МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

**ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

| | |
|---|---|
| «СОГЛАСОВАНО» | «УТВЕРЖДАЮ» |
| Руководитель ОП | Директор департамента математики |
| _____ Ефремов Е.Л. | _____ Заболотский В.С. |
| (подпись) (Ф.И.О.) | (подпись) (Ф.И.О.) |
| «28» декабря 2021 г. | «28» декабря 2021 г. |

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации
**Направление подготовки 01.04.01 Математика**
Математика и моделирование сложных систем
**Форма подготовки очная**

курс 2 семестр 3
лекции 18 час.
практические занятия 32 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. - / пр. 14 / лаб. 00 час.
всего часов аудиторной нагрузки 50 час.
в том числе с использованием МАО 14 час.
самостоятельная работа 58 час.
в том числе на подготовку к экзамену - час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 3 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 01.04.01 Математика, утвержденного приказом Министерства образования и науки Российской Федерации от 10 октября 2018 г. № 12.

Рабочая программа обсуждена на заседании департамента математики
протокол № 6 от «28» декабря 2021 г.

Директор департамента Заболотский В.С.
Составитель к.ф.-м.н. Чеканов С.Г.

Владивосток
2021

**I. Рабочая программа пересмотрена на заседании департамента**:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании департамента**:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**III. Рабочая программа пересмотрена на заседании департамента**:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

**IV. Рабочая программа пересмотрена на заседании департамента**:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

1. Цель и задачи освоения дисциплины

Дисциплина «Криптографические методы защиты информации» предназначена для магистрантов 2 курса магистратуры 01.04.01 Математика, магистерской программы «Математика и моделирование сложных систем».

Дисциплина «Криптографические методы защиты информации» входит в блок дисциплин по выбору части дисциплин, формируемой участниками образовательных отношений (Б1.В.ДВ.02), реализуется на 2 курсе, в 3 семестре, завершается зачётом. Общая трудоемкость освоения дисциплины составляет 3 З.Е. (108 час.). Учебным планом предусмотрены лекционные занятия (18 час.), практические занятия (32 час.), самостоятельная работа (58 час.).

Язык реализации – русский.

**Цель**: изучение современных концепций и теоретических моделей криптографических примитивов.

**Задачи**:

- Овладеть основными концепциями информационной безопасности.
- Познакомиться с современными криптографическими алгоритмами.
- Изучить основные понятий и конструкции для построения протоколов.
- Научиться применять полученные знания при построении моделей криптографических примитивов и оценке их стойкости.

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность видеть методологические аспекты построения математических теорий;
- применять системный подход в формализации математических задач;
- способностью к абстрактному мышлению, анализу, синтезу.

В результате изучения данной дисциплины у обучающихся формируются профессиональные компетенции.

Профессиональные компетенции выпускников и индикаторы их достижения:

| Тип задач | Код и наименование профессиональной компетенции (результат освоения) | Код и наименование индикатора достижения компетенции |
|---|---|---|
| научно-исследовательский | ПК-2 Способен к организации научно-исследовательских и научно-производственных работ, к управлению | ПК-2.1 Использует методы современной математики и моделирования при решении теоретических и прикладных задач |
| | | ПК-2.2 Осуществляет организационное управление научно-исследовательскими и научно-производственными работами, научным |

| Тип задач | Код и наименование профессиональной компетенции (результат освоения) | Код и наименование индикатора достижения компетенции |
|---|---|---|
| | научным коллективом | коллективом |
| | | ПК-2.3 Готовит научные публикации и выступления на научных семинарах |
| педагогический | ПК-4 Способен участвовать в проектировании предметной среды образовательной программы | ПК-4.1 Организует и проводит исследование рынка услуг дополнительного образования детей и взрослых, обосновывает включение научно-исследовательских и научно-образовательных объектов в образовательную среду и процесс обучения математике и моделированию |
| | | ПК-4.2 Проектирует элементы образовательной среды школьной математики на основе учета возможностей конкретного региона |
| | | ПК-4.3 Планирует и проектирует образовательный процесс, элементы образовательной программы |

| Код и наименование индикатора достижения компетенции | Наименование показателя оценивания (результата обучения по дисциплине) |
|---|---|
| ПК-2.1 Использует методы современной математики и моделирования при решении теоретических и прикладных задач | Знает профессиональную терминологию, способы воздействия на аудиторию в рамках профессиональной коммуникации |
| | Умеет правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач |
| | Владеет навыками подготовки научных публикаций |
| ПК-2.2 Осуществляет организационное управление научно-исследовательскими и научно-производственными работами, научным коллективом | Знает основные принципы организации работы научно-исследовательских коллективов |
| | Умеет распределить обязанности среди членов научного коллектива |
| | Владеет навыками контроля деятельности членов коллектива |
| ПК-2.3 Готовит научные публикации и выступления на научных семинарах | Знает основные принципы построения научного доклада и написания научных статей |
| | Умеет донести до слушателей наиболее важные факты и доказательства, содержащиеся в докладе |
| | Владеет умением излагать материал на хорошем научном уровне |
| ПК-4.1 Организует и проводит исследование рынка услуг дополнительного образования детей и взрослых, обосновывает включение научно-исследовательских и научно-образовательных объектов в образовательную среду и процесс обучения математике и моделированию | Знает принципы и подходы к организации предметной среды математики; научно-исследовательский и научно-образовательный потенциал конкретного региона, где осуществляется образовательная деятельность |
| | Умеет использовать возможности социокультурной среды региона в целях достижения результатов обучения математике |
| | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона |
| ПК-4.2 Проектирует элементы образовательной среды школьной математики на основе учета | Знает компоненты образовательной среды и их дидактические возможности |
| | Умеет обосновывать и включать научно-исследовательские и |

| | |
|---|---|
| возможностей конкретного региона | научно-образовательные объекты в образовательную среду и процесс обучения математике |
| | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона |
| ПК-4.3 Планирует и проектирует образовательный процесс, элементы образовательной программы | Знает принципы организации образовательных процессов |
| | Умеет проектировать учебные дисциплины и формировать образовательные программы |
| | Владеет навыками реализации образовательных программ |

## 2. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 3 зачётные единицы (108 академических часов). Форма обучения – очная.

Видами учебных занятий и работы обучающегося по дисциплине являются:

| Обозначение | Виды учебных занятий и работы обучающегося |
|---|---|
| Лек | Лекции |
| Пр | Практические занятия |
| Лаб | Лабораторные работы |
| СР | Самостоятельная работа обучающегося в период теоретического обучения |
| Контроль | Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации |

Структура дисциплины:

| № | Наименование раздела дисциплины | Семестр | Количество часов по видам учебных занятий и работы обучающегося | | | | | Формы промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | | Лек | Пр | Лаб | СР | Контроль | |
| 1 | Раздел 1. Шифры замены | 3 | 4 | 10 | | 30 | | УО-1, ПР-6 |
| 2 | Раздел 2. Оценка стойкости шифров. Совершенные шифры | 3 | 4 | 8 | | 24 | | УО-1, ПР-1 |
| 3 | Раздел 3. Поточные и блочные шифры | 3 | 4 | 6 | | 18 | | УО-3, ПР-4 |
| 4 | Раздел 4 Асимметричные шифры и хеш функции | 3 | 6 | 12 | | 36 | | УО-1, ПР-1 |
| | Итого: | | 18 | 32 | | 58 | | |

## I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

### Лекционные занятия (18 часов)

**Раздел 1. Шифры замены (4 часа)**

**Тема 1. Шифры простой замены (2 часа)**

Определение алгебраической модели шифра. Понятие алгебраической платформы шифра. Примеры шифров простой замены.

**Тема 2. Многоалфавитные шифры замены (2 часа)**

Представление естественных алфавитов элементами алгебраических систем. Криптоанализ шифров замены.

**Раздел 2. Оценка стойкости шифров. Совершенные шифры (4 часа)**

**Тема 1. Вероятностная модель шифра (2 часа)**

Энтропия и избыточность языка. Теоретическая стойкость шифров. Совершенные шифры.

**Тема 2. Имитостойкость шифров (2 часа)**

Оценка имитостойкости шифров. Шифры, не распространяющие искажений.

**Раздел 3. Поточные и блочные шифры (2 часов)**

**Тема 1. Блочные шифры (2 часа)**

Примеры блочных шифров. Методы анализа блочных шифров. Режимы использования блочных шифров.

**Тема 2. Поточные шифры (2 часа)**

Принципы построения поточных шифров. Примеры поточных шифров. Генераторы ключевых последовательностей.

**Раздел 4. Асимметричные шифры (6 часов)**

**Тема 1. Меры сложности (2 часа)**

Понятие меры вычислительной сложности. Машинно-независимые утверждения. Теорема о неограниченности сложности. Временная и пространственная сложность алгоритмов.

**Тема 2. Шифры с открытым ключом (2 часов)**

Шифр RSA. Шифрсистема Эль-Гамаля.

**Тема 3. Криптографические функции хеширования (4 часа)**

Ключевые и бесключевые функции хеширования. Целостность данных и аутентификация сообщений. Возможные атаки на функции хеширования.

## II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

### Практические занятия (32 часа)

**Занятие 1.** Построение шифров простой замены (2 часа).

**Занятие 2.** Криптоанализ шифров простой замены (2 часа).

**Занятие 3.** Представление естественных алфавитов алгебраическими системами (2 часа).

**Занятие 4.** Криптоанализ шифра Виженера (4 часа).

**Занятие 5.** Энтропия и избыточность языка (2 часа).

**Занятие 6.** Совершенные шифры (2 часа).

**Занятие 7.** Шифры, не распространяющие искажений (2 часа).

**Занятия 8-9.** Блочные шифры (4 часа).

**Занятия 10-11.** Поточные шифры (4 часа).

**Занятия 12-13.** Шифры с открытыми ключами (4 часа).

**Занятия 14-15.** Хеш функции (4 часа).

### Примеры контрольных работ

### Раздел: Шифры замены

Вариант 1.

1. Зашифровать сообщение «Прежде чем сдаваться, вспомни ради чего ты все начинал» методом одиночной перестановки по ключу. В качестве ключа использовать слово СОТРУДНИК.
2. Зашифровать методом двойной перестановки сообщение: ПРИЛЕТАЮ ВОСЬМОГО Для шифрования использовать ключи: По столбцам – 4132, по строкам – 3142
3. Сообщение «ТНПВЕ ГЛЕАР АДОНР ТИЕЪВ ОМОБТ МПЧИР ЫСООЬ» зашифровано методом одиночной перестановки по ключу. Таблица имеет размерность 7Х5. Расшифровать сообщение.

### Примеры индивидуальных домашних заданий

### Раздел: Асимметричные шифры

1. Зашифруйте фразу «СЕССИЯ СДАНА НА ОТЛИЧНО» методом перестановки с использованием шифрующей таблицы с параметрами n (число строк) и k (число столбцов) (табл. 1).

Таблица 1.

| вариант | n | k |
|---|---|---|
| 1 | 4 | 5 |
| 2 | 5 | 4 |
| 3 | 2 | 10 |
| 4 | 10 | 2 |
| 5 | 5 | 4 |
| 6 | 4 | 5 |
| 7 | 5 | 4 |
| 8 | 4 | 5 |
| 9 | 2 | 10 |
| 10 | 10 | 2 |

2. Зашифруйте фразу «СЕССИЯ СДАНА НА ОТЛИЧНО» методом одиночной перестановки по ключу К (табл. 2).

Таблица 2.

| вариант | К |
|---|---|
| 1 | Полет |
| 2 | Дома |
| 3 | Нора |
| 4 | Мода |
| 5 | Зачет |
| 6 | Сова |
| 7 | Успех |
| 8 | Лиса |
| 9 | Волк |
| 10 | Парки |

3. Зашифруйте фразу «СЕССИЯ СДАНА НА ОТЛИЧНО» методом двойной перестановки с ключами $К_1$ (задает перестановку по столбцам) и $К_2$ (задает перестановку по строкам) из табл. 3.

Таблица 3.

| вариант | $К_1$ | $К_2$ |
|---|---|---|
| 1 | Полет | Зима |
| 2 | Дома | Цветы |
| 3 | Нора | Арбуз |
| 4 | Мода | Флора |
| 5 | Зачет | Лето |

| | | |
|---|---|---|
| 6 | Сова | Осень |
| 7 | Успех | Снег |
| 8 | Лиса | Забор |
| 9 | Волк | Мышка |
| 10 | Парки | Коты |

## III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине включает в себя:

– план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

– требования к представлению и оформлению результатов самостоятельной работы;

– критерии оценки выполнения самостоятельной работы.

### План-график выполнения самостоятельной работы по дисциплине

| № п/п | Дата/сроки выполнения | Вид самостоятельной работы | Примерные нормы времени на выполнение | Форма контроля |
|---|---|---|---|---|
| 1 | В течение семестра | Подготовка к практическим занятиям, изучение литературы | 6 часов | Работа на практических занятиях (ПР-6) |
| 2 | 1-4 неделя семестра | Выполнение контрольной работы № 1 | 6 часов | ПР-6 |
| 3 | 5-8 неделя семестра | Выполнение индивидуального домашнего задания № 1 | 6 часов | УО-1 (собеседование/устный опрос) |
| 4 | 9-11неделя семестра | Выполнение контрольной работы № 2 | 6 часов | УО-1 (собеседование/устный опрос) |
| 5 | 12-15 неделя семестра | Выполнение индивидуального домашнего задания № 2 | 6 часов | зачет |
| 6 | 16-18 неделя семестра | Подготовка к зачету | 18 часов | зачет |
| Итого: | | | 48 часов | |

**Рекомендации по самостоятельной работе студентов**

*Планирование и организация времени, отведенного на выполнение заданий самостоятельной работы.*

Изучив график выполнения самостоятельных работ, следует правильно её организовать. Рекомендуется изучить структуру каждого задания, обратить внимание на график выполнения работ, отчетность по каждому заданию предоставляется в последнюю неделю согласно графику. Обратить внимание, что итоги самостоятельной работы влияют на окончательную оценку по итогам освоения учебной дисциплины.

*Работа с литературой.*

При выполнении ряда заданий требуется работать с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ (http://www.dvfu.ru/library/) и других ведущих вузов страны, а также доступных для использования научно-библиотечных систем.

В процессе выполнения самостоятельной работы, в том числе при написании эссе рекомендуется работать со следующими видами изданий:

а) Научные издания, предназначенные для научной работы и содержащие теоретические, экспериментальные сведения об исследованиях. Они могут публиковаться в форме: монографий, научных статей в журналах или в научных сборниках;

б) Учебная литература подразделяется на:

- учебные издания (учебники, учебные пособия, тексты лекций), в которых содержится наиболее полное системное изложение дисциплины или какого-то ее раздела;

- справочники, словари и энциклопедии – издания, содержащие краткие сведения научного или прикладного характера, не предназначенные для сплошного чтения. Их цель – возможность быстрого получения самых общих представлений о предмете.

Существуют два метода работы над источниками:

– сплошное чтение обязательно при изучении учебника, глав монографии или статьи, то есть того, что имеет учебное значение. Как правило, здесь требуется повторное чтение, для того чтобы понять написанное. Старайтесь при сплошном чтении не пропускать комментарии, сноски, справочные материалы, так как они предназначены для пояснений и помощи. Анализируйте рисунки (карты, диаграммы, графики), старайтесь понять, какие тенденции и закономерности они отражают;

– метод выборочного чтения дополняет сплошное чтение; он применяется

для поисков дополнительных, уточняющих необходимых сведений в словарях, энциклопедиях, иных справочных изданиях. Этот метод крайне важен для повторения изученного и его закрепления, особенно при подготовке к зачету.

Для того чтобы каждый метод принес наибольший эффект, необходимо фиксировать все важные моменты, связанные с интересующей Вас темой.

Тезисы – это основные положения научного труда, статьи или другого произведения, а возможно, и устного выступления; они несут в себе больший объем информации, нежели план. Простые тезисы лаконичны по форме; сложные – помимо главной авторской мысли содержат краткое ее обоснование и доказательства, придающие тезисам более весомый и убедительный характер. Тезисы прочитанного позволяют глубже раскрыть его содержание; обучаясь излагать суть прочитанного в тезисной форме, вы сумеете выделять из множества мыслей авторов самые главные и ценные и делать обобщения.

Конспект – это способ самостоятельно изложить содержание книги или статьи в логической последовательности. Конспектируя какой-либо источник, надо стремиться к тому, чтобы немногими словами сказать о многом. В тексте конспекта желательно поместить не только выводы или положения, но и их аргументированные доказательства (факты, цифры, цитаты).

Писать конспект можно и по мере изучения произведения, например, если прорабатывается монография или несколько журнальных статей.

Составляя тезисы или конспект, всегда делайте ссылки на страницы, с которых вы взяли конспектируемое положение или факт, – это поможет вам сократить время на поиск нужного места в книге, если возникает потребность глубже разобраться с излагаемым вопросом или что-то уточнить при написании письменных работ.

**Методические рекомендации по выполнению заданий для самостоятельной работы и критерии оценки**

*Контрольная работа №1.* От обучающегося требуется:

1. Знать и понимать определение шифра замены.

2. Уметь шифровать и проводить криптоанализ шифра замены.

*Критерии оценки.* Используется зачетная система. Для получения зачета необходимо решить не менее, чем две трети задач.

*Индивидуальная работа № 1.* От обучающегося требуется:

1. Знать и понимать определение совершенного шифра.

2. Уметь строить простейшие модели совершенных шифров.

*Критерии оценки.* Используется зачетная система. Для получения зачета

необходимо решить не менее, чем две трети задач.

*Контрольная работа №2.* От обучающегося требуется:

1. Знать и понимать определения поточного и блочного шифров.

2. Уметь применять основные принципы построения блочных и поточных шифров.

*Критерии оценки*. Используется зачетная система. Для получения зачета необходимо решить не менее, чем две трети задач.

*Индивидуальная работа № 2.* От обучающегося требуется:

1. Знать и понимать определение ассиметричного шифра.

2. Уметь применять алгоритмы шифрования и дешифрования асимметричных шифров.

*Критерии оценки*. Используется зачетная система. Для получения зачета необходимо решить не менее, чем две трети задач.

## IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

| № п/п | Контролируемые модули/ разделы / темы дисциплины | Код индикатора достижения компетенции | Результаты обучения | Оценочные средства – наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Раздел I. Шифры замены | ПК-4.1 Организует и проводит исследование рынка услуг дополнительного образования детей и взрослых, обосновывает включение научно-исследовательских и научно-образовательных объектов в образовательную среду и процесс обучения математике и моделированию | Знает принципы и подходы к организации предметной среды математики; научно-исследовательский и научно-образовательный потенциал конкретного региона, где осуществляется образовательная деятельность | УО-1 собеседование / устный опрос; ПР-6 контрольная работа | вопросы к зачету 1-5 |
| | | | Умеет использовать возможности социокультурной среды региона в целях достижения результатов обучения математике | УО-1 собеседование / устный опрос; | |
| | | | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона | ПР-6 контрольная работа | |
| | | ПК-4.2 Проектирует элементы | Знает компоненты образовательной среды и их дидактические возможности | УО-1 собеседование / устный опрос; | |

| | | | | | |
|---|---|---|---|---|---|
| | | образовательной среды школьной математики на основе учета возможностей конкретного региона | Умеет обосновывать и включать научно-исследовательские и научно-образовательные объекты в образовательную среду и процесс обучения математике | ПР-6 контрольная работа | |
| | | | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона | УО-1 собеседование / устный опрос; | |
| | | ПК-4.3 Планирует и проектирует образовательный процесс, элементы образовательной программы | Знает принципы организации образовательных процессов | ПР-6 контрольная работа | |
| | | | Умеет проектировать учебные дисциплины и формировать образовательные программы | УО-1 собеседование / устный опрос; | |
| | | | Владеет навыками реализации образовательных программ | ПР-6 контрольная работа | |
| 2 | Раздел 2. Оценка стойкости. Совершенные шифры | ПК-2.1 Использует методы современной математики и моделирования при решении теоретических и прикладных задач | Знает профессиональную терминологию, способы воздействия на аудиторию в рамках профессиональной коммуникации | УО-1 собеседование / устный опрос; ПР-12 индивидуальное домашнее задание | вопросы к зачету 6-13 |
| | | | Умеет правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач | УО-1 собеседование / устный опрос; | |
| | | | Владеет навыками подготовки научных публикаций | ПР-12 индивидуальное домашнее задание | |
| | | ПК-2.2 Осуществляет организационное управление научно-исследовательскими и научно-производственными работами, научным коллективом | Знает основные принципы организации работы научно-исследовательских коллективов | УО-1 собеседование / устный опрос; | |
| | | | Умеет распределить обязанности среди членов научного коллектива | ПР-12 индивидуальное домашнее задание | |
| | | | Владеет навыками контроля деятельности членов коллектива | УО-1 собеседование / устный опрос; | |
| | | ПК-2.3 Готовит научные публикации и выступления на научных семинарах | Знает основные принципы построения научного доклада и написания научных статей | УО-1 собеседование / устный опрос; | |
| | | | Умеет донести до слушателей наиболее важные факты и доказательства, содержащиеся в докладе | ПР-12 индивидуальное домашнее задание | |
| | | | Владеет умением излагать материал на хорошем научном уровне | УО-1 собеседование / устный опрос; | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Раздел 3. Поточные и блочные шифры | ПК-4.1 Организует и проводит исследование рынка услуг дополнительного образования детей и взрослых, обосновывает включение научно-исследовательских и научно-образовательных объектов в образовательную среду и процесс обучения математике и моделированию | Знает принципы и подходы к организации предметной среды математики; научно-исследовательский и научно-образовательный потенциал конкретного региона, где осуществляется образовательная деятельность | УО-1 собеседование / устный опрос; | вопросы к зачету 14-19 |
| | | | Умеет использовать возможности социокультурной среды региона в целях достижения результатов обучения математике | ПР-12 контрольная работа | |
| | | | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона | УО-1 собеседование / устный опрос; | |
| | | ПК-4.2 Проектирует элементы образовательной среды школьной математики на основе учета возможностей конкретного региона | Знает компоненты образовательной среды и их дидактические возможности | ПР-12 контрольная работа | |
| | | | Умеет обосновывать и включать научно-исследовательские и научно-образовательные объекты в образовательную среду и процесс обучения математике | УО-1 собеседование / устный опрос; | |
| | | | Владеет умениями по проектированию элементов образовательной среды школьной математики на основе учета возможностей конкретного региона | ПР-12 контрольная работа | |
| | | ПК-4.3 Планирует и проектирует образовательный процесс, элементы образовательной программы | Знает принципы организации образовательных процессов | УО-1 собеседование / устный опрос; | |
| | | | Умеет проектировать учебные дисциплины и формировать образовательные программы | ПР-12 контрольная работа | |
| | | | Владеет навыками реализации образовательных программ | УО-1 собеседование / устный опрос; | |
| 4 | Раздел 4. Ассиметричные шифры | ПК-2.1 Использует методы современной математики и моделирования при решении теоретических и прикладных задач | Знает профессиональную терминологию, способы воздействия на аудиторию в рамках профессиональной коммуникации | УО-1 собеседование / устный опрос; ПР-6 индивидуальное домашнее задание | вопросы к зачету 20-25 |
| | | | Умеет правильно ставить задачи по выбранной тематике, выбирать для исследования необходимые методы; применять выбранные методы к решению научных задач | УО-1 собеседование / устный опрос; | |
| | | | Владеет навыками подготовки научных публикаций | ПР-6 индивидуальное домашнее | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | задание | |
| | | ПК-2.2 Осуществляет организационное управление научно-исследовательским и и научно-производственным и работами, научным коллективом | Знает основные принципы организации работы научно-исследовательских коллективов | УО-1 собеседование / устный опрос; | |
| | | | Умеет распределить обязанности среди членов научного коллектива | ПР-6 индивидуальное домашнее задание | |
| | | | Владеет навыками контроля деятельности членов коллектива | УО-1 собеседование / устный опрос; | |
| | | ПК-2.3 Готовит научные публикации и выступления на научных семинарах | Знает основные принципы построения научного доклада и написания научных статей | ПР-6 индивидуальное домашнее задание | |

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также качественные критерии оценивания, которые описывают уровень сформированности компетенций, представлены в разделе VIII.

## V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература


1. Сагалович, Ю.Л. Введение в алгебраические коды: учебное пособие/ Ю.Л. Сагалович. – 3-е изд., перераб. и доп. – М.: ИППИ РАН, 2014. – 310 с. https://lib.dvfu.ru/lib/item?id=chamo:756734&theme=FEFU
2. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2012 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU
3. Ларин С.И. Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов по естественнонаучным направлениям / С. В. Ларин. Москва : Юрайт, 2020

https://lib.dvfu.ru/lib/item?id=chamo:884134&theme=FEFU

4. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Изд-во Горячая линия-Телеком, 2017 https://e.lanbook.com/book/111097

5. Криптографические методы защиты информации: лабораторный практикум. Изд-во Северо-Кавказского федерального университета, 2015

https://e.lanbook.com/book/155280

6. Мартынов Л.М. Алгебра для криптографии. Часть 1: учебное пособие, Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129189

7. Мартынов Л.М. Алгебра для криптографии. Часть 2: учебное пособие, Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129188

8. Мартынов Л.М. Алгебра для криптографии. Часть 3: учебное пособие, Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129190

**Дополнительная литература**

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:5790&theme=FEFU

2. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU

3. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-399&theme=FEFU

4. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-46&theme=FEFU

5. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:103102&theme=FEFU

**Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

1. http://e.lanbook.com/books/element.php?pl1_id=62755 Серёдкин А.Н., Роганов В.Р., Филиппенко В.О. Основы защиты информации и информационные технологии: Учебное пособие в 3 частях. – Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ: Изд-во ПензГТУ.-2013

**Профессиональные базы данных и информационные справочные системы**

1. База данных Scopus http://www.scopus.com/home.url
2. База данных Web of Science http://apps.webofknowledge.com/

3. Общероссийский математический портал Math-Net.Ru http://www.mathnet.ru

4. Электронная библиотека диссертаций Российской государственной библиотеки http://diss.rsl.ru/

5. Электронная библиотека Европейского математического общества https://www.emis.de/

6. Электронные базы данных EBSCO http://search.ebscohost.com/

## VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

**Планирование и организация времени, отведенного на изучение дисциплины.** Приступить к освоению дисциплины следует незамедлительно в самом начале учебного семестра. Рекомендуется изучить структуру и основные положения Рабочей программы дисциплины. Обратить внимание, что кроме аудиторной работы (лекции, лабораторные занятия) планируется самостоятельная работа, итоги которой влияют на окончательную оценку по итогам освоения учебной дисциплины. Все задания (аудиторные и самостоятельные) необходимо выполнять и предоставлять на оценку в соответствии с графиком.

В процессе изучения материалов учебного курса предлагаются следующие формы работ: чтение лекций, лабораторные занятия, задания для самостоятельной работы.

*Лекционные занятия* ориентированы на освещение вводных тем в каждый раздел курса и призваны ориентировать студентов в предлагаемом материале, заложить научные и методологические основы для дальнейшей самостоятельной работы студентов.

*Лабораторные занятия* акцентированы на наиболее принципиальных и проблемных вопросах курса и призваны стимулировать выработку практических умений.

Особо значимой для профессиональной подготовки студентов является *самостоятельная работа* по курсу. В ходе этой работы студенты отбирают необходимый материал по изучаемому вопросу и анализируют его. Студентам необходимо ознакомиться с основными источниками, без которых невозможно полноценное понимание проблематики курса.

Освоение курса способствует развитию навыков обоснованных и самостоятельных оценок фактов и концепций. Поэтому во всех формах контроля знаний, особенно при сдаче зачета, внимание обращается на понимание проблематики курса, на умение практически применять знания и делать выводы.

**Работа с литературой.** Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ и электронные библиотеки (http://www.dvfu.ru/library/), а также доступные для использования другие научно-библиотечные системы.

**Подготовка к зачету** К сдаче зачета допускаются обучающиеся, выполнившие все задания (лабораторные, самостоятельные), предусмотренные учебной программой дисциплины, посетившие не менее 85% аудиторных занятий.

## VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

**Материально-техническое и программное обеспечение дисциплины**

| Наименование специальных помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
|---|---|---|
| D820 - учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (36 п.м.) | Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718. | |
| D732 - учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (45 п.м.) | Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electron, 300x173 см, размер рабочей области 290x163 Документ-камера Avervision CP 355 AF Мультимедийный проектор, Mitsubishi | |

| | | |
|---|---|---|
| | FD630U, 4000 ANSI Lumen, 1920x1080<br>Сетевая видеокамера Multipix MP-HD718<br>ЖК-панель 47", Full HD, LG M4716 CCBA<br>ЖК-панель 42", Full HD, LG M4214 CCBA<br>ЖК-панель 42", Full HD, LG M4214 CCBA. | |

Для проведения учебных занятий по дисциплине, а также для организации самостоятельной работы студентам доступно следующее лабораторное оборудование и специализированные кабинеты, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

## VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Для дисциплины «Криптографические методы защиты информации» используются следующие оценочные средства:

Устный опрос:

1. Собеседование (УО-1)
2. Презентация / сообщение (УО-3)

Письменные работы:

1. Индивидуальное домашнее задание (ПР-6)
2. Контрольная работа (ПР-3)

**Устный опрос**

Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки.

Обучающая функция состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту.

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с

изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Презентация / сообщение (УО-3) – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

**Письменные работы**

Письменный ответ приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе.

Контрольная работа (ПР-6) – средство для закрепления и практического освоения материала по определенному разделу.

Индивидуальное домашнее задание (ПР-12) – средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине.

## Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

### Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Криптографические методы защиты информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – зачёт (3-й, осенний семестр). Зачет по дисциплине включает ответы на 2 вопроса. Один из вопросов носит теоретический характер. Он направлен на раскрытие студентом знаний по «сквозным» вопросам и проблемам теории моделей. Второй вопрос носит практический характер.

### Методические указания по сдаче зачёта

Зачёт принимается ведущим преподавателем. При большом количестве групп у одного преподавателя или при большой численности потока по распоряжению директора департамента (заместителя директора по учебной и воспитательной работе) допускается привлечение в помощь ведущему преподавателю других преподавателей. В первую очередь привлекаются преподаватели, которые проводили лабораторные занятия по дисциплине в группах.

В исключительных случаях, по согласованию с заместителем директора Института по учебной и воспитательной работе, директор департамента имеет право принять зачёт в отсутствие ведущего преподавателя.

Форма проведения зачёта (устная, письменная и др.) утверждается на заседании департамента по согласованию с руководителем в соответствии с рабочей программой дисциплины.

Во время проведения зачёта студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего зачёт, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Время, предоставляемое студенту на подготовку к ответу на зачёте, должно составлять не более 20 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на зачёте посторонних лиц (кроме лиц, осуществляющих проверку) без разрешения соответствующих лиц (ректора либо проректора по учебной и воспитательной работе, директора Института, руководителя ОПОП или директора департамента) не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются на зачёт с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «зачтено» или «не зачтено», которая вносится в экзаменационную ведомость. При неявке студента на зачёт в ведомости делается запись «не явился».

## Вопросы к зачёту

1. Математическая модель шифров замены
2. Шифры перестановки
3. Поточные шифры простой замены
4. Шифр Виженера
5. Энтропия и избыточность языка
6. Теоретическая стойкость шифра
7. Совершенные шифры
8. Имитостойкость шифров
9. Принципы построения блочных шифров
10. Принципы построения поточных шифров
11. Генераторы ключевых последовательностей
12. Шифрсистема RSA
13. Шифрсистема Эль-Гамаля
14. Криптографические хеш функции

## Критерии выставления оценки студенту на зачёте

К зачёту допускаются обучающиеся, выполнившие программу обучения по дисциплине, прошедшие все этапы текущей аттестации.

| Оценка | Требования к сформированным компетенциям |
|---|---|
| **«зачтено»** | Студент показал развернутый ответ, представляющий собой связное, логическое, последовательное раскрытие поставленного вопроса, широкое знание литературы. Студент обнаружил понимание материала, обоснованность суждений, способность применить полученные знания на практике. Допускаются некоторые неточности в ответе, которые студент исправляет самостоятельно. |
| **«не зачтено»** | Студент обнаруживает незнание большей части проблем, связанных с изучением вопроса, допускает ошибки в ответе, искажает смысл текста, беспорядочно и неуверенно излагает материал. Данная оценка характеризует недостатки в подготовке студента, которые являются серьезным препятствием к успешной профессиональной и научной деятельности. |

## Оценочные средства для текущей аттестации

Текущая аттестация студентов по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме контрольных мероприятий (контрольной работы, индивидуального домашнего задания) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− результаты самостоятельной работы.

Составляется календарный план контрольных мероприятий по дисциплине. Оценка посещаемости, активности обучающихся на занятиях, своевременность выполнения различных видов заданий ведётся на основе журнала, который ведёт преподаватель в течение учебного семестра.