МИНОБРНАУКИ РОССИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**
декан факультета прикладной
математики, информатики
и механики

_____А. И. Шашкин
*подпись, расшифровка подписи*
23.05.2020

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
# Б1.Б.51.05 Математические основы защиты информации и информационной безопасности

**1. Код и наименование направления подготовки/специальности:**

10.05.01 Компьютерная безопасность

**2. Профиль подготовки/специализация:**

математические методы защиты информации

**3. Квалификация (степень) выпускника:**

Специалист по защите информации

**4. Форма обучения:**

очная

**5. Кафедра, отвечающая за реализацию дисциплины:**

ERP-систем и бизнес-процессов

**6. Составители программы:**

Воронков Борис Николаевич, к. т. н., доцент кафедры ERP-систем и бизнес-процессов

**7. Рекомендована:**

Научно-методическим советом факультета прикладной математики, информатики и механики 23.05.2020 г., протокол № 9

_____
*отметки о продлении вносятся вручную)*

**8. Учебный год:** 2023/2024 **Семестр(ы):** 8

**9**. **Цели и задачи учебной дисциплины:** Цель дисциплины – сформировать у обучающихся знания по обеспечению информационной безопасности информационно-управляющих и информационно-логистических систем. Задачи дисциплины: дать обучающимся необходимые знания, умения и навыки, в том числе: теоретические и практические проблемы обеспечения информационной безопасности информационно-управляющих и информационно-логистических систем; навыки самостоятельного, творческого использования теоретических знаний для предотвращения незаконного использования информации в практической деятельности

**10. Место учебной дисциплины в структуре ООП:** Дисциплина «Математические основы защиты информации и информационной безопасности» входит в дисциплины специализации учебного плана и изучается в 8-ом семестре.

| № п/п | Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы |
|---|---|
| 1. | Б1.Б.44 Криптографические методы защиты информации |
| 2. | Б1.Б.51.04 Криптографические протоколы |

**11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):**

| Компетенция | | Планируемые результаты обучения |
|---|---|---|
| Код | Название | |
| ПСК-2.1. | способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации. | Знание вычислительных алгоритмов, реализующих современные математические методы защиты информации.<br>Умение решать задачи факторизации и дискретного логарифмирования.<br>Владение навыками программной реализации криптографических алгоритмов. |

**12. Объем дисциплины в зачетных единицах/час.**(*в соответствии с учебным планом)* – 3/108.

**Форма промежуточной аттестации***(зачет/экзамен)* зачёт с оценкой.

## 13. Виды учебной работы

| Вид учебной работы | Трудоёмкость (часы) | | | | | |
|---|---|---|---|---|---|---|
| | Всего | В том числе в интерактивной форме | По семестрам | | | |
| | | | 8 | | | |
| Аудиторные занятия | 48 | | 48 | | | |
| в том числе: лекции | 16 | | 16 | | | |
| Практические | 0 | | 0 | | | |
| Лабораторные | 32 | | 32 | | | |
| Самостоятельная работа | 60 | | 60 | | | |
| Контроль | | | | | | |
| Итого: | 108 | | 108 | | | |
| Форма промежуточной аттестации | | | ЗаО | | | |

## 13.1. Содержание дисциплины

| № п/п | Наименование раздела дисциплины | Содержание раздела дисциплины |
|---|---|---|
| 1 | Элементы теории чисел и модулярная арифметика | Теорема Эйлера и малая теорема Ферма; вычисление обратных по модулю величин |
| 2 | Криптосистемы Эль Гамаля и RSA | Дискретный логарифм, задачи факторизации |
| 3 | Математические модели шифрования с использованием конечных полей | Первообразные корни, поля Галуа |
| 4 | Идеальные криптосистемы | Теоремы Шеннона, ограничения на использование теоретически-стойких криптосистем |
| 5 | Математические методы аутентификации и хэширования | Однонаправленные функции, алгоритмы электронных подписей и формирования хэш-функций |
| **2. Практические занятия** не предусмотрены | | |
| **3. Лабораторные работы** | | |
| 3.1 | Лабораторная работа №1 Тема: Алгоритм Евклида и расширенный алгоритм Евклида. | *Теоретические сведения*<br>1. Теорема и алгоритм деления.<br>2. Алгоритм Евклида.<br>3. Расширенный алгоритм Евклида.<br>4. Оценка сложности алгоритмов.<br>*Практическая часть*<br>1. Реализация алгоритмов.<br>2. Подготовка и защита отчёта по лабораторной работе. |
| 3.2 | Лабораторная работа №2 Тема: Алгоритм быстрого возведения в степень по модулю. | *Теоретические сведения*<br>1. Квадратичный алгоритм.<br>2. Алгоритм без двоичного представления.<br>*Практическая часть*<br>1. Реализация и исследование алгоритмов.<br>2. Подготовка и защита отчёта по лабораторной работе. |
| 3.3 | Лабораторная работа №3 Тема: Алгоритмы факторизации. | *Теоретические сведения*<br>1. Метод пробных делений.<br>2. Алгоритм факторизации Ферма.<br>*Практическая часть*<br>1. Реализация алгоритмов в виде приложения<br>2. Подготовка и защита отчёта по лабораторной работе. |

### 13.2. Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование раздела дисциплины | Виды занятий (часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Практ. | Лаб. раб. | Самостоятельная работа | Всего |
| 1 | Элементы теории чисел и модулярная арифметика. | 4 | | 8 | 16 | 28 |
| 2 | Криптосистемы Эль Гамаля и RSA. | 4 | | 8 | 14 | 26 |
| 3 | Математические модели шифрования с использованием конечных полей. | 4 | | 8 | 10 | 22 |
| 4 | Идеальные криптосистемы | 2 | | 2 | 8 | 12 |
| 5 | Математические методы аутентификации и хэширования | 2 | | 6 | 12 | 20 |
| | Итого: | 16 | | 32 | 60 | 108 |

### 14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой библиографии, итоговое повторение теоретического материала. Подготовка отчётов по лабораторным работам и подготовка к зачёту с оценкой.

### 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

*(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

| № п/п | Источник |
|---|---|
| *1.* | *Рябко Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия – Телеком, 2012. – 229 с. –(URL: e.lanbook.com) (ЭБС издательства Лань, дата обращения: 02.06.2016)* |
| *2.* | *Ишмухаметов Ш. Т. Математические основы защиты информации: электронное учебное пособие / Ш. Т. Ишмухаметов, Р. Г. Рубцова. – Казань: Казанский федеральный университет, 2012. – 139 с. –(URL: e.lanbook.com) (ЭБС издательства Лань, дата обращения: 02.06.2016)* |
| *3.* | *Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с.* |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| *1.* | *Воронков Б. Н. Методическое пособие по разработке средств защиты информации в вычислительных сетях / Б. Н. Воронков, В. И.Тупота. – Воронеж : ВГУ, 2000. – 112 с.* |
| *2.* | *Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; Под ред. В. Ф. Шаньгина. –2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376с.* |
| *3.* | *Воронков Б. Н. Криптографические методы защиты информации : учеб. пособие для вузов / Б. Н. Воронков. – Воронеж : ИД ВГУ, 2018. – 113 с.* |

в) информационные электронно-образовательные ресурсы**:**

| № п/п | Источник |
|---|---|
| *4* | https://e.lanbook.com/ - ЭБС «Лань» |
| *5* | *www.lib.vsu.ru — Зональная научная библиотека ВГУ* |

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

### 16. Перечень учебно-методического обеспечения для самостоятельной работы

*(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным

программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам.

## 17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Windows7. Мультимедийные лекционные демонстрации. Презентации на базе конспекта лекций.

## 18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

## 19. Фонд оценочных средств:

### 19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

| Код и содержание компетенции | Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков) | Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование) | ФОС* (средства оценивания) |
|---|---|---|---|
| ПСК-2.1. Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации | Знание вычислительных алгоритмов, реализующих современные математические методы защиты информации. | Раздел 1. Элементы теории чисел и модулярная арифметика<br>Раздел 2. Криптосистемы Эль Гамаля и RSA | Устный опрос, лабораторные работы |
| | Умение решать задачи факторизации и дискретного логарифмирования. | Раздел 3. Математические модели шифрования с использованием конечных полей.<br>Раздел 4. Идеальные криптосистемы.<br>Раздел 5. Математические методы аутентификации и хэширования | Устный опрос, лабораторные работы |
| | Владение навыками программной реализации криптографических алгоритмов. | Разделы 2, 4, 5 | Защита отчетов по лабораторным работам |
| **Промежуточная аттестация** | | | Комплект КИМ |

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

### 19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

**Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.**

Для оценивания результатов обучения на зачёте с оценкой используется – шкала и критерии оценивания в соответствии с таблицей.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

| Компетенция | Показатель сформированности компетенции | Шкала и критерии оценивания уровня освоения компетенции | | | |
|---|---|---|---|---|---|
| | | 5 | 4 | 3 | 2 |
| ПСК-2.1.. Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации. | Знание вычислительных алгоритмов, реализующих современные математические методы защиты информации. | Сформированные знания | Сформированные знания, но содержащие отдельные пробелы | Неполные знания | Фрагментарные знания или их отсутствие |
| | Умение решать задачи факторизации и дискретного логарифмирования. | Сформированные умения | Успешные умения, но содержащие отдельные пробелы | Успешные, но не системные умения | Фрагментарные умения или отсутствие умений |
| | Владение навыками программной реализации криптографических алгоритмов. | Сформированные умения | Успешные умения, но содержащие отдельные пробелы | Успешные, но не системные умения | Фрагментарные умения или отсутствие умений |

**19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы**

### 19.3.1 Примеры контрольных вопросов и заданий:

1. Теорема Эйлера и малая теорема Ферма.
2. Квадратичные вычеты.
3. Вычисление обратных по модулю величин.
4. Китайская теорема об остатках.
5. Алгоритм Гарнера.
6. Расширенный алгоритм Евклида.
7. Алгоритмы факторизации.
8. Однонаправленные функции.
9. Цифровая подпись.
10. Алгоритм Диффи-Хеллмана.

### 19.3.2. Примеры заданий к лабораторной работе

1. Ознакомиться с алгоритмами нахождения НОД и НОК.
2. Изучить методы оценки сложности алгоритмов.
3. Реализовать алгоритм Евклида и расширенный алгоритм.
4. Оценить сложности алгоритмов..
5. Ответить на контрольные вопросы.
6. Составить отчёт о проделанной работе.

**19.3.3. Пример контрольно-измерительного материала**

**УТВЕРЖДАЮ**

заведующий кафедрой
*ERP-систем и бизнес-процессов*
_____ Й. Беккер
*подпись, расшифровка подписи*
_03.06.2019

Направление подготовки / специальность ___10.05.01_Компьютерная безопасность
*шифр, наименование*
Дисциплина__Криптографические протоколы_____

Вид контроля _____зачёт с оценкой_____
*промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы*

Контрольно-измерительный материал №_1_

1. Вычислительно-трудные задачи в криптографии.

2. Алгоритм Диффи-Хеллмана.

Преподаватель _____ .____
*подпись расшифровка подписи*

**19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций**

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторные работы; тестирования. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по вопросам компьютерной безопасности.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.