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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев
(подпись)
03.07.2018

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

**Б1.Б.31 Криптографические методы защиты информации**
*Код и наименование дисциплины в соответствии с Учебным планом*

**1. Шифр и наименование направления подготовки/специальности:**
10.05.04 Информационно-аналитические системы безопасности

**2. Профиль подготовки/специализации:** Информационная безопасность финансовых и экономических структур

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

**4. Форма образования:** Очная

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

**6. Составители программы:**
Шабров Сергей Александрович, канд. Физ.-мат. наук, доцент

**7**. **Рекомендована:** Научно-методическим Советом математического факультета протокол №0500-07 от 03.07.2018г.
*(наименование рекомендующей структуры, дата, номер протокола)*

**8. Учебный год:** 2018/2019 **Семестр(-ы): 6**

**9. Цели и задачи учебной дисциплины:**
Основной целью дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, основными алгоритмами шифрования и криптографическими протоколами обмена информацией.

**10. Место учебной дисциплины в структуре ООП:**
Дисциплина «Криптографические методы защиты информации» является базовой дисциплиной основного раздела Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 10.05.04 «Информационно-аналитические системы безопасности».

**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 | |
| ОК – 8 | способность к самоорганизации и самообразованию | знать: основные определения, понятия и идеи изучаемых разделов курса.<br>уметь: выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности.<br>владеть: математическим аппаратом, необходимым для самообразования. |
| ОПК – 7 | способностью применять методы и средства обеспечения информационной безопасности специальных ИАС | знать**:** этапы разработки компьютерных моделей систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования, технологии организации и проведения статистического компьютерного моделирования компьютерных систем.<br>уметь: анализировать адекватность модели и результаты модельного эксперимента, сопоставляя получаемые и планируемые результаты.<br>владеть: практическими навыками применения средств и технологий; создания, планирования эксперимента и тестирования компьютерных моделей сложных систем (массового обслуживания, передачи информации, конфликтного взаимодействия систем). |

**12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —** 2/72.
**Форма промежуточной аттестации - экзамен**

**13. Виды учебной работы:**

| Вид учебной работы | Трудоемкость (часы) | | | | |
|---|---|---|---|---|---|
| | Всего | По семестрам | | | |
| | | 6 сем. | | | |
| Аудиторные занятия | 36 | 36 | | | |
| в том числе: лекции | 18 | 18 | | | |
| практические | | | | | |
| лабораторные | 18 | 18 | | | |

| | | | | | |
|---|---|---|---|---|---|
| Самостоятельная работа | 36 | 36 | | | |
| Контрольные работы | | | | | |
| Итого: | 72 | 72 | | | |

### 13.1 Содержание разделов дисциплины: 13.1. Содержание дисциплины

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины |
|---|---|---|
| | | **1. Лекции** |
| 1.1 | История развития криптографии. Основные понятия | Основные понятия криптографии. Стойкость шифров. Теоретическая и практическая стойкость криптосистем. Обобщенная схема для криптосистем с закрытыми ключами шифрования. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Основы криптоанализа. История создания частотного анализа. Одноалфавитный шифр. Многоалфавитные шифры. Омофонический шифр замены. Диграф. Великий шифр. Шифр Билля. Шифр Виженера. Взлом шифра Виженера. |
| 1.2 | Математические основы криптографии | Понятие вычета по модулю. Понятие сравнимости двух чисел. Введение в конечные поля. Понятие группы. Операции в группах. Кольцо. Поле. Поле Галуа. Неприводимые многочлены.<br>Простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Мультипликативность функции. Китайская теорема об остатках. Теорема Ферма. Функция Эйлера. Теорема Эйлера. Алгоритм Евклида. Расширенный алгоритм Евклида. Показатели и первообразные корни. Дискретные логарифмы. Генераторы случайных чисел. Проверка качества работы ГСЧ. Преобразование Уолша–Адамара. Эллиптические кривые. Тесты числа на простоту. Принципы построения больших простых чисел. Алгоритм Адлемана–Ленстры. Разложение составных чисел на множители. |
| 1.3 | Надежность шифров. Основы теории К. Шеннона | Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. «Ненадёжность шифра» и «расстояние единственности». Практически стойкие шифры. |
| 1.4. | Хеш-функции | Понятие хеш-функции. Коллизия. Хеш-функции Наорра и Юнга. Проверка целостности информации с использованием хеш-функций. Нахождение коллизий хеш-функций в общем случае. Парадокс о днях рождения. Атака «встреча посередине» для хеш-функций. Линейное разделение секрета. |
| 1.5 | Введение в криптографические методы защиты информации | Особенности криптографических методов защиты информации. Криптология, криптография и криптоанализ. Шифромашины. Основные понятия криптографии: шифра, алгоритма шифрования, ключа шифрования, криптосистемы. Атаки на шифр. Правило Керкхоффа. Стойкость шифра. Зависимость криптографии от уровня технологий. |

| 3 Лабораторные занятия | | |
|---|---|---|
| 3.1 | Системы симметричного шифрования | Простейшие шифры и их свойства, шифры замены и перестановки, композиции шифров. Блочные и поточные (потоковые) шифры. Алгоритмы шифрования на основе сетей Фейстеля. Стандарты шифрования данных DES, AES и ГОСТ 28147-89. Режимы работы блочных шифров. Алгоритмы Lucifer, IDEA, Blowfish. Потоковые шифры A5 и RC4. |
| 1.2 | Системы асимметричного шифрования | Криптография с открытыми ключами. Односторонние функции. Алгоритм Диффи-Хеллмана обмена ключевой информацией. Криптосистема RSA.<br>Криптографические протоколы. Проблемы криптографических протоколов. Последние достижения в криптоанализе. |
| 3.3 | Электронная цифровая подпись. Открытое распространение ключей | Электронная цифровая подпись: требования к цифровой подписи, стандарт DSS, прямая цифровая подпись, технологии арбитражной цифровой подписи. Криптографические функции хеширования.<br>Отечественные стандарты криптографической защиты информации ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ Р34.10-2001.<br>Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты. Протоколы и механизмы аутентификации на основе открытых ключей и сертификатов (стандарт ITU-T X.509). |
| 3.4 | Криптографические методы защиты информации в телекоммуникационных сетях | Угрозы безопасности и способы информационной защиты в сети Интернет. Протоколы передачи данных с применением криптографических средств и средств аутентификации.<br>Средства электронной цифровой подписи. Системы защищенного электронного документооборота.<br>Системы электронной безопасности в финансовой сфере. Аутентификация данных на картах. Статическая и динамическая аутентификация. |

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

| № п/п | Наименование раздела дисциплины | Виды занятий (часов) | | | | |
|---|---|---|---|---|---|---|
| | | Лекции | Практические | Лабораторные | Самостоятельная работа | Всего |
| 01 | Понятие криптографического протокола | 6 | | 6 | 10 | 22 |
| 02 | Аутентификация и ключи | 6 | | 8 | 13 | 27 |
| 03 | Криптографические стандарты | 6 | | 4 | 13 | 23 |

## 14. Методические указания для обучающихся по освоению дисциплины

*(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)*

Перечень вопросов, содержащихся в рабочей программе дисциплины, может быть изложен с различной степенью глубины в соответствии с объемом часов на самостоятельную работу студентов.

**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 | **Гашков, Сергей Борисович**. Криптографические методы защиты информации : [учебное пособие для студ. вузов, обуч. по направлению "Приклад. математика и информатика" и "Информ. технологии"] / С.Б. Гашков, Э.А. Применко, М.А. Черепнев .— М. : Академия, 2010 .— 297, [1] с |
| 2 | **Рябко, Борис Яковлевич**. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| 1 | **Молдовян, Н.А.** Введение в криптосистемы с открытым ключом : учебное пособие / Н.А. Молдовян, А.А. Молдовян .— СПб. : БХВ-Петербург, 2005 .— 286 с |
| 2 | **Мао, Венбо**. Современная криптография : теория и практика / Венбо Мао ; пер. с англ. и ред. Д.А. Клюшина .— М. [и др.] : Вильямс, 2005 .— 763 с |
| 3 | Горбатов, В.С. Основы технологии PKI / В. С. Горбатов, О.Ю. Полянская. – М.: Горячая линия – Телеком, 2004 |

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

| № п/п | Источник |
|---|---|
| 4 | Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/) |
| 5 | http://www.machinelearning.ru/ - профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных |

**16. Перечень учебно-методического обеспечения для самостоятельной работы** *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

| № п/п | Источник |
|---|---|
| 6 | Практикум по курсу "Моделирование систем" [Электронный ресурс] : учебно-методическое пособие для вузов : [для студ. 4-5 курсов фак. компьютер. наук днев. и вечер. формы обу- чения; для направлений: 230200 - Информ. системы, 230400 - Информ. системы и техно- логии; специальности, 230201 - Информ. системы и технологии]. Ч. 1,2 / Воронеж. гос. ун-т ; сост.: А.А. Сирота, Е.Ю. Митрофанова , М.А. Дрюченко .— Электрон. текстовые дан. — Воронеж : Издательско-полиграфический центр Воронежского государственного универси- тета, 2013 |
| 7 | Алгазинов, Эдуарт Константинович. Анализ и компьютерное моделирование информаци- онных процессов и систем : [учебное пособие для студ. вузов, обуч. по специальности 080801 "Приклад. информатика" и др. междисциплинар. специальностям] / Э.К. Алгазинов, А.А. Сирота ; под общ. ред. А.А. Сироты .— М. : Диалог-МИФИ, 2009 .— 416 с. : ил .— Библиогр. в конце разд. — ISBN 978-5-86404-233-5 |

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

---

**18. Материально-техническое обеспечение дисциплины:**

Доска, мел, тряпка, учебные пособия, компьютер

---

**19. Фонд оценочных средств:**

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

| Код и содержание компетенции (или ее части) | 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) |
|---|---|---|---|
| ОК – 8 способность к самоорганизации и самообразованию | знать: основные определения, понятия и идеи изучаемых разделов курса | Раздел 1. | |
| | уметь: выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности | Раздел 2 | |
| | владеть: математическим аппаратом, необходимым для самообразования | Раздел 4. | Контрольная работа |
| ОПК – 7 способностью применять методы и средства обеспечения информационной безопасности специальных ИАС | знать**:** этапы разработки компьютерных моделей систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования, технологии организации и проведения статистического компьютерного моделирования компьютерных систем | Все разделы | |
| | уметь: анализировать адекватность модели и результаты модельного эксперимента, сопоставляя получаемые и планируемые результаты | Все разделы | |
| | владеть: практическими навыками применения средств и технологий; создания, планирования эксперимента и тестирова- | Все разделы | |

| | | | |
|---|---|---|---|
| | ния компьютерных моделей сложных систем (массового обслуживания, передачи информации, конфликтного взаимодействия систем) | | |
| **Промежуточная аттестация** | | | КИМ |

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

| *Критерии оценивания компетенций* | Уровень сформированности компетенций | Шкала оценок |
|---|---|---|
| Ответ на контрольно-измерительный материал соответствует одному или более чем одному из перечисленных показателей, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует знание учебного материала, возможно с некоторыми ошибками. | Пороговый уровень и выше порогового | *зачтено* |
| Ответ на контрольно-измерительный материал не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или отсутствие их. | | *не зачтено* |

**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 Перечень вопросов к экзамену:**

| № | |
|---|---|
| 1 | Математические описания систем и моделей систем в рамках теоретико-множественного подхода. |
| 2 | Системы и проблемы. Системный подход и системный анализ. Качественные и количественные методы. |
| 3 | Общая методика системного анализа применительно к проектированию информационных и информационно-измерительных систем. |
| 4 | Задачи анализа и синтеза систем. Эволюционная технологическая схема синтеза сложных систем. |
| 5 | Метод анализа иерархий. Технология структурирования целей при разработке системы. Использование МАИ на начальной стадии разработки системы. |
| 6 | Морфологические методы и генерация альтернативных вариантов системы. |
| 7 | Современные информационно-аналитические технологии структурного системного анализа. |
| 8 | Объектно-ориентированный анализ и моделирование систем. |
| 9 | Обоснование структуры трехрубежной системы информационной безопасности организации. |
| 10 | Типовые математические схемы элементов сложной системы |
| 11 | Комбинированный подход. Математическая схема агрегата. Гибридные |

| | |
|---|---|
| | автоматы. |
| 12 | Метод статистических испытаний Монте-Карло. Способы организации модельного времени и квазипараллелизма имитационной модели. |
| 13 | Моделирование случайных величин с заданным законом распределения. Датчики случайных чисел. |
| 14 | Моделирование случайных величин с произвольным законом распределения. |
| 15 | Языки и инструментальные средства имитационного моделирования. |
| 16 | Принципы моделирования информационного конфликта систем. |

**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 форме *устного опроса и контрольной работы.* 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.

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