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 **Основы криптографии**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): к.т.н., доцент, Анисимов Владимир Викторович

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 Основы криптографии

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	Виды контроля в семестрах:	
в том числе:		зачёты (семестр)	6
контактная работа	78	РГР	6 сем. (2)
самостоятельная работа	66		

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	32	32	32	32
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	8	8	8	8
Итого ауд.	64	64	64	64
Контактная работа	78	78	78	78
Сам. работа	66	66	66	66
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	История криптографии; классификация шифров; шифры замены, перестановки и гаммирования; генераторы гамм; комбинированные шифры; квантовое шифрование; шифрование с открытым ключом; основы теории чисел (простые числа; разложение числа на простые сомножители; тестирование числа на простоту); основы криптоанализа; стеганография; кодирование информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.25
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Операционные системы
2.1.2	Дискретная математика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Основы программно-аппаратных средств защиты информации

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-10: Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
Знать:
Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах и систем электронного документооборота
Уметь:
Разрабатывать и анализировать программные модели средств криптографической защиты информации
Владеть:
Навыками использования и исследования криптографических средств защиты информации, разрабатываемых различными фирмами-производителями, при решении профессиональных задач

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	Информационная безопасность и защита информации. Объекты защиты. Категории и носители информации. Средства защиты. /Лек/	6	2	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э4 Э5	0	
1.2	История криптографии. Основные термины и определения. Классификация шифров. /Лек/	6	2	ОПК-10	Л1.1 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э4 Э5	0	
1.3	Шифры замены, перестановки и гаммирования. Генераторы гамм. /Лек/	6	2	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	2	Проблемная лекция
1.4	Комбинированные шифры. ADFGX и ADFGVX. Сети Фейстеля. DES. ГОСТ 28147-89. AES. ГОСТ 34.12-2015. /Лек/	6	2	ОПК-10	Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5	0	
1.5	Шифрование с открытым ключом. RSA. Алгоритм шифрования на основе задачи об укладке ранца. Алгоритм шифрования Эль-Гамаля. Алгоритм на основе эллиптических	6	2	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	2	Проблемная лекция
1.6	Основы теории чисел. Простые числа. Разложение числа на простые сомножители. Тестирование числа на простоту. Определение НОД. Основы криптоанализа. /Лек/	6	2	ОПК-10	Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5	0	

1.7	Стеганография. /Лек/	6	2	ОПК-10	Л1.3Л2.1Л3.1 Э1 Э5	0	
1.8	Кодирование. /Лек/	6	2	ОПК-10	Л1.2Л2.1Л3.1 Э1 Э5	0	
	Раздел 2. Лабораторные работы и практические занятия						
2.1	Шифры перестановки. /Лаб/	6	4	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	0	
2.2	Шифры замены. /Лаб/	6	4	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	0	
2.3	Шифры гаммирования. /Лаб/	6	4	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	0	
2.4	Шифрование с открытым ключом. /Лаб/	6	4	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5	0	
2.5	Комбинированные шифры. /Пр/	6	12	ОПК-10	Л1.3Л2.1Л3.1 Э1 Э5	2	Занятия с применением затрудняющих условий
2.6	Стеганография. /Пр/	6	10	ОПК-10	Л1.3Л3.1Л3.2 Э1 Э5	2	Занятия с применением затрудняющих условий
2.7	Кодирование. /Пр/	6	10	ОПК-10	Л1.3Л2.1Л3.1 Э1 Э5	0	
	Раздел 3. Самостоятельная работа						
3.1	Работа с лекционным материалом /Ср/	6	10	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э5	0	
3.2	Подготовка к лабораторным работам /Ср/	6	8	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5	0	
3.3	Подготовка к практическим занятиям /Ср/	6	8	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5	0	
3.4	РГР 1. Стеганография /Ср/	6	8	ОПК-10	Л1.1 Л1.3Л2.1Л3.2 Л3.1 Э1 Э2 Э5	0	
3.5	РГР 2. Кодирование /Ср/	6	8	ОПК-10	Л1.1 Л1.3Л2.1Л3.2 Л3.1 Э1 Э2 Э5	0	
3.6	Работа с литературой /Ср/	6	16	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	0	

3.7	Подготовка к сдаче зачета /Ср/	6	8	ОПК-10	Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6	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	Романьков В. А.	Алгебраическая криптография: Учебное пособие	Омск: Омский государственный университет, 2013, http://biblioclub.ru/index.php?page=book&id=238045
Л1.2	Фороузан Б. А.	Математика криптографии и теория шифрования	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=428998
Л1.3	Лапонина О. Р.	Криптографические основы безопасности	Москва: Национальный Открытый Университет «ИНТУИТ», 2016, http://biblioclub.ru/index.php?page=book&id=429092

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Молдовян А.А., Молдовян Н.А.	Криптография: учебник	Санкт-Петербург: Лань, 2001,

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Долгов В.А., Анисимов В.В.	Криптографические методы защиты информации: учеб. пособие	Хабаровск: Изд-во ДВГУПС, 2008,
Л3.2	Анисимов В.В.	Криптография: Метод. указания по выполнению лаб. работ по дисц. "Информ. безопасность и защита информации"	Хабаровск: Изд-во ДВГУПС, 2004,
Л3.3	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	Электронно-библиотечная система «Университетская библиотека ONLINE»	biblioclub.ru
Э2	Галатенко, В.А. Основы информационной безопасности.	www.intuit.ru
Э3	Басалова, Г.В. Основы криптографии.	www.intuit.ru
Э4	Галатенко, В.А. Информационная безопасность: основные стандарты и спецификации.	www.intuit.ru
Э5	Учебная и научная деятельность Анисимова В.В.	sites.google.com/site/anisimovkhv
Э6	ЦИК РФ	cikrf.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

ПО DreamSpark Premium Electronic Software Delivery - Подписка на программное обеспечение компании Microsoft. В подписку входят все продукты Microsoft за исключением Office, контракт 203

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

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

Аудитория	Назначение	Оснащение
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
207	Компьютерный класс для лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	столы, стулья, мультимедийный проектор, экран, ноутбук (компьютер)
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

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

Лекции, методические и учебные пособия, задания на лабораторные, практические и расчетно-графические работы, вопросы к зачету размещены на сайте «http://sites.google.com/site/anisimovkhv».

При выполнении РГР студент должен руководствоваться лекционным материалом, а также обязательно использовать другие литературные источники по своему усмотрению, в частности, приведенные в списке литературы настоящей программы. В ходе выполнения РГР студент должен произвести обзор типовых средств в соответствии с тематикой РГР, произвести конфигурирование и тестирование отдельных их представителей. В результате требуется предоставить сводную характеристику возможностей исследованных средств. После выполнения РГР студент допускается к защите. Защита РГР проходит в форме собеседования по вопросам, касающихся особенностей применения исследованных инструментов.

Темы РГР.
РГР 1. Стеганография.
Вопросы к защите РГР:
1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Классическая стеганография.
5. Компьютерная стеганография.

РГР 2. Кодирование.
Вопросы к защите РГР:
1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Общие сведения о кодировании.
5. Общедоступные кодовые системы.
6. Представление чисел в двоичном виде.
7. Секретные кодовые системы.

Отчет по РГР 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.

Текущий контроль знаний студентов осуществляется на лабораторных и практических занятиях в соответствии с тематикой работ путем устного опроса. Кроме этого в середине семестра проводится промежуточная аттестация студентов дневной формы обучения, согласно рейтинговой системе ДВГУПС. Контроль усвоения лекционного материала производится проверкой преподавателем конспектов.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу. 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.

Технология организации самостоятельной работы обучающихся включает использование информационных и материально-технических ресурсов университета: библиотеку с читальным залом, укомплектованную в соответствии с существующими нормами; учебно-методическую базу учебных кабинетов, лабораторий и зала кодификации; компьютерные классы с возможностью работы в Интернет; аудитории (классы) для консультационной деятельности; учебную и учебно-методическую литературу, разработанную с учетом увеличения доли самостоятельной работы студентов, и иные методические материалы.