

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 **Криптографические методы защиты информации**

для направления подготовки 09.04.02 Информационные системы и технологии

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

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 Криптографические методы защиты информации
разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 917

Квалификация **магистр**

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 | Виды контроля в семестрах: |
| в том числе: | | экзамены (семестр) 3 |
| контактная работа | 72 | зачёты (семестр) 2 |
| самостоятельная работа | 144 | курсовые работы 3 |
| часов на контроль | 36 | РГР 2 сем. (1) |

Распределение часов дисциплины по семестрам (курсам)

| Семестр (<Курс>.<Семестр на курсе>) | 2 (1.2) | | 3 (2.1) | | Итого | |
|---|---------|-----|---------|-----|-------|-----|
| | Неделя | | 11 2/6 | | | |
| Вид занятий | УП | РП | УП | РП | УП | РП |
| Лекции | 16 | 16 | 16 | 16 | 32 | 32 |
| Практические | 16 | 16 | 16 | 16 | 32 | 32 |
| Контроль самостоятельной работы | 4 | 4 | 4 | 4 | 8 | 8 |
| В том числе инт. | 4 | 4 | 4 | 4 | 8 | 8 |
| Итого ауд. | 32 | 32 | 32 | 32 | 64 | 64 |
| Контактная работа | 36 | 36 | 36 | 36 | 72 | 72 |
| Сам. работа | 72 | 72 | 72 | 72 | 144 | 144 |
| Часы на контроль | | | 36 | 36 | 36 | 36 |
| Итого | 108 | 108 | 144 | 144 | 252 | 252 |

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

| | |
|-----|--|
| 1.1 | История криптографии; основные термины и определения; классификация шифров; шифры замены; шифры перестановки; шифры гаммирования; квантовое шифрование; комбинированные шифры; шифрование с открытым ключом; хеш-функции; криптографические протоколы; протоколы обмена ключами; протоколы аутентификации (идентификации); протоколы электронной цифровой подписи; протоколы контроля целостности; протоколы электронных платежей; протоколы голосования; протоколы тайных многосторонних вычислений и разделения секрета; некоторые сведения из теорий алгоритмов и чисел; основы криптоанализа; стеганография. |
|-----|--|

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

| | |
|-----------------|--|
| Код дисциплины: | Б1.О.10 |
| 2.1 | Требования к предварительной подготовке обучающегося: |
| 2.1.1 | Методы проектирования защищенных информационных систем |
| 2.2 | Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее: |
| 2.2.1 | Преддипломная практика |
| 2.2.2 | Безопасность операционных систем |

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

| |
|---|
| ОПК-2: Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач; |
| Знать: |
| Основные методы обработки экспериментальных данных, построения доверительных интервалов и проверки статистических гипотез и планирования научного эксперимента; построения регрессий и проверки их адекватности опытным данным; основные методы анализа временных рядов |
| Уметь: |
| Реализовывать методы и процедуры обработки данных в виде компьютерных программ; использовать специализированные пакеты прикладных программ для выполнения анализа обработки экспериментальных данных |
| Владеть: |
| Навыками реализации компьютерных программ, содержащих алгоритмы обработки данных; навыками использования современных пакетов прикладных программ для анализа данных в задачах профессиональной деятельности |

ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

| |
|---|
| Знать: |
| Современное программное и аппаратное обеспечение информационных и автоматизированных систем. |
| Уметь: |
| Разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач. |
| Владеть: |
| Навыками разработки и методами проектирования программного и аппаратного обеспечения информационных и автоматизированных систем для решения 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 | Компетенции | Литература | Инте ракт. | Примечание |
|-------------|--|----------------|-------|-------------|---|------------|------------|
| | Раздел 1. Лекции | | | | | | |
| 1.1 | Основы информационной безопасности и защиты информации /Лек/ | 2 | 1 | ОПК-5 | Л1.1 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э4 Э5 | 0 | |
| 1.2 | История криптографии /Лек/ | 2 | 1 | ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |

| | | | | | | | |
|------|--|---|---|-----------------|--|---|--|
| 1.3 | Основные термины и определения. Классификация шифров /Лек/ | 2 | 1 | ОПК-2 ОПК -5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5 | 0 | |
| 1.4 | Шифры перестановки /Лек/ | 2 | 1 | ОПК-2 ОПК -5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.5 | Шифры замены /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.6 | Шифры гаммирования /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.7 | Квантовое шифрование /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.8 | Комбинированные шифры /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л3.1 Л1.1 Л1.2 Л1.3Л2.1Л3.2 Э1 Э3 Э5 | 0 | |
| 1.9 | Шифрование с открытым ключом /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.10 | Хеш-функции /Лек/ | 2 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 1.11 | Криптографические протоколы /Лек/ | 3 | 1 | ОПК-2 ОПК -5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 1.12 | Протоколы обмена ключами /Лек/ | 3 | 1 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 1.13 | Протоколы аутентификации (идентификации) /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 1.14 | Протоколы электронной цифровой подписи /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.1 Л3.3 Э1 Э3 Э5 | 0 | |
| 1.15 | Протоколы контроля целостности /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э2 Э3 Э5 | 0 | |
| 1.16 | Протоколы электронных платежей /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 1.17 | Протоколы голосования /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 Э6 | 0 | |
| 1.18 | Протоколы тайных многосторонних вычислений и разделения секрета /Лек/ | 3 | 2 | ОПК-2 ОПК -5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |

| | | | | | | | |
|---|---|---|----|-------------|--|---|----------|
| 1.19 | Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа /Лек/ | 3 | 1 | ОПК-2 ОПК-5 | Л1.1 Л1.2Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 1.20 | Стеганография /Лек/ | 3 | 1 | ОПК-2 ОПК-5 | Л1.3Л2.1Л3.2 Э1 Э2 Э5 | 0 | |
| Раздел 2. Лабораторные работы и практические занятия | | | | | | | |
| 2.1 | Шифры замены. /Пр/ | 2 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 4 | Тренинги |
| 2.2 | Шифры перестановки. /Пр/ | 2 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | Тренинги |
| 2.3 | Шифры гаммирования. /Пр/ | 2 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | Тренинги |
| 2.4 | Шифрование с открытым ключом. /Пр/ | 2 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Л3.3 Э1 Э3 Э5 | 0 | Тренинги |
| 2.5 | Комбинированный блочный шифр DES. /Пр/ | 3 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 4 | Тренинги |
| 2.6 | Режим DES-ECB. /Пр/ | 3 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э3 Э5 | 0 | Тренинги |
| 2.7 | Режим DES-CBC. /Пр/ | 3 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э3 Э5 | 0 | Тренинги |
| 2.8 | Режим тройной DES. /Пр/ | 3 | 4 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э3 Э5 | 0 | Тренинги |
| Раздел 3. Самостоятельная работа | | | | | | | |
| 3.1 | Работа с лекционным материалом /Ср/ | 2 | 16 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 | 0 | |
| 3.2 | Выполнение РГР /Ср/ | 2 | 8 | ОПК-2 ОПК-5 | Л1.1 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 | 0 | |
| 3.3 | Подготовка к практическим занятиям /Ср/ | 2 | 16 | ОПК-2 ОПК-5 | Л1.1Л2.1Л3.2 Л3.1 Э1 Э5 | 0 | |
| 3.4 | Работа с литературой /Ср/ | 2 | 17 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 Э6 | 0 | |
| 3.5 | Подготовка к сдаче зачета /Ср/ | 2 | 15 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5 | 0 | |

| | | | | | | | |
|----------------------------------|---|---|----|-------------|---|---|--|
| 3.6 | Работа с лекционным материалом /Ср/ | 3 | 8 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5 | 0 | |
| 3.7 | Подготовка к практическим занятиям /Ср/ | 3 | 8 | ОПК-2 ОПК-5 | Л1.1Л2.1Л3.2 Л3.1 Э1 Э3 Э5 | 0 | |
| 3.8 | Разработка курсовой работы /Ср/ | 3 | 42 | ОПК-2 ОПК-5 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э3 Э5 | 0 | |
| 3.9 | Работа с литературой /Ср/ | 3 | 14 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э3 Э5 | 0 | |
| Раздел 4. Контроль знаний | | | | | | | |
| 4.1 | Экзамен /Экзамен/ | 3 | 36 | ОПК-2 ОПК-5 | Л1.1 Л1.2 Л1.3Л2.1Л3.2 Л3.1 Л3.3 Э1 Э2 Э3 Э4 Э5 | 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 | Лапоница 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 |
|-----------|--|---|
| 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 |
| 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)

Лекции, методические и учебные пособия, задания на лабораторные, практические и расчетно-графические работы, вопросы к зачету и экзамену 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, касающимся особенностей применения исследованных инструментов.

Тема РГР (2 семестр).

РГР 1. Электронная цифровая подпись.

Вопросы к защите РГР:

1. Алгоритм шифрования RSA.
2. Алгоритм шифрования Эль-Гамала.
3. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
4. Алгоритм шифрования на основе эллиптических кривых.
5. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.

6. ЭЦП на базе алгоритма RSA.
7. Алгоритм цифровой подписи ГОСТ 34.10-94.
8. Алгоритм цифровой подписи ГОСТ 34.10-2001.
9. Простые числа.
10. Разложение числа на простые множители.

Отчет по РГР должен соответствовать следующим требованиям:

1. Отчет результатов РГР оформляется в текстовом редакторе MS Word на листах формата А4 (297x210).
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.

При выполнении курсовой работы 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 курсовой работы студент должен произвести обзор типовых средств в соответствии с тематикой курсовой работы, произвести конфигурирование и тестирование отдельных их представителей. В результате требуется предоставить сводную характеристику возможностей исследованных средств. После выполнения курсовой работы студент допускается к защите. Защита курсовой работы проходит в форме собеседования по вопросам, касающимся особенностей применения исследованных инструментов.

Тема курсовой работы - Разработка криптографической программы (стандарт DES).

Вопросы к защите курсовой работы.

1. Криптография. Основные термины и определения.
2. Классификация криптографических систем.
3. Схема режима шифрования DES-ECB.
4. Схема режима шифрования DES-CBC.
5. Схема режима шифрования DES-CPB и DES-OFB.
6. Тройной DES.
7. Сферы применения различных режимов DES.

Курсовая работа должна соответствовать следующим требованиям:

1. Пояснительная записка оформляется в текстовом редакторе MS Word на листах формата А4 (297x210).
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.

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».

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.

Текущий контроль знаний студентов осуществляется на лабораторных и практических занятиях в соответствии с тематикой работ путем устного опроса, а также при защите РГР и курсовой работы. 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/экзамену необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу. При подготовке к сдаче зачета/экзамена студент весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету/экзамену, контролировать каждый день выполнение намеченной работы. В период подготовки к зачету/экзамену студент вновь обращается к уже изученному (пройденному) учебному материалу. о