

|  |  |  |        |
|--|--|--|--------|
| Документ подписан простой электронной подписью<br>Информация о владельце:<br>ФИО: Таскаев Сергей Валерьевич<br>Должность: Ректор<br>Дата подписания: 04.06.2025 12:35:17<br>Уникальный программный ключ:<br>04c19ed8bf10867b6cb77a486b9a8788b8722727 | МИНОВЕР НАУКИ РОССИИ<br>Федеральное государственное бюджетное образовательное учреждение высшего образования<br>«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ») | Рабочая программа дисциплины "Дополнительные главы криптографии" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ» | стр. 1 |
|--|--|--|--------|

## **Рабочая программа дисциплины (модуля)\***

### **Дополнительные главы криптографии**

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 2025

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

Челябинск 2025 г.



## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре ОПОП
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)
4. Объем дисциплины (модуля)
5. Структура и содержание дисциплины (модуля)
6. Фонд оценочных средств
  - 6.1. Перечень видов оценочных средств
  - 6.2. Типовые контрольные задания и иные материалы для текущей аттестации
  - 6.3. Типовые контрольные вопросы и задания для промежуточной аттестации
  - 6.4. Критерии оценивания
7. Учебно-методическое и информационное обеспечение дисциплины (модуля)
  - 7.1. Рекомендуемая литература
  - 7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"
  - 7.3. Перечень информационных технологий
8. Материально-техническое обеспечение дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Специальные условия освоения дисциплины обучающимися с инвалидностью и ограниченными возможностями здоровья



### 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель: Успешное освоение дисциплины позволит студентам глубже понять и научиться анализировать механизмы защиты, применяемые в современных ассиметричных шифрах.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей.

ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП: Б1.В.ДВ.02.01

#### 2.1 Требования к предварительной подготовке обучающегося:

Методы и средства криптографической защиты информации

Криптографические протоколы

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

Данная дисциплина завершает блок математических и криптографических дисциплин, читаемых на кафедре. На базе данной дисциплины возможно выполнение студентами дипломных проектов.

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

#### ПК-3: Способен проводить анализ безопасности компьютерных систем

##### Знать:

- роль эллиптических кривых в современных ассиметричных шифрах;
- формальные требования, предъявляемые к криптографическим эллиптическим кривым.

##### Уметь:

- анализировать криптографические эллиптические кривые на предмет их защищённости;
- конструировать эллиптические кривые, обладающие заданными свойствами.

##### Владеть:

- навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых.

#### В результате освоения дисциплины обучающийся должен

##### 3.1 Знать:

- 3.1.1 – принципы криптографии на эллиптических кривых;
- 3.1.2 – понятие "группа точек эллиптической кривой" (определение операции и свойства);
- 3.1.3 – определение и примеры изоморфизмов эллиптических кривых. j-инвариант;
- 3.1.4 – следующие понятия: эндоморфизмы, степень, отделимость, точки кручения, полиномы деления;
- 3.1.5 – теорему Хассе, алгоритм Шуфа и его модификации;
- 3.1.6 – криптосистему Эль-Гамала и атаки на неё, определение цифровой подписи на эллиптической кривой, идентификацию и подпись Шнорра; безопасность подписи Шнорра; алгоритм ECDSA;
- 3.1.7 – алгоритм Полига-Хеллмана; алгоритм "Baby step-giant step"; ро-алгоритм Полларда; лямбда-алгоритм Полларда;
- 3.1.8 – гомоморфное шифрование (определение и обзор гомоморфных криптосистем).



**3.2 Уметь:**

3.2.1 – проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;

3.2.2 – формулировать и разрабатывать предложения по устранению выявленных уязвимостей.

**3.3 Владеть:**

3.3.1 – способностью участвовать в разработке и конфигурировании программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых;

3.3.2 – выполнять анализ уязвимости компьютерных систем.

3.3.3

**4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)**

| Общая трудоемкость   | З ЗЕТ                                       |
|--|---|
| Часов по учебному плану : 108<br>в том числе :<br>аудиторные занятия : 50<br>самостоятельная работа : 52,9<br>:<br>контактная работа: 55,1<br>ИКР: 5,1 | Виды контроля в семестрах:<br><br>зачеты 10 |

**5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

| Код занятия | Наименование разделов и тем /вид занятия/  | Семестр / Курс | Часов | Литература                 |
|-------------|--|----------------|-------|----------------------------|
|             | <b>Раздел 1. Основы</b>  |                |       |                            |
| 1.1         | Введение в криптографию на эллиптических кривых.<br>Что есть криптография? Что есть криптография на эллиптических кривых?<br>/Лек/   | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.2         | Вычисления на эллиптических кривых<br>Почему мы используем эллиптические кривые в криптографии? Группа точек эллиптической кривой. Эллиптические кривые в системах компьютерной алгебры SAGE и MAGMA. Curve25519, Curve448,<br>/Лек/ | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.3         | Изоморфизмы эллиптических кривых<br>Сингулярные кривые. Определение и примеры изоморфизмов. j-инвариант. Изогении. /Лек/   | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.4         | Эндоморфизмы и кручение.<br>Эндоморфизмы, степень, отделимость. Примеры: умножение на n, эндоморфизм Фробениуса. Точки кручения. Полиномы деления.<br>/Лек/  | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.5         | Практическое изучение свойств малых эллиптических кривых без использования компьютера /Пр/   | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.6         | Практическое изучения свойств эллиптических кривых с использованием систем компьютерной алгебры SAGE и MAGMA. Curve25519, Curve448.<br>/Пр/  | 10             | 2     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 1.7         | Введение в криптографию на эллиптических кривых. Вычисления на эллиптических кривых. Изоморфизмы эллиптических кривых. Эндоморфизмы и кручение. /Ср/   | 10             | 9     | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
|             | <b>Раздел 2. Эллиптические кривые над конечными полями</b>   |                |       |                            |



|   |   |    |   |                            |
|---|---|----|---|----------------------------|
| 2.1   | Размер группы точек эллиптической кривой.<br>Структура n-кручения. Символ Лежандра и подсчет точек. Теорема Хассе.<br>Эллиптические кривые над подполями. Суперсингулярные кривые.<br>Алгоритм Шуфа и его модификации.<br>/Лек/   | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 2.2   | Контрольная работа по базовым свойствам эллиптических кривых. /Пр/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 2.3   | Реализация алгоритма Шуфа вычисления порядка группы точек эллиптической кривой (допускается использование арифметики многочленов и конечных полей) /Пр/   | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 2.4   | Эллиптические кривые над конечными полями. /Ср/   | 10 | 9 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| <b>Раздел 3. Криптосистемы на эллиптических кривых</b>                              |   |    |   |                            |
| 3.1   | Определение операции шифрования на эллиптической кривой.<br>Криптосистема Эль-Гамала и атаки на неё. Определение цифровой подписи на эллиптической кривой. Идентификация и подпись Шнорра.<br>Безопасность подписи Шнорра. Алгоритм ECDSA. Алгоритм Диффи-Хеллмана обмена ключами для эллиптической кривой<br>/Лек/       | 10 | 6 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 3.2   | Реализация криптосистемы Эль-Гамала, подписи Шнорра и алгоритма ECDSA /Пр/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 3.3   | Криптосистемы на эллиптических кривых. /Ср/   | 10 | 9 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| <b>Раздел 4. Атаки, связанные с операцией дискретного логарифмирования</b>          |   |    |   |                            |
| 4.1   | Базовые алгоритмы.<br>Алгоритм Полига-Хеллмана. Алгоритм "Baby step-giant step". Ро-алгоритм Полларда. Лямбда-алгоритм Полларда. /Лек/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 4.2   | Атака Менезеса-Окамото-Ванстоуна и слабые эллиптические кривые.<br>Сопряжение Вейля и сведение задачи дискретного логарифмирования на эллиптической кривой к задаче дискретного логарифмирования в конечном поле. Атака Менезеса-Окамото-Ванстоуна (Menezes-Okamoto-Vanstone). Степень вложения. Аномальные кривые. /Лек/ | 10 | 4 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 4.3   | Реализация алгоритмов Полига-Хеллмана, "Baby step-giant step", Ро-алгоритм Полларда, Лямбда-алгоритм Полларда. /Пр/   | 10 | 4 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 4.4   | Реализация атаки Менезеса-Окамото-Ванстоуна /Пр/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 4.5   | Атаки, связанные с операцией дискретного логарифмирования /Ср/  | 10 | 9 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| <b>Раздел 5. Криптосистемы, основанные на сопряжении Вейля</b>                      |   |    |   |                            |
| 5.1   | Обмен ключами и шифрование на основе идентификации (identity-based encryption).<br>Определения шифрования на основе идентификации. Схема Боне-Франклина. /Лек/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 5.2   | Шифрование на основе идентификации и цифровая подпись.<br>Схема подписи Боне-Линна-Сакама. /Лек/  | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 5.3   | Гомоморфное шифрование<br>Частично гомоморфные и полностью гомоморфные криптосистемы.<br>Криптосистема Боне-Го-Ниссима. /Лек/   | 10 | 2 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 5.4   | Криптосистемы, основанные на сопряжении Вейля /Ср/  | 10 | 9 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| <b>Раздел 6. Вспомогательные алгоритмы для криптографии на эллиптических кривых</b> |   |    |   |                            |



|   |   |    |     |                            |
|---|---|----|-----|----------------------------|
| 6.1                                     | Вычисление сопряжений Вейля и Тейта.<br>Дивайзоры и функции. Определение сопряжений и их свойства. Алгоритм Миллера. /Лек/  | 10 | 2   | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 6.2                                     | Метод комплексного умножения для конструирования кривых.<br>Эллиптические кривые над полем комплексных чисел и комплексное умножение. Вычисление полинома гильбертова класса. /Лек/ | 10 | 2   | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 6.3                                     | Факторизация и доказательство простоты с помощью эллиптических кривых.<br>Алгоритм Ленстры для факторизации. Алгоритм Поклингтона- Лемера для доказательства простоты. /Лек/        | 10 | 2   | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| 6.4                                     | Вспомогательные алгоритмы для криптографии на эллиптических кривых /Ср/   | 10 | 7,9 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |
| <b>Раздел 7. Иная контактная работа</b> |   |    |     |                            |
| 7.1                                     | Иная контактная работа: индивидуальные консультации, текущий контроль. /ИКР/  | 10 | 5,1 | Л1.1 Л1.2 Л1.3Л2.1<br>Л2.2 |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Перечень видов оценочных средств

Контрольная работа.  
Лабораторные работы.  
Перечень вопросов к зачету.

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

Задания контрольной работы:

№ п/п Формулировка задания

- 1 Дана эллиптическая кривая  $y^2 = x^3 - x + 1$  над  $R$  и точки  $P = (0, 1)$ ,  $Q = (1, 1)$ ,  $T = (3, 5)$ , лежащие на данной кривой. Вычислить точку  $2P + 3Q - T$ .
- 2 Дана эллиптическая кривая  $y^2 = x^3 - x + 1$  над  $Z_{11}$ . Построить таблицу Кэли для группы точек этой кривой.
- 3 Дана эллиптическая кривая  $y^2 = x^3 - x + 1$  над  $Z_{13}$ . Определить какой абелевой группе изоморфна группа точек этой кривой.
- 4 Продемонстрировать на примере кривой  $y^2 = x^3 - x + 1$  над  $Z_{13}$  полный цикл генерации общего ключа по протоколу Диффи-Хеллмана для эллиптических кривых.
- 5 Продемонстрировать на примере кривой  $y^2 = x^3 - x + 1$  над  $Z_{13}$  работу алгоритма ECDSA.

Список лабораторных работ:

№ п/п Формулировка задания

- 1 Написать программу, реализующую алгоритм Шуфа.
- 2 Написать программу, реализующую алгоритмы: Полига-Хеллмана, "Baby step - giant step", Ро-алгоритм Полларда, Лямбда-алгоритм Полларда.
- 3/4 Написать программу, реализующую алгоритм ECDSA/Написать программу, реализующую криптосистему Эль- Гамала, реализовать две различные атаки на эту криптосистему.

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

Список теоретических вопросов к зачету:

№ п/п Формулировка вопроса

- 1 Что есть криптография на эллиптических кривых?
- 2 Группа точек эллиптической кривой (определение операции и свойства).
- 3 Определение и примеры изоморфизмов эллиптических кривых. j-инвариант
- 4 Эндоморфизмы, степень, отделимость. Примеры эндоморфизмов. Точки кручения. Полиномы деления.
- 5 Теорема Хассе. Алгоритм Шуфа и его модификации.
- 6 Криптосистема Эль-Гамала и атаки на неё. Определение цифровой подписи на эллиптической кривой. Идентификация и подпись Шнора. Безопасность подписи Шнора. Алгоритм ECDSA.
- 7 Алгоритм Полига-Хеллмана. Алгоритм "Baby step - giant step". Ро-алгоритм Полларда. Лямбда-алгоритм Полларда.
- 8 Гомоморфное шифрование (определение и обзор гомоморфных криптосистем).



#### 6.4. Критерии оценивания

В течение семестра студентам необходимо выполнить контрольную работу, которая в случае безупречного выполнения оценивается в 30 баллов.

Также в течение семестра выполняется три лабораторные работы, каждая из которых оценивается в 10 баллов. Кроме того, в рамках зачета студентам предлагается 2 вопроса, каждый из которых оценивается в 10 баллов.

Сводная таблица рейтинга успеваемости

№ Перечень контрольных мероприятий в семестре Максимальное кол-во баллов

|   |                              |         |    |
|---|------------------------------|---------|----|
| 1 | Контрольная работа           | 30      |    |
| 2 | Лабораторная работа №1-4     | 4x10=40 |    |
| 3 | Зачет (теоретический вопрос) | 2x10=20 |    |
|   | Итого                        |         | 90 |

Критерии оценивания теоретического вопроса зачета и лабораторной работы

Максимальный балл за ответ на теоретический вопрос и за одну лабораторную работу – 10 баллов.

Отлично/зачтено/9-10 баллов - Обучающийся отлично знает материал, умеет анализировать проблему и грамотно сформулировать доказательство.

Хорошо/зачтено/7-8 баллов - Обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.

Удовлетворительно/зачтено/5-6 баллов - Обучающийся знаком с материалом, но допускает фактические ошибки.

Неудовлетворительно/не зачтено/0-4 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 задания контрольной работы

Максимальный балл за работу – 30 баллов.

Максимальный балл за задание – 6 баллов.

Отлично/зачтено/6 баллов - Задание выполнено в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно сформулировать доказательство.

Хорошо/зачтено/4-5 балла - Задание выполнено в срок, обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.

Удовлетворительно/зачтено/3 балла - Задание выполнено и сдано позднее, чем предполагалось, либо обучающийся допускает фактические ошибки.

Неудовлетворительно/не зачтено/0-2 балла - Задание не выполнено, 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:

0 – 59 баллов – не зачтено;

60 – 90 баллов – зачтено.

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

### 7.1. Рекомендуемая литература

#### 7.1.1. Основная литература

|      | Авторы, составители  | Заглавие  | Издательство, год                       | Ресурс |
|------|--|---|---|--------|
| Л1.1 | Глухов М. М.,<br>Круглов И. А.,<br>Пичкур А. Б.,<br>Черемушкин А. В. | Введение в теоретико-числовые методы криптографии: учебное пособие для вузов  | Санкт-Петербург<br>[и др.] : Лань, 2011 |        |
| Л1.2 | Мартынов Л. М.   | Алгебра и теория чисел для криптографии: учебное пособие для вузов<br>( <a href="https://e.lanbook.com/book/362942">https://e.lanbook.com/book/362942</a> ) | Санкт-Петербург<br>: Лань, 2024         | ЭБС    |
| Л1.3 | Панкратова И. А.   | Булевы функции в криптографии: учебное пособие для вузов<br>( <a href="https://e.lanbook.com/book/440309">https://e.lanbook.com/book/440309</a> )           | Санкт-Петербург<br>: Лань, 2025         | ЭБС    |



### 7.1.2. Дополнительная литература

|      | Авторы, составители  | Заглавие   | Издательство, год   | Ресурс |
|------|--|--|---|--------|
| Л2.1 | Шубович В. Г.,<br>Капитанчук В. В.,<br>Знаенко Н. С.,<br>Титаренко Ю. И. | Разработка моделей криптографической защиты информации:<br>монография<br>( <a href="https://biblioclub.ru/index.php?page=book&amp;id=278070">https://biblioclub.ru/index.php?page=book&amp;id=278070</a> )           | Ульяновск :<br>Ульяновский<br>государственный<br>педагогический<br>университет<br>(УлГПУ), 2013 | ЭБС    |
| Л2.2 | Серр Ж. П., Манин<br>Ю. И., Цукерман Г.<br>М.                            | Абелевы L-адические представления и эллиптические кривые:<br>научная литература<br>( <a href="https://biblioclub.ru/index.php?page=book&amp;id=450346">https://biblioclub.ru/index.php?page=book&amp;id=450346</a> ) | Москва : Мир,<br>1973   | ЭБС    |

### 7.3 Перечень информационных технологий

#### 7.3.1 Программное обеспечение

Adobe Reader

Maxima

Notepad++

Octave

Python

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

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челябин. 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] / Челябин. 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] / Челябин. 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, лабораторные 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 лабораторных занятиях происходит практическое изучение свойств эллиптических кривых, реализация криптосистемы Эль-Гамала, подписи Шнора и алгоритма ECDSA, реализация атаки Менезеса-Окамото-Ванстоуна и проч. Рекомендуется перед каждым практическим занятием выполнить домашнее задание, что позволит лучше



усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на практических 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 информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и 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 с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности 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



МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное  
учреждение высшего образования  
«Челябинский государственный университет» (ФГБОУ ВО «ЧелГУ»)

Рабочая программа дисциплины "Дополнительные главы криптографии" по направлению подготовки (специальности) 10.05.01 "Компьютерная безопасность" направленности (профилю) специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" ФГБОУ ВО «ЧелГУ»

стр. 10

здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. 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.

