6. Криптосхемы асимметричной криптографии: шифры RSA и Эль-Гамаля /Лаб/	7	2			0	
2.12	ЛР 7. Криптосистема, основаная на проблеме Диффи-Хеллмана. Вычисление кода аутентификации сообщения. Хэш-функции /Лаб/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.13	Введение в эллиптические кривые. Криптосистема Эль-Гамаля на эллиптической кривой /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	Работа в малых группах
2.14	ЛР 8. Введение в эллиптические кривые. Криптосистема Эль-Гамаля на эллиптической кривой /Лаб/	7	2			0	
2.15	Электронные цифровые подписи (ЭЦП). ЭЦП на основе эллиптической кривой (ECDSA) /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.16	ЛР 9. Электронные цифровые подписи (ЭЦП). ЭЦП на основе эллиптической кривой (ECDSA /Лаб/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.17	ЛР 10. Случайные числа в криптографии. Генераторы псевдослучайных чисел /Лаб/	7	0			0	
2.18	ЛР 11. Программная реализация алгоритмов встраивания "водяных знаков" /Лаб/	7	0			0	
2.19	Итоговое занятие /Пр/	7	2	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
	Раздел 3. Самостоятельная работа						
3.1	Изучение литературы теоретического курса /Ср/	7	20	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
3.2	Оформление и подготовка отчетов по ЛР /Ср/	7	20	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
3.3	Подготовка к лабораторным занятиям /Ср/	7	18	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
3.4	Подготовка к практическим занятиям /Ср/	7	18	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	
	Раздел 4. Контроль						
4.1	Подготовка к экзамену /Экзамен/	7	36	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	0	

4.2	/РГР/	7	0	УК-2 ОПК-3 ОПК-4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2	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	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

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,
Л2.2	Иванов М. А., Чугунков И. В.	Криптографические методы защиты информации в компьютерных системах и сетях	Москва: МИФИ, 2012, http://biblioclub.ru/index.php?page=book&id=231673

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Коломийцева С.В.	Введение в эллиптическую криптографию: метод. пособие по выполнению лабораторной работы	Хабаровск: Изд-во ДВГУПС, 2012,

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

Э1	Национальный открытый университет ИНТУИТ	http://www.intuit.ru
Э2	Microsoft Developer Network	http://msdn.microsoft.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

Windows 7 Pro - Операционная система, лиц. 60618367

Free Conference Call (свободная лицензия)

Zoom (свободная лицензия)

6.3.2 Перечень информационных справочных систем

https://elibrary.ru/

https://www.intuit.ru/

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

Аудитория	Назначение	Оснащение
420	Учебная аудитория для проведения занятий лекционного типа	Оснащенность: комплект учебной мебели, доска, переносное демонстрационное оборудование, экран.
428	Учебная аудитория для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория "Технологии виртуальной, дополненной и смешанной реальности".	Оснащенность: комплект учебной мебели, доска, экран. Технические средства обучения: компьютерная техника с возможностью подключения к сети Интернет, графическая станция, проектор, очки виртуальной реальности, очки дополненной реальности, платформа виртуальной реальности.
433	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования	компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, экран для переносного проектора, комплект учебной мебели, проектор переносной

Аудитория	Назначение	Оснащение
	(выполнения курсовых работ), а также для самостоятельной работы. Компьютерный класс.	
101	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы.	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 4Gb, int Video, 1 Tb, DVD+RW, ЖК 19"
104/1	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23", доска
104/2	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	комплект учебной мебели: столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Intel(R) Core(TM) i5-3570K CPU @ 3.40GHz, 8 Gb, 1Tb, DVD+RW, ЖК 23"

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для рационального распределения времени обучающегося по разделам дисциплины и по видам самостоятельной работы студентам предоставляется календарный план дисциплины, а также учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе.