# Рабочая программа дисциплины (модуля)*

Методы и средства криптографической защиты информации

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2023

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2023 г.

# Содержание

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины являются:

– приобретение студентами умения самостоятельно изучать новые алгоритмы и методы в криптографии;

– приобретение студентами умения формулировать задачи по криптографическим методам защиты информации;

– приобретение студентами умения самостоятельно оценивать надежность криптографических методов.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК-10.1 Знает основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты.

ОПК-10.2 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов.

ОПК-10.3 Владеет навыками использования типовых криптографических алгоритмов.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

| Цикл (раздел) ОПОП: | Б1.О.24 |
|---|---|

**2.1 Требования к предварительной подготовке обучающегося:**

Алгебра

Теория информации

Теория вероятностей и математическая статистика

Теоретико-числовые методы в криптографии

Дискретная математика

**2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

Криптографические протоколы

## 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;**

**Знать:**

– основные понятия и классификацию средств криптографической защиты информации;
– различия между стеганографией и криптографией;
– основные методы симметричного шифрования;
– классификацию методов симметричного шифрования;
– основные свойства симметричных криптосистем;
– понятие хеш-функции;
– основные понятия, основные алгоритмы электронной цифровой подписи;
– основные стандарты на алгоритмы цифровой подписи;
– основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.

**Уметь:**

– использовать блочные алгоритмы шифрования для формирования хеш-функции;
– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;
– использовать односторонние функции в целях построения криптосистем;
– использовать алгоритмы генерации, хранения и распределения ключей;
– проектировать и использовать системы электронной цифровой подписи;
– применять на практике алгоритмы управления открытыми ключами.

**Владеть:**

– основными методами симметричного шифрования; алгоритмами формирования хеш-функций;
– инструментами обеспечения безопасной работы в сети Интернет;

– методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом;
– технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.

**В результате освоения дисциплины обучающийся должен**

| | |
|---|---|
| **3.1** | **Знать:** |
| 3.1.1 | – основные понятия и классификацию средств криптографической защиты информации; |
| 3.1.2 | – основные методы симметричного шифрования; |
| 3.1.3 | – понятие хеш-функции; |
| 3.1.4 | – основные понятия, алгоритмы электронной цифровой подписи; |
| 3.1.5 | – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. |
| **3.2** | **Уметь:** |
| 3.2.1 | – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; |
| 3.2.2 | – использовать блочные алгоритмы шифрования для формирования хеш-функции; |
| 3.2.3 | – использовать односторонние функции в целях построения криптосистем; |
| 3.2.4 | – использовать алгоритмы генерации, хранения и распределения ключей; |
| 3.2.5 | – проектировать и использовать системы электронной цифровой подписи; |
| 3.2.6 | – применять на практике алгоритмы управления открытыми ключами. |
| **3.3** | **Владеть:** |
| 3.3.1 | – навыками симметричного шифрования; формирования хеш-функций; |
| 3.3.2 | – навыками обеспечения безопасной работы в сети Интернет; |
| 3.3.3 | – навыками применения асимметричных криптосистем; управления ключами в системах с открытым ключом; |
| 3.3.4 | – навыками по созданию электронной цифровой подписи, по обеспечению безопасной работы в сети Интернет. |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

| | |
|---|---|
| Общая трудоемкость | **7 ЗЕТ** |
| Часов по учебному плану : 252<br>в том числе :<br>аудиторные занятия : 100<br>самостоятельная работа : 110,7<br>часов на контроль : 27<br>контактная работа: 114,3<br>ИКР: 14,3 | Виды контроля в семестрах:<br><br>экзамены 8<br>зачеты 7 |

## 5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр / Курс | Часов | Литература |
|---|---|---|---|---|
| | **Раздел 1. Криптографические методы защиты информации: история криптографии; виды информации, подлежащие закрытию, их модели и свойства; Математические модели шифров и открытых текстов.** | | | |
| 1.1 | История вопроса. Математические модели шифров и открытых текстов. /Лек/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.2 | Шифры простой замены и перестановочные шифры. Решение задач. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.3 | Блочные системы шифрования. Решение задач.<br>Поточные системы шифрования. Решение задач. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.4 | Генераторы псевдослучайных последовательностей. Тесты на псевдослучайность. Решение задач /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

| | | | | |
|---|---|---|---|---|
| 1.5 | Криптоанализ блочных шифров. Решение задач /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 1.6 | Криптографические методы защиты информации /Ср/ | 7 | 16 | Л1.1 Л1.2Л2.1 Л2.2 |
| | **Раздел 2. Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Дисковые многоалфавитные шифры замены. Шифры гаммирования. Криптоанализ шифра Виженера.** | | | |
| 2.1 | Шифры замены. Шифры простой замены. Криптоанализ шифра простой замены. Полиграммное шифрование /Лек/ | 7 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.2 | Шифры подстановки. Полиалфавитное подстановочное шифрование. Криптоанализ шифра гаммирования /Лек/ | 7 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.3 | Математические основы криптографии. Решение задач. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.4 | Библиотека GMP. Алгоритм Диффи-Хеллмана. Решение задач. Программная реализация. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.5 | Криптосистема RSA. Решение задач. Программная реализация. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.6 | Криптографические хеш-функции. Решение задач. Программная реализация. /Пр/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 2.7 | Шифры простой замены и перестановки. Поточные и блочные шифры простой замены. Дисковые многоалфавитные шифры замены. Шифры гаммирования. Криптоанализ шифра Виженера. /Ср/ | 7 | 15 | Л1.1 Л1.2Л2.1 Л2.2 |
| | **Раздел 3. Криптографическая стойкость шифров: основные требования к шифрам. Совершенные шифры; теоретико-информационный подход к оценке криптостойкости шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров. Энтропия и избыточность языка. Расстояние единственности.** | | | |
| 3.1 | Криптографическая стойкость шифров. Энтропия и избыточность языка. Расстояние единственности.Совершенные шифры /Лек/ | 7 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 3.2 | Криптографическая стойкость шифров: основные требования к шифрам. /Ср/ | 7 | 15 | Л1.1 Л1.2Л2.1 Л2.2 |
| | **Раздел 4. Блочные системы шифрования. Стандарты шифрования ГОСТ 28147-89 и DES. Анализ алгоритмов блочного шифрования. Поточные системы шифрования. Синхронизация поточных шифрсистем. Примеры поточных шифрсистем. Линейные регистры сдвига. Методы анализа поточных шифрсистем.** | | | |
| 4.1 | Блочные системы шифрования. Преобразование Фейстеля. Алгоритм шифрования DES Стандарты шифрования ГОСТ 28147-89. Режимы использования блочных шифров. /Лек/ | 7 | 6 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 4.2 | Поточное шифрование. Линейные рекуррентные генераторы. Усложнение линейных рекуррентных последовательностей /Лек/ | 7 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 4.3 | Поточное шифрование. Алгоритм А5 шифрования кодированной речи. /Лек/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 4.4 | Блочные системы шифрования. Криптоанализ блочных шифров /Ср/ | 7 | 12 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | **Раздел 5. Алгоритмы классификации псевдослучайных последовательностей. Криптостойкие генераторы на основе односторонних функций. Тестирование псевдослучайных последовательностей.** | | | |
| 5.1 | Генераторы псевдослучайных последовательностей. Криптостойкие генераторы на основе односторонних функций /Лек/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

| | | | | |
|---|---|---|---|---|
| 5.2 | Тестирование псевдослучайных последовательностей. Универсальный алгоритм тестирования. Тесты на основе приращения энтропии, на основе алгоритма сжатия Лемпеля – Зива и др. /Лек/ | 7 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 5.3 | Алгоритмы построения и тестирования псевдослучайных последовательностей /Ср/ | 7 | 15,9 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | **Раздел 6. Криптоанализ блочных шифров. Линейный криптоанализ. Шифр SPN. Дифференциальный криптоанализ.** | | | |
| 6.1 | Криптоанализ блочных шифров. Линейный криптоанализ. Разностный криптоанализ. /Лек/ | 7 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 6.2 | Криптоанализ блочных шифров. Линейный криптоанализ. Разностный криптоанализ. /Ср/ | 7 | 15 | Л1.1 Л1.2Л2.1 Л2.2 |
| | **Раздел 7. Зачет** | | | |
| 7.1 | Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/ | 7 | 5,1 | |
| | **Раздел 8. Асимметричные системы шифрования. Алгоритмы Диффи-Хеллмана. Шифрсистемы RSA, Эль-Гамаля, Мак-Элиса, Рабина. Криптоанализ асимметричных систем шифрования. Алгоритмы факторизации и дискретного логарифмирования.** | | | |
| 8.1 | Вводная лекция.<br>Задачи криптографии. Этапы развития криптографии. Зарождение асимметричной криптографии. Модели симметричных и асимметричных шифров. Задачи асимметричной криптографии. /Лек/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.2 | Алгебраические основы.<br>Группы. Нормальные подгруппы. Гомоморфизмы групп. Факторгруппы. Кольца. Идеалы. Факторкольца. Поля. /Лек/ | 8 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.3 | Теоретико-числовые основы.<br>Вычеты. Системы вычетов. Теорема Эйлера. Малая теорема Ферма. Квадратичные вычеты. Символ Лежандра. Символ Якоби. Простые числа. Тесты на простоту. Китайская теорема об остатках. /Лек/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.4 | Алгоритм Диффи-Хеллмана.<br>Задача Диффи-Хеллмана. Задача дискретного логарифмирования. Атаки на алгоритм. Параметры алгоритма.<br>/Лек/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.5 | Криптосистема RSA.<br>Описание системы. Взаимосвязь параметров системы. Атаки на RSA. Алгоритмы факторизации. Выбор параметров системы. /Лек/ | 8 | 6 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.6 | Асимметричные криптосистемы.<br>Криптосистема Голдвассера-Микали. Рюкзачный метод шифрования.<br>Криптосистема Эль-Гамаля.<br>Криптосистема Рабина. Криптосистема Мак-Элиса.<br>/Лек/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.7 | Методы дискретного логарифмирования..<br>Метод Полига-Хеллмана. Метод больших и малых шагов. р-метод Полларда. Индекс метод. /Лек/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.8 | Математические основы криптографии. Решение задач. /Пр/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.9 | Библиотека GMP. Алгоритм Диффи-Хеллмана Решение задач. Программная реализация. /Пр/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.10 | Реализация алгоритма Диффи-Хеллмана.<br>Решение задач. Программная реализация.<br>/Пр/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 8.11 | Криптоанализ системы RSA.<br>Решение задач. Программная реализация. /Пр/ | 8 | 2 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |

| | | | | |
|---|---|---|---|---|
| 8.12 | Алгоритмы асимметричной криптографии. /Ср/ | 8 | 7 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | **Раздел 9. Криптографические хеш-функции. Требования. Назначение. Схемы построения. Стандарты. Криптоанализ.** | | | |
| 9.1 | Криптографические хеш-функции.<br>Определение. Требования. Назначение. Блочно-итерационная схема. Функция губки. Стандарты. Криптоанализ. /Лек/ | 8 | 6 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 9.2 | Криптографические хеш-функции.<br>Решение задач. Программная реализация. /Пр/ | 8 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 9.3 | Хеш-функции. /Ср/ | 8 | 7 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | **Раздел 10. Электронная цифровая подпись. Модель ЭЦП. Задачи ЭЦП. Алгоритмы и стандарты ЭЦП.** | | | |
| 10.1 | Электронная цифровая подпись.<br>Модель ЭЦП. Задачи ЭЦП. Схема Диффи-Лампорта. Вероятностная схема Рабина. Схема Эль-Гамаля. DSA. ГОСТ Р 34.10-94. Схема Онга -Шнорра-Шамира. Схема Шнорра. Схема Фиата-Шамира. Схемы с восстановлением сообщения. /Лек/ | 8 | 8 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 10.2 | Электронная цифровая подпись.<br>Решение задач. Программная реализация. /Пр/ | 8 | 4 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 10.3 | Электронная цифровая подпись /Ср/ | 8 | 7,8 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| | **Раздел 11. Экзамен** | | | |
| 11.1 | /Экзамен/ | 8 | 27 | Л1.1 Л1.2Л2.1 Л2.2 Л2.3 |
| 11.2 | Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/ | 8 | 9,2 | |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Перечень видов оценочных средств

Проверочная работа.
Перечень вопросов к экзамену.
Перечень вопросов к зачету.

### 6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для проверочных работы
1. Формальные модели шифров, включая шифр простой замены и шифр перестановки.
2. Математические модели открытых текстов.
3. Шифры простой замены.
4. Блоковые шифры простой замены.
5. Шифры гаммирования.
6. Надежность шифров.
7. Сеть Фейстеля.
8. Поточные системы шифрования:
9. Методы криптоанализа симметричных криптосистем.
10. Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования. Атаки.
11. Криптосистема RSA (шифрование, расшифрование, корректность). Задача RSA.
12. Атаки на RSA.
13. Алгоритмы факторизации.
14. Выбор параметров криптосистемы RSA. Генерация сильно простых чисел методом Гордона. Использование китайской теоремы об остатках в RSA.
15. Криптосистемы с открытым ключом.
16. Алгоритмы дискретного логарифмирования:
17. Хеш-функции. Требования. Предназначение.
18. Стандарты хеш-функций.
19. Общая схема алгоритмов MD4, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
20. Криптоанализ хеш-функций.

21. Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
22. Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
23. Схема ЭЦП Эль-Гамаля. Уменьшение размера подписи в схеме Эль-Гамаля.

**6.3. Типовые контрольные вопросы и задания для промежуточной аттестации**

Вопросы к зачету (7 семестр)
Основные понятия:
1. Формальные модели шифров, включая шифр простой замены и шифр перестановки.
2. Математические модели открытых текстов.
Шифры простой замены:
1. Аффинный шифр простой замены;
2. Криптоанализ поточного шифра простой замены.
Блоковые шифры простой замены:
1. Шифр Плейфера;
2. Шифр Хилла.
Шифры гаммирования:
1. Шифр модульного гаммирования Виженера;
2. Шифр Вернама.
Надежность шифров:
1. Энтропия H языка . Избыточность языка R;
2. Неопределенность шифра по ключу H(K|Y ), неопределенность шифра по открытому тексту H(X|Y ). Формула Шеннона для неопределенности шифра по ключу;
3. Расстояние единственности;
4. Совершенные шифры, теорема Шеннона о совершенном шифре.
Стандарты шифрования:
1. Сеть Фейстеля;
2. Алгоритмы шифрования DES, ГОСТ 28147 - 89.
Поточные системы шифрования:
1. Принципы построения поточных шифросистем;
2. Статистическое тестирование псевдослучайных последовательностей: тест 2-серий, тест на основе приопщения энтропии, тест, основанный на алгоритме сжатия Лемпеля - Зива.
3. Псевдослучайные последовательности, линейный регистр сдвига с
обратной связью. Минимальный характеристический многочлен, линейная сложность ЛРП, период ЛРП, ЛРП максимального периода.
4. Шифросистема A5;
5. Усложнение линейных рекуррентных последовательностей;
6. Генератор ANSI X9.17, BBS - алгорит генерации псевдослучайных
последовательностей.
Методы криптоанализа симметричных криптосистем:Линейный криптоаналих Митсуру Матсуи;

Вопросы к экзамену (8 семестр)
1. Алгоритм Диффи-Хеллмана. Задача Диффи-Хеллмана. Задача дискретного логарифмирования.
Атаки:
- использование в качестве g числа малого порядка
- навязывание в качестве g^x (g^y) числа малого порядка
- при малых значениях секретных ключей x; y навязывание малых значений g^y, g^x.
Использование надежных простых чисел (safe prime). Уменьшение размера надежного простого числа.
2. Криптосистема RSA (шифрование, расшифрование, корректность). Задача RSA.
Сведение задачи RSA к другим задачам (факторизации, дискретного логарифмирования, извлечения корней). Связь параметров системы p, q, \phi(n), d (вычисление по любому из них остальных).
3. Атаки на RSA
- малое значение открытого текста;
- шифрование одного открытого текста на одинаковых малых открытых экспонентах;
- частично известный открытый текст (линейное соотношение, произвольные соотношения);
- метод повторного шифрования при малом порядке открытой экспоненты по модулю n (для расшифрования) либо по модулю p (для факторизации);
- нахождение закрытого ключа другого пользователя при использовании одного основания n;
- шифрование одного открытого текста на взаимно простых открытых экс-
понентах при использовании одного основания n;
- нахождение \phi(n) по d;

- биты сообщения – взаимосвязь p(y), h(y), D(y);
- использование одинаковых ключей для шифрования и цифровой подписи.

4. Алгоритмы факторизации:
- метод пробных делений;
- метод Ферма;
- метод больших и малых шагов;
- p - 1 – метод Полларда;
- \rho– метод Полларда;
- алгоритм Диксона.

5. Выбор параметров криптосистемы RSA. Генерация сильно простых чисел методом Гордона. Использование китайской теоремы об остатках в RSA.
6. Схема шифрования RSA-OAEP.
7. Криптосистемы с открытым ключом.
- система Голдвассера-Микали;
- рюкзачный метод шифрования Меркла Хеллмана;
- система Эль-Гамаля;
- система Рабина;
- система Мак-Элиса.

8. Алгоритмы дискретного логарифмирования:
- метод больших и малых шагов;
- \rho – метод Полларда;
- индекс метод;
- метод Полига Хеллмана.

9. Хеш-функции. Требования. Предназначение. Модель Меркле-Дамгарда. Функция губки (sponge function).
10. Стандарты хеш-функций.
11. Общая схема алгоритмов MD4, ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94.
12. Криптоанализ хеш-функций. Модель случайного оракула (ROM).

Атака на основе парадокса дней рождений:
- \rho – метод Полларда;
- § \lambda – метод Полларда.

Time-memory Trade-off:
- методХеллмана;
- радужныетаблицы.

Криптоанализ схемы Меркле-Дамгарда.
13. Электронная цифровая подпись (ЭЦП). Задачи ЭЦП.
14. Схема ЭЦП Диффи-Лампорта. Вероятностная схема ЭЦП Рабина.
15. Схема ЭЦП Эль-Гамаля. Уменьшение размера подписи в схеме Эль-Гамаля.
16. ЭЦП DSA.
17. ЭЦП ГОСТ Р 34.10-94.
18. ЭЦП Онга-Шнорра-Шамира.
19. ЭЦП Шнорра.
20. Схемы ЭЦП с восстановлением сообщений (на основе RSA, на основе ЭЦП Эль-Гамаля, ЭЦП Рабина).
21. Слепая ЭЦП Чаума (на основе RSA).

**6.4. Критерии оценивания**

Порядок проведения промежуточной аттестации
В течение каждого семестра студентам необходимо выполнить проверочные работы, которые в случае безупречного выполнения оцениваются в 25 баллов.
В рамках зачета студентам предлагается 1 вопрос, оцениваемый в 20 баллов.
В рамках экзамена студентам предлагается 2 вопроса, каждый из которых оценивается в 25 баллов.

Сводная таблица рейтинга успеваемости (7 семестр)

| № | Перечень контрольных мероприятий в семестре | Максимальное кол-во баллов |
|---|---|---|
| 1 | Проверочная работа №1,2 | 2x25=50 |
| 2 | Зачет (теоретический вопрос) | 20 |
| Итого | | 70 |

Сводная таблица рейтинга успеваемости (8 семестр)
№ Перечень контрольных мероприятий в семестре Максимальное кол-во баллов

| | |
|---|---|
| 1 Проверочная работа №1,2 | 2x25=50 |
| 2 Экзамен (теоретический вопрос) | 2x25=50 |
| Итого | 100 |

Критерии оценивания теоретического вопроса для зачета
Максимальный балл за ответ на теоретический вопрос – 20 баллов.
Отлично/зачтено/17-20 баллов - Обучающийся отлично знает материал, понимает основы симметричной криптографии. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/13-16 баллов - Обучающийся хорошо знает материал, понимает основы симметричной криптографии. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/9-12 баллов - Обучающийся знаком с материалом, владеет базовыми знаниями симметричной криптографии. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-8 баллов - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания теоретического вопроса для экзамена
Максимальный балл за ответ на теоретический вопрос – 25 баллов.
Отлично/зачтено/21-25 баллов - Обучающийся отлично знает материал, понимает основы асимметричной криптографии. Обучающийся практически не допускает ошибок.
Хорошо/зачтено/16-20 баллов - Обучающийся хорошо знает материал, понимает основы асимметричной криптографии. Обучающийся допускает незначительные ошибки.
Удовлетворительно/зачтено/11-15 баллов - Обучающийся знаком с материалом, владеет базовыми знаниями асимметричной криптографии. Обучающийся допускает фактические ошибки.
Неудовлетворительно/не зачтено/0-10 балла - Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

Критерии оценивания проверочных работы
Максимальный балл за работу – 25 баллов.
Отлично/зачтено/21-25 баллов - Проверочная работа выполнена правильно, в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.
Хорошо/зачтено/16-20 баллов - Выполнено 3/4 проверочной работы, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу, но допускает незначительные ошибки.
Удовлетворительно/зачтено/11-15 баллов - Выполнено 1/2 проверочной работы, либо работа сдана значительно позднее, чем предполагалось, при этом обучающийся знает материал, но допускает ошибки.
Неудовлетворительно/не зачтено/0-10 баллов - Работа не выполнена, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:
При подведении итогов зачета учитываются:
0 – 35 баллов – не зачтено;
36 – 70 баллов – зачтено.
При подведении итогов экзамена учитываются :
0 – 59 баллов – неудовлетворительно (2);
60 – 74 баллов – удовлетворительно (3);
75 – 90 баллов – хорошо (4);
91 – 100 баллов – отлично (5).

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 7.1. Рекомендуемая литература

#### 7.1.1. Основная литература

| | Авторы, составители | Заглавие | Издательство, год | Ресурс |
|---|---|---|---|---|

| | Авторы, составители | Заглавие | Издательство, год | Ресурс |
|---|---|---|---|---|
| Л1.1 | Фороузан Б. А. | Математика криптографии и теория шифрования: учебное пособие (https://biblioclub.ru/index.php?page=book&id=428998) | Москва : Национальный Открытый Университет «ИНТУИТ», 2016 | ЭБС |
| Л1.2 | Зубов А. Ю., Кузьмин А. С., Черемушкин А. В., Алферов А. П. | Основы криптографии: учебное пособие | Москва : Гелиос АРВ, 2002 | |

**7.1.2. Дополнительная литература**

| | Авторы, составители | Заглавие | Издательство, год | Ресурс |
|---|---|---|---|---|
| Л2.1 | Василенко О. Н. | Теоретико-числовые алгоритмы в криптографии: монография (https://biblioclub.ru/index.php?page=book&id=61814) | Москва : МЦНМО, 2006 | ЭБС |
| Л2.2 | Зубов А. Ю. | Криптографические методы защиты информации. Совершенные шифры: учебное пособие | Москва : Гелиос АРВ, 2005 | |
| Л2.3 | | Информационный мир XXI века. Криптография- основа информационной безопасности: учебно-методическая литература (https://znanium.com/catalog/document?id=353538) | Москва : Дашков и К, 2020 | ЭБС |

**7.3 Перечень информационных технологий**

**7.3.1 Программное обеспечение**

MS Office365

Adobe Reader

Octave

Notepad++

Visual Studio

**7.3.2 Профессиональные базы данных и информационно-справочные системы**

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке ]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

**8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

## 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, практические занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.
На практических занятиях решаются задачи с целью изучения криптографических систем шифрования . Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции (вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

## 10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.
1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков;

программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.
Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.
Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).
В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:
а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);
б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);
в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.
Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

**Специальность 10.05.01 Компьютерная безопасность**
**Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»**
**Рабочая программа дисциплины «Методы и средства криптографической защиты информации»**
**2023 год набора, очная форма обучения**

Проректор по учебной работе утверждено 24.04.2023 В.Е. Федоров

Ученым советом математического факультета

Протокол заседания № 8 от 13.04.2023

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

**Заседанием кафедры компьютерной безопасности и прикладной алгебры**

Протокол заседания № 10 от 31.03.2023

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

**Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1**