МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Рязанский государственный университет имени С.А. Есенина»

Утверждаю

декан физико-математического факультета

___ ___ Н.Б. Федорова

«30» августа 2018 г.

**Рабочая программа дисциплины**
**«Математические основы защиты информации и информационной безопасности»**

**Уровень основной образовательной программы:** МАГИСТРАТУРА

**Направление подготовки:** 02.04.02 Фундаментальная информатика и информационные технологии (информационные системы)

**Программа:** Информационные системы

**Форма обучения:** очная

**Сроки освоения ООП:** 2 года **(**нормативный)

**Физико-математический факультет**

**Кафедра:** Информатики, вычислительной техники и методики преподавания информатики

Рязань, 2018

# ВВОДНАЯ ЧАСТЬ

**1. Цели освоения дисциплины**

Целью освоения учебной дисциплины «Математические основы защиты информации и информационной безопасности» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения информатики и программирования для последующего применения в учебной и практической деятельности.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, математическими моделями и стандартами шифрования;
- изучение математических основ защиты информации: арифметики целых чисел, модульной арифметики, теории чисел, а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и связи;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа
- формирование современной культуры программирования.

**2. Место дисциплины в структуре ОПОП магистратуры**

**2.1.** Дисциплина «Математические основы защиты информации и информационной безопасности» относится к базовой части блока Б1.Б.2

**2.2.** Для изучения дисциплины «Математические основы защиты информации и информационной безопасности» необходимы следующие знания, умения, навыки, формируемые предшествующими дисциплинами:

- «Компьютерная графика» (вариативная часть профессионального цикла ОПОП бакалавриата по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем):
- «Математический анализ» или аналогичные дисциплины других направлений бакалавриатов
- «Информатика и программирование» или аналогичные дисциплины других направлений бакалавриатов.

**2.3.** Перечень последующих учебных дисциплин, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной:

- «Основы цифровой обработки информации» вариативной части Блока 1 данной ОПОП;
- Научно-исследовательская работа (с семинаром)

**3. Требования к результатам освоения учебной дисциплины «Математические основы защиты информации и информационной безопасности»**

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих общепрофессиональных(ОПК) и профессиональных (ПК) компетенций:

| № п/п | Номер/ индекс компе-тенции | Содержание компетенции (или ее части) | Перечень планируемых результатов обучения по дисциплине В результате изучения учебной дисциплины обучающиеся должны: | | |
|---|---|---|---|---|---|
| | | | Знать: | Уметь: | Владеть (навыками): |
| 1 | 2 | 3 | 4 | 5 | 6 |
| | ОК-2 | готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения | Основные принципы административно-правовой защиты информации | Быстро реагировать на различные угрозы информационной безопасности | Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак |
| 1 | ОПК-3 | Способность использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий | математические принципы, лежащие в основе криптографических моделей<br>теорию простых чисел и модульной арифметики<br>этапы решения задачи на компьютере; | уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования | владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования<br>владеть навыками решения задач криптоанализа и шифрования |
| 2 | ПК-2 | Способность использовать углубленные и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий. | терминологию из области криптографии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;<br>основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики;<br>математические криптологические системы, включая средства описания; | уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;<br>уметь использовать математические модели для построения криптологических систем;<br>уметь применять современные технологии создания брандмауэров и IDS-комплексов; | основными методами, способами и средствами шифрования и криптографиии;<br>навыками решения задач модульной и целочисленной арифметики, теории простых чисел<br>Приемами обнаружения вирусных угроз<br>Приемами обнаружения сетевых проникновений;<br>Навыками работы по обнаружению и защите от DDOS-атак |

| КАРТА КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ | | | | | |
|---|---|---|---|---|---|
| **НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ: МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** | | | | | |
| **Цель дисциплины** | Целями освоения учебной дисциплины «Математические основы защиты информации и информационной безопасности» является формирование у обучающихся общепрофессиональных и профессиональных компетенций в процессе изучения фундаментальной информатики и информационных технологий для последующего применения в учебной и практической деятельности | | | | |
| **Задачи (НАУЧИТЬ)** | | | | | |
| | систематизация, формализация и расширение знаний по основным положениям теории информации, математическими моделями и стандартами шифрования; | изучение математических основ защиты информации: арифметики целых чисел, модульной арифметики, теории чисел, а так же методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и связи; | дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение; | привитие навыков работы с методами шифрования и криптоанализа | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технологии формирования** | **Форма оценочного средства** | **Уровни освоения компетенций** |
| **ИНДЕКС** | **ФОРМУЛИРОВКА** | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 |
| ОК-2 | готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения | Знать Основные принципы административно-правовой защиты информации<br>Уметь Быстро реагировать на различные угрозы информационной безопасности<br>Владеть навыками Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак | Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов | Лабораторные работы, экзамен | **Пороговый**<br>Способен решать стандартные задачи информационной безопасности<br>**Повышенный**<br>Способен быстро решать задачи определения взлома и атак злоумышленников повышенной сложности |
| ОПК-3 | Способность использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий | Знать: математические принципы, лежащие в основе криптографических моделей<br>теорию простых чисел и модульной арифметики<br>этапы решения задачи на компьютере;<br>Уметь: уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования | Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов | Лабораторные работы, экзамен | **Пороговый**<br>Способен решать стандартные задачи<br>**Повышенный**<br>Способен решать задачи криптографии повышенной сложности |

| | | | | | |
|---|---|---|---|---|---|
| | | Владеть: владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования<br>владеть навыками решения задач криптоанализа и шифрования | | | |
| ПК-2 | Способность использовать углубленные и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий. | Знать: терминологию из области криптографии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений;<br>основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики;<br>математические криптологические системы, включая средства описания;<br>Уметь: уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач;<br>уметь использовать математические модели для построения криптологических систем;<br>уметь применять современные технологии создания брандмауэров и IDS-комплексов;<br>Владеть: основными методами, способами и средствами шифрования и криптографиии;<br>навыками решения задач модульной и целочисленной арифметики, теории простых чисел<br>Приемами обнаружения вирусных угроз<br>Приемами обнаружения сетевых проникновений; Навыками работы по обнаружению и защите от DDOS-атак | Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий, организации самостоятельной работы студентов | Лабораторные работы, экзамен | **Пороговый**<br>Способен находить, анализировать и контекстно обрабатывать учебную научно-техническую информацию с помощью обучающего<br>**Повышенный**<br>Способен самостоятельно находить, анализировать и контекстно обрабатывать научно-техническую информацию |

## ОСНОВНАЯ ЧАСТЬ

### 1. Объем учебной дисциплины и виды учебной работы

| Вид учебной работы | | Всего часов | Семестры |
|---|---|---|---|
| | | | № 2 |
| | | | часов |
| | | | - |
| **Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)** | | **54** | **54** |
| В том числе: | | | |
| Лекции (Л) | | 18 | 18 |
| Лабораторные работы (ЛР) | | 18 | 18 |
| Практические занятия (ПЗ) | | 18 | 18 |
| **Самостоятельная работа студента (всего)** | | **54** | **54** |
| **В том числе:** | | | |
| **СРС в семестре** | | **54** | **54** |
| Изучение литературы и других источников | | 13 | 13 |
| Подготовка к выполнению лабораторных работ | | 9 | 9 |
| Подготовка к защите лабораторных работ | | 9 | 9 |
| Подготовка к практическим занятиям | | 12.5 | 12.5 |
| Выполнение индивидуальных домашних заданий | | 10.5 | 10.5 |
| **Контроль (подготовка к экзамену)** | | **36** | **36** |
| **Вид промежуточной аттестации** | **Экзамен** | | + |
| **ИТОГО: общая трудоемкость** | **часов** | **144** | **144** |
| | **зач. ед.** | **4** | **4** |

### 2. Содержание учебной дисциплины

### 2.1. Содержание разделов учебной дисциплины

| № семестра | № раздела | Наименование раздела учебной дисциплины | Содержание раздела в дидактических единицах |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 2 | 1 | **Основные составляющие информационной безопасности** | Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Криптографические методы защиты и шифрование. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности |
| 2 | 2 | **Криптографические способы защиты информации** | Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая |

| | | | |
|---|---|---|---|
| | | | подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA |
| 2 | 3 | **Антивирусная защита** | Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы |
| 2 | 4 | **Сетевая безопасность** | Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS |

## 1.2. Разделы учебной дисциплины, виды учебной деятельности и формы контроля

| № семестра | № раздела | Наименование раздела учебной дисциплины | Виды учебной деятельности, включая самостоятельную работу студентов ( в часах) | | | | | | Формы текущего контроля успеваемости (*по неделям семестра*) |
|---|---|---|---|---|---|---|---|---|---|
| | | | Л | ЛР | ПЗ | СРС | контроль | всего | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 8 | 9 |
| 2 | 1 | **Основные составляющие информационной безопасности** | 2 | | 2 | 2 | | 6 | *1 неделя:*<br>Практическое занятие 1 |
| 2 | 2 | **Криптографические способы защиты информации** | 6 | 8 | 8 | 30 | | 52 | *2 неделя:*<br>Лабораторная работа №1<br>*3 неделя:*<br>Практическое занятие 2<br>4 неделя<br>ЛР №1<br>*5 неделя:*<br>Практическое занятие 3<br>*6 неделя*<br>ЛР №2<br>*7 неделя:*<br>Практическое занятие 4<br>*8 неделя:*<br>*9 неделя:*<br>Практическое занятие 5 |
| 2 | 3 | **Антивирусная защита** | 4 | 6 | 4 | 12 | | 26 | *10 неделя:*<br>ЛР №3<br>*11 неделя:*<br>Практическое занятие 6<br>12 неделя<br>13 неделя<br>Практическое занятие 7<br>14 неделя<br>ЛР №4 |
| 2 | 4 | **Сетевая безопасность** | 6 | 4 | 4 | 10 | | 24 | 15 неделя<br>Практическое занятие 8<br>*16 неделя:*<br>*17 неделя:*<br>Практическое занятие 9<br>*18 неделя:*<br>ЛР № 5 |
| 2 | Все | **Контроль** | | | | | 36 | 108 | **ЭКЗАМЕН** |
| | | **ИТОГО 8 семестр** | **18** | **18** | **18** | **54** | **36** | **144** | |
| | | **ИТОГО** | **18** | **18** | **18** | **54** | **36** | **144** | |

## 2.3. Лабораторный практикум

| № семестра | № раздела | Наименование раздела учебной дисциплины | Наименование лабораторных работ | Всего часов |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 2 | 1 | **Основные составляющие информационной безопасности** | ЛР по данному разделу не предусмотрена | - |
| 2 | 2 | **Криптографические способы защиты информации** | ЛР №1. *Написание, ввод, отладка и тестирование программ шифрования подстановкой* | 4 |
| | | | ЛР №2. *Написание, ввод, отладка и тестирование программ шифрования перестановкой, аналитически и гаммированием* | 2 |
| | | | ЛР № 3. *Написание, ввод, отладка и тестирование программ шифрования методом контекстного моделирования, словарными алгоритмами* | 4 |
| 2 | 3 | **Антивирусная защита** | ЛР №4. *Диагностика антивирусной программы и создание тестовых вирусов* | 4 |
| 2 | 4 | **Сетевая безопасность** | ЛР №5 *Создание цифровой подписи* | 4 |
| | | **ИТОГО 2 семестр** | | **18** |

## 2.4. Примерная тематика курсовых работ

Курсовые работы не предусмотрены по учебному плану

## 3. Самостоятельная работа студента

### 3.1. Виды СРС

| № семестра | № раздела | Наименование раздела учебной дисциплины | Виды СРС | Всего часов |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 10 | 1 | **Основные составляющие информационной безопасности** | Изучение литературы и других источников | 1 |
| | | | Подготовка к практическому занятию №1 | 0.5 |
| | | | Выполнение индивидуальных домашних заданий | 0.5 |
| 10 | 2 | **Криптографические способы защиты информации** | Изучение литературы и других источников | 5 |
| | | | Подготовка к практическому занятию №2 | 2 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| | | | Подготовка к выполнению лабораторной работы №1 по теме "Шифрование подстановкой" | 2 |
| | | | Подготовка к защите лабораторной работы (ЛР №1) | 2 |
| | | | Подготовка к практическому занятию №3 | 2 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| | | | Подготовка к выполнению лабораторной работы №2 по теме "Шифрование перестановкой, аналитически и гаммированием" | 2 |
| | | | Подготовка к защите лабораторной работы (ЛР №2) | 2 |
| | | | Подготовка к практическому занятию №4 | 2 |
| | | | Выполнение индивидуальных домашних заданий | 2 |

| | | | | |
|---|---|---|---|---|
| | | | Подготовка к выполнению лабораторной работы №3 по теме "Шифрование алгоритмами контекстного моделирования и словарными алгоритмами" | 2 |
| | | | Подготовка к защите лабораторной работы (ЛР №3) | 2 |
| | | | Подготовка к практическому занятию №5 | 2 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| 10 | 3 | **Антивирусная защита** | Изучение литературы и других источников | 4 |
| | | | Подготовка к практическому занятию №6 | 1 |
| | | | Выполнение индивидуальных домашних заданий в виде реферата | 2 |
| | | | Подготовка к выполнению лабораторной работы №4 по теме "Диагностика работы антивируса и создание тестового вируса" | 1 |
| | | | Подготовка к защите лабораторной работы №4 | 1 |
| | | | Подготовка к практическому занятию №7 | 1 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| 10 | 4 | **Сетевая безопасность** | Изучение литературы и других источников | 3 |
| | | | Подготовка к практическому занятию №8 | 1 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| | | | Подготовка к выполнению лабораторной работы №5 по теме "Создание цифровой подписи" | 2 |
| | | | Подготовка к защите лабораторной работы (ЛР №5) | 1 |
| | | | Подготовка к практическому занятию №9 | 1 |
| | | | Выполнение индивидуальных домашних заданий | 1 |
| | | **ИТОГО 2 семестр** | | **54** |
| | | **ИТОГО** | | **54** |

## 3.2. График работы студента

## Семестр №2

| Форма оценочного средства | Усл. Обозн. | НЕДЕЛЯ | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | сессия |
| Лабораторная работа | ЛР | | | | + | | + | | | + | + | | | | + | | | | + | |
| Практическое занятие | ПЗ | | + | | | + | | + | | | | + | | + | | + | | + | | |
| Экзамен | Э | | | | | | | | | | | | | | | | | | | + |

**Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Математические основы защиты информации и информационной безопасности»**

| **Темы и разделы дисциплины** | **Учебно-методическое обеспечение для соответствующих тем и разделов** |
|---|---|

| | |
|---|---|
| **1.Основные составляющие информационной безопасности** | http://www.intuit.ru/ Криптографические основы безопасности Автор: О.Р. Лапонина http://www.intuit.ru/ Математика криптографии и теория шифрования Автор: Б.А. Фороузан Переводчик: А.Н. Берлин |
| **2.Криптографические способы защиты информации** | |
| **3.Антивирусная защита** | Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003 |
| **4.Сетевая безопасность** | |

## 4. Оценочные средства для контроля успеваемости и результатов освоения учебной дисциплины (*см. Фонд оценочных средств*)

### 4.2. Рейтинговая система оценки знаний обучающихся по учебной дисциплине

*Рейтинговая система не используется.*

## 5. Учебно-методическое и информационное обеспечение дисциплины

### 5.1. Основная литература

| № | Наименование<br>Авторы<br>Год, место издания | Используется при изучении разделов | семестр | Количество экземпляров | |
|---|---|---|---|---|---|
| | | | | В библиотеке | На кафедре |
| 1 | Конеев, Искандер. Информационная безопасность предприятия [Текст] / И.Конеев, А.Беляев. - СПб. : БХВ-Петербург, 2003. - 752с. : ил. - ISBN 5-94157-280-88 : 218-30. | 1-4 | 8 | 15 | 1 |
| 2 | Штарьков, Ю. М. Универсальное кодирование: Теория и алгоритмы [Электронный ресурс] / Ю. М. Штарьков. – М. : Физматлит, 2013. – 280 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=275569 (дата обращения 15.06.2018). | 1-4 | 8 | ЭБС | |

### 5.2. Дополнительная литература

| № | Наименование<br>Авторы<br>Год, место издания | | | Используется при изучении разделов | семестр | Количество экземпляров | |
|---|---|---|---|---|---|---|---|
| | | | | | | В библиотеке | На кафедре |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | Буза, М. К. Архитектура компьютеров [Электронный ресурс] : учебник / М. К. Буза. – Минск : Вышэйшая школа, 2015. – 416 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=449925 (дата обращения 15.06.2018). | | | 1 | 8 | ЭБС | - |
| 2 | Внуков, А. А. Защита информации [Электронный ресурс] : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М. : Издательство Юрайт, 2017. – 261 с. – Режим доступа: https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1 (дата обращения 20.06.2018). | | | 1-2 | 8 | ЭБС | - |
| 3 | Долозов, Н. Л. Программные средства защиты информации [Электронный ресурс] : конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический | | | 3-4 | 8 | ЭБС | - |

| | | | | | |
|---|---|---|---|---|---|
| | университет. – Новосибирск : НГТУ, 2015. – 63 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438307 (дата обращения 15.06.2018). | | | | |
| 4 | Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения 15.06.2018). | 1-4 | 8 | ЭБС | - |
| 5 | Осокин, А. Н. Теория информации [Электронный ресурс] : учебное пособие для прикладного бакалавриата / А. Н. Осокин, А. Н. Мальчуков. – М. : Издательство Юрайт, 2017. – 205 с. – Режим доступа: https://www.biblio-online.ru/book/1D5E1FA9-0F42-4040-A1F4-269E2063616F (дата обращения 20.06.2018). | | 8 | ЭБС | |
| 6 | Петренко, В. И. Теоретические основы защиты информации же [Электронный ресурс] : учебное пособие / В. И. Петренко ; Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации. – Ставрополь : СКФУ, 2015. – 222 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=458204 (дата обращения 15.06.2018). | 2-4 | 8 | ЭБС | - |
| 7 | Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения 15.06.2018). | 4 | 8 | ЭБС | - |

### 5.3. Базы данных, информационно-справочные и поисковые системы

1. BOOK.ru [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://www.book.ru (дата обращения: 20.06.2018).
2. East View [Электронный ресурс] : [база данных]. – Доступ к полным текстам из сети РГУ имени С.А. Есенина. – Режим доступа: https://dlib.eastview.com (дата обращения: 20.06.2018).
3. Moodle [Электронный ресурс] : среда дистанционного образования / Ряз.гос.ун-т. – Рязань, [Б.г.]. – Доступ, после регистрации из сети РГУ имени С.А. Есенина. – Режим доступа: https://e-learn2.rsu.edu.ru/moodle2 (дата обращения: 20.06.2018).
4. Znanium.com [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://znanium.com (дата обращения: 20.06.2018).
5. Труды преподавателей [Электронный ресурс] : коллекция // Электронная библиотека Научной библиотеки РГУ имени С.А. Есенина. – Режим доступа к полным текстам по паролю: http://dspace.rsu.edu.ru/xmlui/handle/123456789/3 (дата обращения: 01.06.2018).
6. Университетская библиотека ONLINE [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: http://biblioclub.ru/index.php?page=main_ub_red (дата обращения: 01.06.2018).
7. Электронный каталог диссертаций [Электронный ресурс] : официальный сайт / Рос.гос.б-ка. – Москва : Рос.гос.б-ка, 2003. – Доступ к полным текстам из комплексного читального зала НБ РГУ имени С.А. Есенина. – Режим доступа: http://diss.rsl.ru (дата обращения: 01.06.2018).
8. Юрайт [Электронный ресурс] : электронная библиотека. – Доступ к полным текстам по паролю. – Режим доступа: https://www.biblio-online.ru (дата обращения: 20.06.2018).

**5.4. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины**

1. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 01.06.2018).
2. КиберЛенинка [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://cyberleninka.ru, свободный (дата обращения: 01.06.2018).
3. Википедия [Электронный ресурс] : свободная энцикл. – Режим доступа: http://ru.wikipedia.org/wiki, свободный (дата обращения: 01.06.2018).
4. ИНТУИТ [Электронный ресурс] : Национальный Открытый Университет. – Режим доступа: http://www.intuit.ru, свободный (дата обращения: 01.06.2018).
5. Российский общеобразовательный портал [Электронный ресурс] : [образовательный портал]. – Режим доступа: http://www.school.edu.ru, свободный (дата обращения: 15.06.2018).
6. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] : федеральный портал. – Режим доступа: http://school-collection.edu.ru, свободный (дата обращения: 15.06.2018).
7. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео [Электронный ресурс] / Д. Ватолин [и др.]. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с. – Режим доступа: http://www.compression.ru/book, свободный (дата обращения: 15.06.2018).
8. Сэломон, Д. Сжатие данных, изображения и звука [Электронный ресурс] / Д. Сэломон. – М.: Техносфера, 2004. – 367 с. – Режим доступа: http://da.kalinin.ru/books/salmon.pdf, свободный (дата обращения: 15.06.2018).

## 6. Материально-техническое обеспечение дисциплины

**6.1. Требования к аудиториям для проведения занятий:**

Класс персональных компьютеров под управлением MS Windows XP Pro/7/8/10, включенных в локальную сеть университета с возможностью выхода в Internet.

Стандартно оборудованные лекционные аудитории с мультимедиапроектором, подключенным к компьютеру, настенным экраном.

**6.2. Требования к оборудованию рабочих мест преподавателя и обучающихся:**

Персональный компьютер под управлением MS Windows XP Pro/7/8/10, Microsoft Office, системы программирования Turbo-Pascal и Turbo-C++, Delphi, комплект архиваторов, файлов для архивации, антивирус.

## 7. Образовательные технологии *(Заполняется только для стандарта ФГОС ВПО)*

## 8. Методические указания для обучающихся по освоению дисциплины

| Вид учебных занятий | Организация деятельности студента |
|---|---|
| Лекция | Освоение дисциплины идет с помощью объектно-ориентированных сред языков программирования. Учитывая, что курс выстроен по разделам, большинство из которых охватывает теоретические вопросы, преподавателю необходимо соблюсти баланс между количеством материала на самостоятельную работу и лабораторными работами.<br>Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в |

| | |
|---|---|
| | рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям*:*<br>*Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Цифровая подпись. Установление подлинности объекта. Управление ключами. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. угрозы, атаки, целостность, аутентификация, конфиденциальность, доступность, хэш-функции, антивирусы, сигнатуры, эвристический анализ, брандмауэры, шифрование перестановкой, подстановкой, гаммирование* |
| Лабораторная работа | Лабораторные работы, предложенные в данном курсе, выстраиваются в схему практического освоения алгоритмов криптографии и изучения антивирусной защиты, на изучение которых и нацелены.<br>В лекционной части курса описание работы в антивирусных системах не предусмотрено, поэтому рекомендуется преподавателям давать задание на самостоятельный поиск и изучение сетевого антивирусного ПО. Наилучшим вариантом может служить предоставление лабораторных работ в виде практикума с непременной практико-теоретической частью в электронном виде, где были бы представлены практические приемы работы, описание основных инструментов архивации, необходимых для выполнения задания конкретной темы лабораторной работы.<br>В соответствии с запланированным на самостоятельную работу временем (раздел 3.1) изучить соответствующий теоретический материал и практические рекомендации.<br>В соответствии с запланированным на самостоятельную работу временем составить схемы алгоритмов и программы решения соответствующего варианта учебной задачи.<br>Согласовать заранее составленные схемы и программы с преподавателем, ведущим занятие. Тексты программ должны содержать короткие комментарии, отражающие тему и номер лабораторной работы, номер варианта, фамилию студента, связь тех или иных переменных с условием задачи, а также комментарии, отражающие основные шаги алгоритмов.<br>Защитить оформленную лабораторную работу, продемонстрировав теоретические и практические знания, умения и навыки по соответствующей теме. |
| Практическое занятие | Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, прослушивание аудио- и видеозаписей по заданной теме, решений задач по алгоритму и др. |
| Подготовка к экзамену | При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, типовые практические задания и др. |

## 9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для организации учебной и самостоятельной работы обучаемых используется технология удаленного доступа. Для каждой из учебных групп на сервере кафедры ИВТ и МПИ созданы каталоги с соответствующими правами доступа. В каталоге группы создан подкаталог для данной учебной дисциплины, в котором по мере необходимости преподавателем размещаются рабочая программа дисциплины, электронные варианты лекций, электронные обучающие ресурсы, задания к лабораторным работам, графики выполнения лабораторных работ, материалы для самостоятельной работы, контрольные материалы, оценки текущих результатов учебной деятельности обучающихся и др.

материалы для организации учебного процесса по данной дисциплине. Материалы, размещенные в каталоге группы доступны любому обучающемуся соответствующей группы посредством локальной компьютерной сети университета с любого рабочего места компьютерных классов кафедры ИВТ и МПИ.

В каталоге группы также для каждого обучающегося создан личный подкаталог, к которому разрешен доступ только обучающемуся и преподавателям кафедры. В личном подкаталоге обучающийся размещает результаты своей учебной деятельности: выполненные лабораторные работы, отчеты и другие результаты.

## 10. Требования к программному обеспечению учебного процесса

| № п/п | Наименование раздела учебной дисциплины (модуля) | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
|---|---|---|
| 1 | 2 | 3 |
| 1 | Все разделы дисциплины, для которых проводятся практические занятия, семинары и лекции. | 1. Антивирус Kaspersky Endpoint Security (договор №14/03/2018-0142от 30/03/2018г.);<br>2. Офисное приложение Libre Office (свободно распространяемое ПО);<br>3. Архиватор 7-zip (свободно распространяемое ПО);<br>4. Браузер изображений Fast Stone ImageViewer (свободно распространяемое ПО);<br>5. PDF ридер Foxit Reader (свободно распространяемое ПО);<br>6. Медиа проигрыватель VLC mediaplayer (свободно распространяемое ПО);<br>7. Запись дисков Image Burn (свободно распространяемое ПО);<br>8. DJVU браузер DjVuBrowser Plug-in (свободно распространяемое ПО);<br>9. Microsoft Office Professional Plus 2010, согласно Microsoft Open License* № 45472941 (от 18/05/2009, авторизационный номер лицензиата 65463391ZZE1105), срок действия бессрочно |
| **2** | Все разделы дисциплины, для которых проводится самостоятельная работа студента | 1. Операционная система WindowsPro (договор №Tr000043844 от 22.09.15г.);<br>2. Антивирус Kaspersky Endpoint Security (договор №14/03/2018-0142от 30/03/2018г.);<br>3. Офисное приложение Libre Office (свободно распространяемое ПО);<br>4. Архиватор 7-zip (свободно распространяемое ПО);<br>5. Браузер изображений Fast Stone ImageViewer (свободно распространяемое ПО);<br>6. PDF ридер Foxit Reader (свободно распространяемое ПО);<br>7. Медиа проигрыватель VLC mediaplayer (свободно распространяемое ПО);<br>8. Запись дисков Image Burn (свободно распространяемое ПО);<br>9. DJVU браузер DjVuBrowser Plug-in (свободно распространяемое ПО);<br>10. Microsoft Office Professional Plus 2010, согласно Microsoft Open License* № 45472941 (от 18/05/2009, авторизационный номер лицензиата 65463391ZZE1105), срок действия бессрочно |
| **3** | Все разделы дисциплины, для | 1. Операционная система WindowsPro (договор №Tr000043844 от 22.09.15г.); |

| | | |
|---|---|---|
| | которых проводятся лабораторные работы | 2. Антивирус Kaspersky Endpoint Security (договор №14/03/2018-0142от 30/03/2018г.);<br>3. Офисное приложение Libre Office (свободно распространяемое ПО);<br>4. Архиватор 7-zip (свободно распространяемое ПО);<br>5. Браузер изображений Fast Stone ImageViewer (свободно распространяемое ПО);<br>6. PDF ридер Foxit Reader (свободно распространяемое ПО);<br>7. Медиа проигрыватель VLC mediaplayer (свободно распространяемое ПО);<br>8. Запись дисков Image Burn (свободно распространяемое ПО);<br>9. DJVU браузер DjVuBrowser Plug-in (свободно распространяемое ПО);<br>10. Microsoft Office Professional Plus 2010, согласно Microsoft Open License* № 45472941 (от 18/05/2009, авторизационный номер лицензиата 65463391ZZE1105), срок действия бессрочно |

**11. Иные сведения**

Нет

**Приложение 1**

**Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

Паспорт фонда оценочных средств по дисциплине
для промежуточного контроля успеваемости

| № п/п | Контролируемые разделы (темы) дисциплины (результаты по разделам) | Код контролируемой компетенции) или её части) | Наименование оценочного средства |
|---|---|---|---|
| 1 | **Основные составляющие информационной безопасности** | ОПК 3<br>ПК-2 | Экзамен |
| 2 | **Криптографические способы защиты информации** | | |
| 3 | **Антивирусная защита** | | |
| 4 | **Сетевая безопасность** | | |

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

| Индекс компе-тенции | Содержание компетенции | Элементы компетенции | Индекс элемента |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| ОК-2 | готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения | Знать | |
| | | Знать Основные принципы административно-правовой и программной защиты информации | ОК-2 З1 |
| | | Уметь | |
| | | Уметь Быстро реагировать на различные угрозы информационной безопасности | ОК-2 У1 |
| | | Владеть | |
| | | Владеть навыками Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак | ОК-2 В1 |
| ОПК-3 | Способность использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий | Знать | |
| | | З1 математические принципы, лежащие в основе криптографических моделей<br>теорию простых чисел и модульной арифметики | ОПК-3 З1 |
| | | З2 этапы решения задачи на компьютере | ОПК-3 З2 |
| | | Уметь | |
| | | использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования | ОПК-3 У1 |
| | | Владеть | |
| | | В1 владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования | ОПК-3 В1 |
| | | В2 владеть навыками решения задач криптоанализа и шифрования | ОПК-3 В2 |
| ПК-2 | Способность использовать углубленные и практические знания в области информационных технологий и прикладной математики, фундаментальных | Знать | |
| | | З1 Знать: терминологию из области криптографии, шифрования, антивирусной защиты, сетевой защиты, защиты от вторжений | ПК-2 З1 |
| | | З2 основные алгоритмы шифрования для решения задач предметной области, их особенности и характеристики;<br>З3 математические криптологические системы, включая средства описания | ПК-2 З2<br>ПК2 З3 |
| | | Уметь | |
| | | У1. уметь выбирать, адаптировать и применять | ПК-2 У1 |

| | | | |
|---|---|---|---|
| | концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий. | необходимые алгоритмы при решении профессиональных задач; | |
| | | У2 уметь использовать математические модели для построения криптологических систем; | ПК-2 У2 |
| | | У3 уметь применять современные технологии создания брандмауэров и IDS-комплексов; | ПК-2 У3 |
| | | Владеть | |
| | | В1 Владеть: основными методами, способами и средствами шифрования и криптографиии | ПК-2 В1 |
| | | В2 навыками решения задач модульной и целочисленной арифметики, теории простых чисел | ПК-2 В2 |
| | | В3 Приемами обнаружения вирусных угроз | ПК-2 В3 |
| | | В4 Приемами обнаружения сетевых проникновений; Навыками работы по обнаружению и защите от DDOS-атак | ПК-2 В4 |

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЕТ)

| Содержание оценочного средства | Индекс оцениваемой компетенции и ее элементов |
|---|---|
| 1. Основные понятия информационной безопасности. Классификация угроз. | ПК-2 З1 ПК-2 У3 ОК-2 З1 ОК-2 У1 ОК-2 В1 |
| 2. Целостность и конфиденциальность. Классификация средств защиты информации. | ПК-2 З1 ПК-2 У3 ОК-2 З1 ОК-2 У1 ОК-2 В1 |
| 3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. | ОПК-3 З2 ПК-2 З1 ПК-2 У3 ОК-2 З1 ОК-2 У1 ОК-2 В1 |
| 4. Словарные методы кодирования. Алгоритм LZ77 | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 |
| 5. Словарные методы кодирования. Алгоритм LZSS | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 |
| 6. Методы Лемпеля-Зива. Алгоритм LZW. | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 |
| 7. Преобразование Барроуза-Уилера (BWT) | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 |
| 8. Базовые понятия теории информации. | ОПК-3 З1 ПК-2 З1 |
| 9. Измерение дискретной информации. Энтропия Шеннона. | ОПК-3 З1 ПК-2 З1 |
| 10. Методы и средства организационно-правовой защиты информации. | ПК-2 З1 ОК-2 З1 ОК-2 У1 |
| 11. Методы и средства инженерно-технической защиты. | ПК-2 З1 ПК-2 В4 ОК-2 З1 ОК-2 У1 |
| 12. Формулы мультипликативных шифров. Аффинные шифры. Криптоанализ аффинного шифра. | ОПК-3 З1 ПК2 З3 |
| 13. Модель сетевой безопасности. Классификация сетевых атак. | ПК-2 З1 ПК-2 У3 ПК-2 В4 ОК-2 З1 ОК-2 У1 |
| 14. Контекстное моделирование | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 ПК2 З3 |
| 15. Сервисы и механизмы безопасности | ПК-2 З1 ПК-2 В3 ПК-2 В4 |
| 16. Модель сетевого взаимодействия, модель безопасности информационной системы | ПК-2 З1 ПК-2 В3 ОК-2 З1 ОК-2 У1 |
| 17. Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка; | ОПК-3 З2 ОПК-3 У1 ОПК-3 В1 ПК-2 З2 ПК-2 У2 ПК-2 В1 ПК2 З3 |
| 18. Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная одноконтурная обыкновенная подстановка( Таблицы Вижинера)**.** | ОПК-3 З2 ОПК-3 У1 ОПК-3 В1 ПК-2 З2 ПК-2 У2 ПК-2 В1 ПК2 З3 |
| 19. Простые криптосистемы. Шифрование методом замены (подстановки): Шифрование многоалфавитной одноконтурной монофонической подстановкой. | ОПК-3 З2 ОПК-3 У1 ОПК-3 В1 ПК-2 З2 ПК-2 У2 ПК-2 В1 ПК2 З3 |
| 20. Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная многоконтурная подстановка. | ОПК-3 З2 ОПК-3 У1 ОПК-3 В1 ПК-2 З2 ПК-2 У2 ПК-2 В1 |
| 21. Арифметика целых чисел. НОД и алгоритм | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |

| | |
|---|---|
| Евклида Бинарные операции. | |
| 22. Расширенный алгоритм Евклида . Линейные диофантовы уравнения. | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 23. Модульная арифметика. Операции по модулю. Система вычетов. Сравнения. Инверсии. | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 24. Шифрование методом перестановки: Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 ПК-2 У2 ПК-2 В1 ПК2 З3 |
| 25. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 ПК-2 У2 ПК-2 В1 |
| 26. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Алгоритм шифрования данных IDEA. | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 ОК-2 В1 ПК2 З3 |
| 27. Стандарт шифрования данных RSA | ОПК-3 З2 ОПК-3 У1 ПК-2 З2 ПК-2 В2 |
| 28. Арифметика простых чисел. Phi-функция Эйлера. Малая теорема Ферма. Теорема Эйлера. | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 29. Генерация простых чисел. Простые числа Мерсенны. Простые числа Ферма | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 30. Испытание простоты чисел. Алгоритм теории делимости. AKS-алгоритм | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 31. Испытание простоты чисел. Вероятностные алгоритмы. Испытание квадратным корнем. Метод Ферма разложения на множители | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 32. Основы работы антивирусных программ: Сигнатурный анализ. Приведите примеры использования | ОПК-3 З2 ПК-2 З1 ПК-2 В3 ОК-2 З1 |
| 33. Эвристический анализ при работе антивирусных программ | ОПК-3 З2 ПК-2 З1 ПК-2 В3 |
| 34. Основные приемы криптоанализа при симметричных ключах. Виды атак. Принцип Керкгоффса. | ОПК-3 З2 ОПК-3 В2 ПК-2 З2 ОК-2 У1 |
| 35. Формулы аддитивных шифров. Криптоанализ. | ОПК-3 З2 ОПК-3 В2 ПК-2 З2 ПК-2 В1 ПК2 З3 |
| 36. Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети. | ПК-2 З1 ПК-2 У3 ПК-2 В3 ОК-2 З1 ОК-2 В1 |
| 37. Принципы организации централизованного управления антивирусной защитой. Компоненты системы удаленного управления. | ОПК-3 В1 ПК-2 У3 ПК-2 В3 ОК-2 З1 ОК-2 У1 ОК-2 В1 |
| 38. Брандмауэры. Определение типов брандмауэров. | ОПК-3 У1 ПК-2 У3 ПК-2 В4 |
| 39. Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры | ПК-2 З1 ПК-2 У3 ПК-2 В4 |
| 40. Криптосистемы Рабина | ОПК-3 З1 ОПК-3 З2 ПК-2 З2 ПК-2 В1 ПК2 З3 |
| 41. Криптографическая система Эль-Гамаля | ОПК-3 З1 ОПК-3 З2 ПК-2 З2 ПК-2 В1 ПК2 З3 |
| 42. Эллиптические кривые в вещественных числах. Криптосистемы на основе метода эллиптических кривых | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |

| | |
|---|---|
| 43. Алгебраические структуры алгебр: группы, кольца и поля. | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 44. Алгебраические структуры алгебр. Использование полиномов | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 45. Алгебраические структуры: теорема Лагранжа | ОПК-3 З1 ПК-2 У2 ПК-2 В2 |
| 46. Блочные шифры как групповые математические перестановки Полноразмерные ключевые шифры транспозиции | ОПК-3 У1 ОПК-3 В1 ОПК-3 В2 ПК-2 З2 ПК-2 У2 ПК2 З3 |
| 47. Шифр Плейфера и его криптоанализ. | ОПК-3 З2 ОПК-3 В1 ОПК-3 В2 ПК-2 З2 ПК-2 У2 ПК2 З3 |
| 48. Одноразовый блокнот и роторные шифры. Устройство и принцип работы шифровальной машины «Энигма» | ОПК-3 У1 ОПК-3 В1 ПК-2 З2 ПК-2 В1 ПК2 З3 |
| 49. Основные приемы криптоанализа при асимметричных ключах | ОПК-3 З2 ОПК-3 В2 ПК-2 З2 ПК-2 У2 ПК-2 В1 ПК2 З3 |
| 50. Базовые методы и алгоритмы стеганографии | ОПК-3 З2 ОПК-3 В2 ПК-2 З1 ПК-2 З2 ПК-2 У2 ПК2 З3 |

## ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

(Шкалы оценивания)

Результаты выполнения обучающимся заданий на зачете оцениваются на экзамене по пятибалльной шкале.

В основе оценивания лежат критерии порогового и повышенного уровня характеристик компетенций или их составляющих частей, формируемых на учебных занятиях по дисциплине «Математические основы защиты информации и информационной безопасности» (Таблица 2.5 рабочей программы дисциплины).

**«Отлично» (5)** – оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

**«Хорошо» (4)** - оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

**«Удовлетворительно» (3)** - оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

**«Неудовлетворительно» (2)** - оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.