МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный педагогический университет»
(ФГБОУ ВО «АлтГПУ»)

УТВЕРЖДАЮ
проректор по образовательной и
международной деятельности
_____С.П. Волохов

Основы криптографии

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и методики обучения математике**
Учебный план ПМ01.03.04_2022.plx

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **2 ЗЕТ**

Часов по учебному плану 72 Виды контроля в семестрах:
в том числе: зачеты 4
аудиторные занятия 28
самостоятельная работа 42

Программу составил(и):

к.ф.-м.н., доцент, Кислицин Алексей Владимирович _____

Рабочая программа дисциплины

Основы криптографии

разработана на основании ФГОС ВО - бакалавриат по направлению подготовки 01.03.04 Прикладная математика (приказ Минобрнауки России от 15.01.2018 г. № 11)

составлена на основании учебного плана 01.03.04 Прикладная математика (Уровень: бакалавриат; квалификация: бакалавр), утвержденного Учёным советом ФГБОУ ВО «АлтГПУ» от 25.04.2022, протокол № 9.

Рабочая программа одобрена на заседании кафедры

Кафедра математики и методики обучения математике

Протокол № 8 от 19.04.2022 20:00:00 г.
Срок действия программы: 2022-2026 уч.г.
Зав. кафедрой Борисенко Оксана Викторовна

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	21			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Практические	14	14	14	14
Контроль самостоятельной работы	2	2	2	2
Итого ауд.	28	28	28	28
Контактная работа	30	30	30	30
Сам. работа	42	42	42	42
Итого	72	72	72	72

1.1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1.1	изучение основ криптографии и элементов теории кодирования - важных разделов современной математики. В последние десятилетия важное значение приобрели вопросы, связанные с сохранением и передачей информации. Возникающие при этом задачи решает криптография – наука о методах преобразования информации в целях её защиты, а также теория кодирования, изучающая вопросы надежной передачи информации по каналу, находящемуся под воздействием «шума».

1.2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.2.1	изложить элементы теории групп и теории сравнений;
1.2.2	изложить конструкцию фактор-кольца коммутативного кольца, доказать существование конечных полей и изучить их строение;
1.2.3	привести классические примеры шифров (Виженера, Хилла, Тритемиуса и др.);
1.2.4	изложить криптосистему RSA, криптосистему без передачи ключей;
1.2.5	доказать неравенство Крафта, изложить оптимальное кодирование Хаффмена и кодирование Фано;
1.2.6	изложить схемы передачи закодированного сообщения и примеров кодов, исправляющих одну ошибку (код «проверки на четность» и код Хэмминга).

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.ДВ.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Вводный курс математики
2.1.2	Линейная алгебра и аналитическая геометрия
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информации в БД
2.2.2	Производственная практика: научно-исследовательская работа
2.2.3	Производственная практика: преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-6.1: Анализирует возможных угроз для безопасности данных
ПК-6.2: Осуществляет выбор основных средств поддержки информационной безопасности на уровне БД

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	теорию сравнений, теорему Лагранжа, метод построения конечного поля порядка; примеры классических шифров (Цезаря, Хилла, Тритемиуса и др.); RSA – криптосистему, криптосистему без передачи ключей; кодирование Фано и оптимальное кодирование Хаффмена.
3.2	**Уметь:**
3.2.1	решать системы линейных уравнений кольце классов вычетов и в конечном поле, находить циклический порождающий конечного поля, пользоваться теоремой Ферма – Эйлера; шифровать и дешифровать текст с помощью классических шифров; использовать RSA- криптосистему (для небольших простых чисел p, q); использовать криптосистему без передачи ключей (для небольших простых чисел p); кодировать двоичным кодом Фано; кодировать двоичным кодом Хаффмена).
3.3	**Владеть:**
3.3.1	методами теории чисел и аппаратом абстрактной алгебры для решения поставленных прикладных задач; теорией и практикой применения RSA – криптосистемы; оптимальным кодированием Хаффмена.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Основы криптографии				
1.1	Элементы алгебры и теории чисел /Лек/	2	4	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Элементы алгебры и теории чисел /Пр/	2	4	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

1.3	Элементы алгебры и теории чисел /Ср/	2	14	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Элементы криптографии /Лек/	2	4	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Элементы криптографии /Пр/	2	4	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Элементы криптографии /Ср/	2	12	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.7	Элементы теории кодирования /Лек/	2	6	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.8	Элементы теории кодирования /Пр/	2	6	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.9	Элементы теории кодирования /Ср/	2	16	ПК-6.1 ПК-6.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Перечень индикаторов достижения компетенций, форм контроля и оценочных средств

ПК-6.1: Анализирует возможных угроз для безопасности данных
ПК-6.2: Осуществляет выбор основных средств поддержки информационной безопасности на уровне БД

5.2. Технологическая карта достижения индикаторов

Перечень индикаторов компетенций: ПК-6.1, ПК-6.2
Виды учебной работы: лекционные занятия
Формы контроля и оценочные средства: устный опрос (10 баллов)
Перечень индикаторов компетенций: ПК-6.1, ПК-6.2
Виды учебной работы: практические занятия
Формы контроля и оценочные средства: контрольная работа (30 баллов)
Перечень индикаторов компетенций: ПК-6.1, ПК-6.2
Виды учебной работы: самостоятельная работа
Формы контроля и оценочные средства: контрольная работа (20 баллов)
Перечень индикаторов компетенций: ПК-6.1, ПК-6.2
Виды учебной работы: зачет
Формы контроля и оценочные средства: вопросы к зачету (40 баллов)

5.3. Формы контроля и оценочные средства

Вопросы для устного контроля:
1. Расшифруйте понятия криптографии, криптологии, криптоанализа.
2. Сформулируйте определение группы.
3. Какие простейшие свойства групп вы знаете?
4. Как определяется группа подстановок?
5. Что такое «порядок группы»?
6. Что называется подгруппой?
7. Сформулируйте критерий подгруппы.
8. Что называется гомоморфизмом и изоморфизмом групп?
9. Сформулируйте теорему о гомоморфном образе группы.
10. Как характеризуется группа порожденная элементом a?
11. Сформулируйте теорему о подгруппе циклической группы.
12. Сформулируйте определение кольца.
13. Какие простейшие свойства колец вы знаете?
14. Сформулируйте определение и критерий подкольца.
15. Что означает поделить одно целое число на другое с остатком?
16. Сформулируйте теорему о делении с остатком.
17. Как определяется кольцо классов вычетов?
18. Что называют наибольшим общим делителем двух чисел?
19. Какие числа называются сравнимыми по модулю? Приведите примеры.
20. Перечислите основные свойства сравнений.
21. Что называется функцией Эйлера?
22. Сформулируйте теорему Эйлера.
23. Сформулируйте теорему Ферма.
24. Опишите алгоритм решения сравнений 1-ой степени с одним неизвестным.
25. Приведите примеры исторических кодов.
26. Какие коды называются перестановочными?
27. В чём состоит суть частотного метода?
28. В чем состоит различие между криптосистемами с открытым и закрытым ключом?
29. Какие коды называются линейными? Приведите примеры.

30. Сформулируйте определение поля.
31. Когда кольцо вычетов по модулю является конечным полем?
32. Что называется характеристикой поля?
33. Каким числом может быть характеристика поля?

Примерные задания контрольных работ:
1. Напишите таблицы для групповых операций в группах (Z4, +4) и (Z*5, □5). Докажите, что эти группы изоморфны, то есть постройте взаимно-однозначное соответствие □ между их элементами, удовлетворяющее следующему свойству: равенство □ + b □ c (mod 5).
2. Докажите, что множество четных чисел является подгруппой аддитивной группы Z целых чисел. Является ли множество нечетных чисел подгруппой группы Z ?
3. Докажите, что множество целых степеней числа 3 является подгруппой мультипликативной группы Q\{0}. Запишите эту подгруппу символически. Является ли она циклической? Каков порядок элемента, порождающего эту группу?
4. Образует ли кольцо следующие множества:
а) множество матриц второго порядка с нулями под главной диагональю; б) множество матриц второго порядка с нулевой побочной диагональю?
5. Напишите таблицы сложения и умножения для кольца (Z5, +, *).
6. Докажите, что кольцо вычетов по простому модулю является полем.
7. Найти все делители нуля, нильпотентные и обратимые элементы кольца 3Z27.
8. Существуют ли примеры полей порядка а) 2;
б) 4;
в) 6?
В случае положительного ответа привести соответствующие примеры.
9. Пусть p – простое число, k – положительное целое число. Докажите, что □(pk) = pk-1 (p – 1).
10. Решите сравнение 35x □ 10 (mod 50).
11. Решите сравнение первой степени: 10x □ 25 (mod 35).
12. Решите уравнения в целых числах: 81 x □ 48 y □ 33.
13. Пользуясь перестановочным кодом, дешифровать данное сообщение если: а) сообщение: ЛВТЕУЗПАСИАНЕТАНР, ключевое слово: Суриков;
б) сообщение: ПИПТИЕРДДРЕИИЕВРВДАЕ, ключевое слово: улица.
14. Пользуясь шифром Тритемиуса, дешифровать данное сообщение если: а) сообщение: НБКЫАКХАЕЭЭУРАКПЩУ, ключевое слово: код;
б) сообщение: ЕЩЦПЗФОФООБЮЦПУЭУЕ, ключевое слово: океан.
15. Пользуясь кодом Цезаря, дешифровать данное сообщение если: а) сообщение: ЫЕЖЬЕЖ, a = 3, b = 4;
б) сообщение: ВОЦКЗ, a = 3, b = 5.

Вопросы к зачету:
1.Шифрование и дешифрование информации. Основные понятия криптографии. 2.Подстановочные шифры на примере кода Цезаря. Недостатки подстановочных шифров. 3.Перестановочный код с использованием секретного слова. Шифр Тритемиуса.
4. Код Хилла.
5. Шифры с открытым ключом. Криптосистема RSA. 6.Определение и примеры колец. Простейшие свойства колец.
7.Определение и примеры полей. Характеристическое свойство поля вычетов. 8.Изоморфизм колец. Прямая сумма колец.
9. Подкольца. Порождающее множество кольца.
10. Делители нуля и обратимые элементы кольца, мультипликативная группа кольца. Описание обратимых элементов и делителей нуля кольца вычетов.
11. Идеалы кольца. Операции над идеалами. 12.Факторкольцо.
13.Гомоморфизмы колец. Теорема о гомоморфизме. 14.Мультипликативная группа прямой суммы колец.
15. Теорема о разложении кольца вычетов. Китайская теорема об остатках.
16. Теорема о разложении мультипликативной группы кольца вычетов. Теорема о порядке мульти- пликативной группы кольца вычетов и ее следствия.
17. Модулярное представление числа. Примеры. Операции над числами, представленными в моду- лярной форме. Достоинства и недостатки модулярного представления в сравнении с позиционным представлением числа.
18. Разложение числа на простые множители. Метод пробных делений. Недостатки метода. 19.Псевдопростые числа. Абсолютно псевдопростые числа (числа Кармайкла).
20.Тест Лукаса простоты числа. Сильно псевдопростые числа. 21.Разложение числа на простые множители. Метод Ферма.

5.4. Оценка результатов обучения в соответствии с индикаторами достижения компетенций

Неудовл.: не достигнут
Удовл. Пороговый уровень: Знает: основы теории сравнений, формулировку теоремы Лагранжа, примеры конечного поля; примеры классических шифров (Цезаря, Хилла, Тритемиуса); основные понятия RSA–криптосистемы, основные понятия криптосистемы без передачи ключей; кодирование Фано. Умеет: решать системы линейных уравнений в конечном поле, пользоваться теоремой Ферма–Эйлера; шифровать и дешифровать текст с помощью основных классических шифров; основу использования RSA-криптосистемы; основу использования криптосистемы без передачи ключей. Владеет: основными методами теории чисел и основами аппарата абстрактной алгебры для решения поставленных базовых прикладных задач; теорией применения RSA–криптосистемы.

Хорошо. Базовый уровень: Знает: теорию сравнений, теорему Лагранжа, метод построения конечного поля; примеры классических шифров (Цезаря, Хилла, Тритемиуса и др.); основные понятия и факты RSA–криптосистемы, основные понятия и факты криптоси- стемы без передачи ключей; кодирование Фано. Умеет: решать системы линейных уравнений кольце классов вычетов и в конечном поле, пользоваться теоремой Ферма–Эйлера; шифровать и дешифровать текст с помощью основных классических шифров; использовать RSA-криптосистему (для небольших простых чисел p, q); использовать криптосистему без передачи ключей (для небольших простых чисел p); кодировать двоичным ко- дом Фано). Владеет: методами теории чисел и аппаратом абстрактной алгебры для решения поставленных прикладных задач; теорией и практикой применения RSA– криптосистемы.
Отлично. Высокий уровень: Знает: теорию сравнений, теорему Лагранжа, метод построения конечного поля; приме- ры классических шифров (Цезаря, Хилла, Тритемиуса и др.); RSA–криптосистему, криптосистему без передачи ключей; кодирование Фано и оптимальное кодирование Хафф- мена. Умеет: решать системы линейных уравнений кольце классов вычетов и в конечном поле, находить циклический порождающий конечного поля, пользоваться теоремой Ферма–Эйлера; шифровать и дешифровать текст с помощью классических шифров; использовать RSA- криптосистему; использовать криптосистему без передачи ключей; ко- дировать двоичным кодом Фано; кодировать двоичным кодом Хаффмена). Владеет: методами теории чисел и аппаратом абстрактной алгебры для решения поставленных прикладных задач повышенной сложности; теорией и практикой применения RSA – криптосистемы; оптимальным кодированием Хаффмена.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Издание	Экз.
Л1.1	Г. В. Басалова	Основы криптографии: учебное пособие — Москва : ИНТУИТ ; Саратов : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/89455.html	9999
Л1.2	М. Е. Ильин, К. А. Ципоркова	Теоретико-числовые методы в криптографии. Часть 1: учебное пособие — Рязань : Рязанский государственный радиотехнический университет, 2020 — URL: https://www.iprbookshop.ru/121800.html	9999
Л1.3	М. Е. Ильин, К. А. Ципоркова	Теоретико-числовые методы в криптографии. Часть 2: учебное пособие — Рязань, 2021 — URL: https://e.lanbook.com/book/220439	9999

6.1.2. Дополнительная литература

	Авторы, составители	Издание	Экз.
Л2.1	Б. А. Фороузан	Криптография и безопасность сетей: учебное пособие — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ) : Ай Пи Ар Медиа, 2021 — URL: https://www.iprbookshop.ru/102017.html	9999
Л2.2	Ж. Земор ; пер. с франц. В. В. Шуликовской	Курс криптографии: монография — Москва ; Ижевск : Институт компьютерных исследований : Регулярная и хаотическая динамика, 2019 — URL: https://www.iprbookshop.ru/91941.html	9999
Л2.3	Ю. В. Пономарчук, Р. А. Ешенко, Е. В. Фалеева	Основы анализа шифров классической криптографии: учебное пособие — Хабаровск : Изд-во ДВГУПС, 2019 — URL: https://e.lanbook.com/book/179357	9999

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет Microsoft Office
6.3.1.2	Операционная система семейства Windows
6.3.1.3	Интернет браузер
6.3.1.4	Программа для просмотра электронных документов формата pdf, djvu

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронная библиотека НПБ / Алтайский государственный педагогический университет, Научно-педагогическая библиотека
6.3.2.2	МЭБ. Межвузовская электронная библиотека / Новосибирский государственный педагогический университет
6.3.2.3	Сетевая электронная библиотека педагогических вузов // Электронно-библиотечная система Лань / Издательство Лань

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Оборудованные учебные аудитории, в том числе с использованием мультимедийных комплектов, подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.2	Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.

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

Студенту следует помнить, что дисциплина «Основы криптографии» предусматривает обязательное посещение студентом лекций и практических занятий. Она реализуется через систему домашних работ, систему рефератов и индивидуальных работ. Самостоятельная работа студентов заключается в выполнении домашних заданий с целью подготовки к практическим занятиям (см. планы практических занятий) и подготовке рефератов. Контроль над самостоятельной работой студентов и проверка их знаний проводится в виде зачета.

Дисциплина «Основы криптографии» призвана сформировать у студентов целостное представление об основных понятиях курса «Введение в криптографию», обеспечить усвоение методов решения задач. Важной составной частью учебного процесса в вузе являются практические занятия. Они помогают студентам глубже усвоить учебный материал, приобрести навыки творческой работы с основной и дополнительной литературой и лекционным материалом. Практическое занятие представляет собой форму организации учебного процесса, в ходе которого студент должен приобрести новые учебные знания, их систематизировать и концептуализировать; оперировать базовыми понятиями и теоретическими конструкциями учебной дисциплины. Целью практических занятий является приобретение студентами новых знаний, умений и навыков, необходимых для профессиональной деятельности, развитие у них естественно-научного мышления и интеллектуальных способностей как средства индивидуального освоения учебной дисциплины. Все это требует тщательной подготовки к практическим занятиям. При подготовке к практическим занятиям следует использовать всю рекомендованную литературу, размещенную на бумажных или электронных носителях. Готовясь к занятию, надо прочитать рекомендованную литературу и составить простые планы прочитанных текстов, а также решить предложенные задачи. Особое внимание следует уделять связям между основными понятиями, рассматриваемыми в теме. Планы практических занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях или в методических указаниях по данной дисциплине. На занятии студенты должны быть готовыми к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление студентов на занятии должно быть правильным, полным и аргументированным. Необходимо, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускается и простое чтение конспекта. Важно, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание,
обосновывал его и мог сделать правильные выводы из сказанного. При этом студент может обращаться к записям конспекта лекций, непосредственно к первоисточникам, использовать знание математической литературы, факты из дополнительных источников. Вокруг такого выступления могут разгореться споры, дискуссии, к участию в которых должен стремиться каждый. Практическое занятие является важнейшей формой усвоения знаний. Важным фактором результативности данного вида занятий, его высокой эффективности является процесс подготовки. Прежде всего, студенты должны уяснить предложенный план занятия, осмыслить вынесенные для обсуждения вопросы, место каждого из вопросов в раскрытии темы занятия. Подготовка активизирует работу студента с книгой, требует обращения к литературе, учит рассуждать. В процессе подготовки к семинару закрепляются и уточняются уже известные и осваиваются новые утверждения и факты. Сталкиваясь в ходе подготовки с недостаточно понятными моментами темы, студенты находят ответы самостоятельно или фиксируют свои вопросы для постановки и уяснения их на самом занятии. В ходе занятия студент учится публично выступать, видеть реакцию слушателей, логично, ясно, четко, грамотным математическим языком излагать мысли, приводить доводы, формулировать аргументы в защиту своей позиции. В ходе семинара каждый студент опирается на свои конспекты, сделанные на лекции, собственные выписки из учебников, первоисточников, статей, другой математической литературы. Практическое занятие – эффективная форма закрепления полученных по обсуждаемой проблеме знаний, видения этой проблемы в целом, осознания ее соотнесенности с другими темами. Подготовку к семинарскому занятию следует начинать с ознакомления с соответствующим разделом учебника и лекции. Во время чтения лекции необходимо составить краткий план-конспект будущего ответа на практическом занятии, для чего целесообразно использовать специальную тетрадь для практических занятий. План ответа не должен представлять собой необработанную компиляцию учебной литературы; лучше, если он будет составлен в виде кратких, легко запоминающихся утверждений, которыми студент может пользоваться при ответе. В подготовке к практическим занятиям большое значение имеет рекомендованная лектором и ведущим практические занятия преподавателем учебная и научная литература. Различные вопросы по-разному раскрыты в учебниках,
поэтому целесообразно иметь студенту один, два учебника (разных авторов), а также по отдельным вопросам обращаться и к иной учебной литературе. Залогом высоких учебных результатов студента является подготовка к практическим занятиям и работа на них на протяжении всего семестра. На практическом занятии не требуется точное воспроизведение лекционного материала или положений учебника. Но в любом случае, студент должен свободно владеть терминологией, понимать доказательства основных теорем, уметь решать основные задачи для того, чтобы чётко и последовательно ответить на поставленные вопросы. Виды аудиторной самостоятельной работы, поэтапное ее выполнение, критерии оценивания представлены в ФОС по дисциплине «Введение в криптографию», технологической карте и учебно-методическом пособии по организации аудиторной самостоятельной работы по предлагаемому курсу. На практических занятиях, лекциях, в ходе самостоятельной работы студенты должны уяснить современные теоретические представления о курсе «Введение в криптографию»; уметь доказывать основные теоремы курса, знать основные алгоритмы, уметь решать основные задачи. По дисциплине «Введение в криптографию» предусмотрен зачет.

Под специальными условиями для получения образования обучающимися с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития, включающие в себя использование специальных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования. Построение образовательного процесса ориентировано на учет индивидуальных возрастных, психофизических особенностей обучающихся, в частности предполагается возможность разработки индивидуальных учебных планов. Реализация индивидуальных учебных планов сопровождается поддержкой тьютора (родителя, взявшего на себя тьюторские функции в процессе обучения, волонтера). Обучающиеся с ОВЗ, как и все остальные студенты, могут обучаться по индивидуальному учебному плану в установленные сроки с учетом индивидуальных особенностей и специальных образовательных потребностей конкретного обучающегося. При составлении индивидуального графика обучения для лиц с ОВЗ возможны различные варианты проведения занятий: проведение индивидуальных или групповых занятий с целью устранения сложностей в усвоении лекционного материала, подготовке к семинарским занятиям, выполнению заданий по самостоятельной работе. Для лиц с ОВЗ, по их просьбе, могут

быть адаптированы как сами задания, так и формы их выполнения. Выполнение под руководством преподавателя индивидуального проектного задания, позволяющего сочетать теоретические знания и практические навыки; применение мультимедийных технологий в процессе ознакомительных лекций и семинарских занятий, что позволяет экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем.

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации преподаватели, в соответствии с потребностями студента, отмеченными в анкете, и рекомендациями специалистов дефектологического профиля, разрабатывает фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). Лицам с ОВЗ может быть предоставлено дополнительное время для подготовки к ответу на экзамене, выполнения задания для самостоятельной работы.

При необходимости студент с ограниченными возможностями здоровья подает письменное заявление о создании для него специальных условий в Учебно-методическое управление Университета с приложением копий документов, подтверждающих статус инвалида или лица с ОВЗ.