

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, Данилова Е.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 **заочная**

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	Виды контроля на курсах:
в том числе:		экзамены (курс) 5
контактная работа	16	контрольных работ 5 курс (1)
самостоятельная работа	155	
часов на контроль	9	

Распределение часов дисциплины по семестрам (курсам)

Курс	5		Итого	
	УП	РП		
Лекции	8	8	8	8
Лабораторные	4	4	4	4
Практические	4	4	4	4
В том числе инт.	4	4	4	4
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	155	155	155	155
Часы на контроль	9	9	9	9
Итого	180	180	180	180

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Основные понятия информационной безопасности. Свойства информации.
1.2	Классификация информации по уровню доступа. Классификация
1.3	уязвимостей, угроз и злоумышленников. Методы аутентификации
1.4	пользователей. Защита паролей. Блочный шифр DES: алгоритм,
1.5	характеристики, особенности применения. Блочный шифр AES: алгоритм,
1.6	характеристики, особенности применения. Классификация атак
1.7	информационных систем изнутри. Виды вредоносного ПО, последствия атак.
1.8	Классификация вирусных программ. Антивирусные программы и
1.9	антивирусная технология. Политика безопасности и механизмы защиты:
1.10	домены защиты, списки управления доступом, перечни возможностей.
1.11	Надежные системы. Дискреционное и принудительное управление доступом.
1.12	Модели многоуровневой защиты Белла-Ла Падуды и Биба. Критерии
1.13	безопасности. Схемы идентификации. Применение «водяных знаков» и
1.14	«отпечатков пальцев» для защиты информации. Основы визуальной
1.15	криптографии

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 в области защиты информации для решения профессиональных задач; основные методы оценки разных способов решения задач по защите информации; действующее законодательство и правовые нормы в сфере информационной безопасности, 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 по защите информации 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 в сфере защиты информации.	
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:

Действующее законодательство и правовые нормы в области защиты информации, регулирующие профессиональную деятельность; основные стандарты в области информационной безопасности

Уметь:

Использовать нормативно-правовую документацию в области защиты информации в профессиональной деятельности; применять основные стандарты в области информационной безопасности

Владеть:

Навыками работы с нормативно-правовой документацией в области защиты информации в профессиональной деятельности; навыками составления технической документации на различных стадиях жизненного цикла информационной системы с использованием основных стандартов в области информационной безопасности

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	Компетенции	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/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
1.2	Классификация уязвимостей, угроз и злоумышленников. Методы аутентификации пользователей. Защита паролей /Лек/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	1	Диспуты
1.3	Модуль 2 – Основные криптографические схемы Блочный шифр DES: алгоритм, характеристики, особенности применения /Лек/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	1	Диспуты
1.4	Блочный шифр AES: алгоритм, характеристики, особенности применения /Лек/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
1.5	Модуль 3 – Основные атаки и уязвимости, управление доступом Классификация атак информационных систем изнутри. Виды вредоносного ПО, последствия атак.	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 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/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
1.7	Дискреционное и принудительное управление доступом. Модели многоуровневой защиты: Белла-Ла Падулы и Биба. Критерии безопасности. /Лек/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
1.8	Схемы идентификации. Применение "водяных знаков" и "отпечатков пальцев" для защиты информации. Основы визуальной криптографии /Лек/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
	Раздел 2. Лабораторные и практические занятия						

2.1	ЛР 1. Криптосхемы классической криптографии: шифры сдвига, подстановки, перестановки, Виженера, Хилла, линейный шифр /Лаб/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.2	ЛР 2. Поточковые шифры: с автоматическим выбором ключей, LFSR. Выдача тем КР /Лаб/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.3	ЛР 3. Криптоанализ потоковых и простейших блочных шифров /Лаб/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.4	ЛР 4. Программная реализация алгоритма DES /Лаб/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.5	ЛР 5. Программная реализация элементов алгоритма AES /Пр/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	1	Работа в малых группах
2.6	ЛР 6. Криптосхемы асимметричной криптографии: шифры RSA и Эль-Гамала /Пр/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	1	Работа в малых группах
2.7	ЛР 7. Криптосистема, основанная на проблеме Диффи-Хеллмана. Вычисление кода аутентификации сообщения. Хэш-функции /Пр/	5	0,5	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.8	ЛР 8. Введение в эллиптические кривые. Криптосистема Эль-Гамала на эллиптической кривой /Пр/	5	0,5	УК-2 ОПК-3 ОПК-4	Л1.2Л2.1Л3.1 Э1 Э2	0	
2.9	Итоговое занятие /Пр/	5	1	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
Раздел 3. Самостоятельная работа							
3.1	Изучение литературы теоретического курса /Ср/	5	30	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
3.2	Оформление и подготовка отчетов по ЛР /Ср/	5	28	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
3.3	Подготовка к лабораторным занятиям /Ср/	5	32	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
3.4	Подготовка к практическим занятиям /Ср/	5	30	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
3.5	Выполнение контрольной работы /Ср/	5	35	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 Э1 Э2	0	
Раздел 4. Контроль							
4.1	Подготовка к экзамену /Экзамен/	5	9	УК-2 ОПК-3 ОПК-4	Л1.2 Л1.1Л2.1Л3.1 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
Л1.2	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

6.1.2. 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,

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

Научная электронная библиотека <https://elibrary.ru/>

ЭИОС lk.dvfgups.ru

Справочно-правовая система Консультант Плюс <http://www.consultant.ru/>

Справочно-правовая система Кодекс <http://vuz.kodeks.ru/>

База данных POLPRED.com <http://www.neicon.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 (выполнения курсовых работ), а также для самостоятельной работы. Компьютерный	компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, экран для переносного проектора, комплект учебной мебели, проектор переносной

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.