**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Факультет **Информатики и Информационных технологий**

# Рабочая программа дисциплины

## «Криптографические протоколы»

Кафедра **Информатики и Информационных технологий**

**Образовательная программа**

10.03.01 Информационная безопасность

**Профиль подготовки:**

Безопасность компьютерных систем

**Уровень высшего образования**:

бакалавриат

**Форма**

**обучения**:

очная

**Статус дисциплины:**

базовая

**Махачкала 2020**

Рабочая программа дисциплины «Криптографические протоколы» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 – Информационная безопасность, уровень подготовки: бакалавриат, утвержденного приказом Минобрнауки РФ от 1 декабря 2016 г. №1515.

Составитель: Ахмедова Написат Мурадовна, старший преподаватель кафедры информатики и информационных технологий

Рабочая программа дисциплины одобрена:
на заседании кафедры ИиИТ эт «13» _03_2020г., протокол № 8

Зав. кафедрой _____ Ахмедов С.А.
(подпись)

на заседании Методической комиссии факультета ИиИТ

от от «_12_» _03_2020__г., протокол №_8_.

председатель _____ Ахмедова З.Х.

Рабочая программа дисциплины согласована с учебно-методическим управлением «16» 03 2020 г. _____
(подпись)

**Аннотация рабочей программы дисциплины.**

Дисциплина Криптографические протоколы защиты информации входит в базовую часть образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете информатики и информационных технологий ДГУ кафедрой информатики и информационных технологий.

Содержание дисциплины охватывает круг вопросов, связанных с защитой информации путем математических преобразований с помощью криптографических алгоритмов.

Дисциплина нацелена на формирование следующих компетенции ОК-5, ОПК-7, ПК-1 выпускника.

Преподавание дисциплины предусматривает проведение следую- щих видов учебных занятий: лекции, практические занятия, лаборатор- ные работы самостоятельная работа студентов.

Рабочая программа дисциплины предусматривает проведение следую- щих видов контроля: текущий контроль успеваемости в форме опросов, защиты расчетных заданий и промежуточный контроль в форме экзаме- на.

Дисциплина реализуется на 4 курсе, в 8 семестре.

Объем дисциплины 4 зачетные единицы, в том числе в академических часах по видам учебных занятий:

| Се-местр | Учебные занятия | | | | | | | Форма про-межуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | в том числе | | | | | | | |
| | Контактная работа обучающихся с преподавателем | | | | | | СРС, в том числе экзамен | |
| | Всего | из них | | | | | | |
| | | Лекции | Лабораторные занятия | Практические занятия | | консультации | | |
| 8 | 144 | 14 | 28 | 20 | | | 82 | экзамен |

## 1. Цели освоения дисциплины

Учебная дисциплина «Криптографические протоколы» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

**Основной целью** дисциплины «Криптографические протоколы» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

**Задачи** дисциплины «Криптографические протоколы»:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

Для изучения данной дисциплины студент должен иметь знания по следующим курсам:

1) Дискретная математика;
2) Теория информации;
3) Теория вероятностей и математическая статистика.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина Криптографические протоколы защиты информации входит в базовую часть образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность. Дисциплина реализуется на 4 курсе, в 8 семестре. Объем дисциплины 4 зачетные единицы.

Аудиторные занятия включают в себя лекции и лабораторные занятия. Самостоятельная работа студентов состоит в самостоятельном изучении отдельных тем по учебной программе. Письменные лабораторные занятия и самостоятельная работа оцениваются и комментируются по мере выполнения.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения)

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

| Код компетенции из ФГОС ВО | Наименование компетенции из ФГОС ВО | Планируемые результаты обучения |
|---|---|---|
| ОК-5 | способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | **Знает:** требования к шифрам и основные характеристики шифров; **Умеет:** применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности **Владеет:** навыками использования ПЭВМ в анализе простейших шифров |
| ОПК-7 | способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | **Знает:** основные задачи и понятия криптографии; **Умеет:** использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; **Владеет:** криптографической терминологией; |
| ПК-1 | способность выполнять работы по установке, настройкеи обслуживанию программных, программно-аппаратных (в том чис- | **Знает:** модели шифров и математические методы их исследования; **Умеет:** для проектирования, разработки и оценки |

| | | |
|---|---|---|
| | ле криптографических) и технических средств защиты информации | защищенности компьютерных систем;<br>**Владеет**:<br>навыками математического моделирования в криптографии |

## 4. Объем, структура и содержание дисциплины

Объем дисциплины составляет 4 зачетных единицы, 144 академических часа.

### Структура дисциплины

| № раз-дела | Наименование разделов и тем | Количество часов | | | | | | Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | | | Внеауд. работа СР | |
| | | | Л | ПЗ | ЛР | | | |
| **Модуль 1. Простые шифры** | | | | | | | | |
| 1 | **Лекция 1.** Введение в криптографию | | 2 | 2 | | | 6 | |
| 1 | **Лекция 2.** Шифр Цезаря. Шифр простой замены. | | | 2 | 2 | | 6 | устный и письменный опросы |
| 1 | **Лекция 3.** Шифр Виженера. Частотный анализ. | | 2 | 2 | 2 | | 10 | коллоквиум |
| | **Итого за модуль 1** | | 4 | 6 | 4 | | 22 | |
| **Модуль 2. Шифрование с закрытым ключом** | | | | | | | | |
| 2 | **Лекция 4.** Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ. | 12 | 2 | 2 | 4 | | 8 | устный и письменный опросы |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | **Лекция 5.** Шифры программирования. Композиции шифров. | | 2 | 2 | 6 | | 10 | устный и письменный опрос |
| | **ИТОГО за модуль 2** | | 4 | 4 | 10 | | 18 | |
| **Модуль 3. Блочные шифры** | | | | | | | | |
| 3 | **Лекция 6.** Сеть Фейстеля | | 2 | 4 | 2 | | 2 | устный и письменный опрос |
| 3 | **Лекция 7.** DES/3DES | | 2 | 2 | 6 | | 2 | устный и письменный опрос |
| 3 | **Ktrwbz 8.** AES | | 2 | 4 | 6 | | 2 | устный и письменный опрос |
| | **Итого за модуль 3** | | 6 | 10 | 14 | | 6 | |
| **Модуль 4. Экзамен** | | | | | | | | |
| | | | | | | | 36 | |
| | **ВСЕГО;** | **144** | **14** | **20** | **28** | | **82** | |

**Содержание дисциплины, структурированное по темам (разделам)**

**Содержание лекционных занятий по дисциплине**

**Модуль1. Криптография.**

Основные понятия криптографии. Введение в криптографию. Криптографические атаки. Криптографический протокол.

Шифр Цезаря. Методы замены

**Модуль 2. Шифры с закрытым ключом.**

Простейшие методы шифрования с закрытым ключом.

Методы перестановки. 2.3.Понятие композиционного шифра.

**Модуль 3. Алгоритмы шифрования DES и AES. Хеширование.**

2.2. Принципы построения блочных шифров с закрытым ключом. Режимы работы блочных шифров. Сеть Фейштеля.
Алгоритмы шифрования DES и AES. Общие сведения. Шифрование и расшифрование.
Криптографические хеш-функции. Понятие хеш-функции. Обзор алгоритмов формирования хеш-функций.

**Модуль 4. Шифры с открытым ключом. Алгоритм RSA. Электронная цифровая подпись. Криптостойкость и имитостойкость шифров.**
3.4. Шифры с открытым ключом. Односторонние функции. Использование ассиметричных алгоритмов для шифрования.
Алгоритм RSA. Основные сведения. Пример вычислений по алго- ритму.
Практическое использование алгоритма RSA.

Электронная цифровая подпись

Криптостойкость и имитостойкость шифров.

**Темы лабораторных работ**

1. Шифрование с закрытым ключом незнакомого теста.
2. Программная реализация шифра Цезаря.
3. Одноалфавитная замена. Пропорциональные шифры.
4. Многоалфавитные подстановки, методы гаммирования.
5. Методы перестановки. Понятие композиционного шифра.
6. Программная реализация шифра Вижинера.
7. Поточные шифры.
8. DES-шифрование.
9. Использование алгоритма хеширования для сокрытия содержимого файла.

**Темы практических занятий**

1. Использование алгоритма хеширования для подтверждения неизменности файла.
2. Base-64.
3. Кодирование бинарных зашифрованных файлов в base 64.
4. Создание цифровых сертификатов.
5. Применение электронной цифровой подписи для проверки авторства.
6. Применение электронной цифровой подписи для проверки неизменности файла.

7. Безопасное хранение файлов с применением криптоконтейнеров.
8. Скрытия факта передачи шифрованного текста (стеганография).
9. Создание файловой системы с поддержкой прозрачного шифрования.

## 5. Образовательные технологии

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

Подготовка студентами докладов по темам, не входящим в план лекций, а также выполнение расчетных работ, позволяют расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов.

### Темы для самостоятельного изучения:

| Наименование темы: | Вид работы: | № занятия | Количество часов |
|---|---|---|---|
| 1.Инструментальные средства и библиотеки для реализации криптографических алгоритмов | Изучение функций библиотек GNU MP и GNU Crypto по технической документации | 1,2 | 10 |
| 2. Теоретико-числовые методы в криптографии. Вычисления в простых полях и кольцах целых чисел | Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях: Алгоритмические аспекты поиска больших простых чисел | 3-4 | 20 |

| | | | |
|---|---|---|---|
| | Подготовка к практическим занятиям | | |
| 3.Система Диффи-Хеллмана, шифр Шамира, шифр Эль-Гамаля (по выбору) | Выполнение расчетного задания в виде компьютерной программы по темам | 5-6 | 10 |
| 4.Сложность дискретного логарифмирования и наиболее быстрые алгоритмы. | Изучение разделов дисциплины по учебной литературе, в том числе вопросов, неосвещаемых на лекциях. Подготовка к практическим занятиям | 7-8 | 10 |
| 5.Шифр RSA, подпись RSA, шифр Рабина (по выбору) | Выполнение расчетного задания в виде компьютерной программы по темам. | 9 | 10 |
| 6.Теория секретных систем Шеннона и современные подходы к теоретико-информационной секретности | Выполнение расчетного задания в виде компьютерной программы по теме: реализация простейших омофонных кодов и их применение для построения идеальной криптосистемы для сообщений, порождаемых источником без памяти с неизвестной статистикой. | 10 | 22 |

**Рекомендуемая литература**

а) основная литература:

1. Замятина Е.Б. Современные теории имитационного моделирования: Специальный курс. - Пермь: ПГУ, 2007. - 119 с.

2. Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. 3-е издание. М.: Вильямс, 2011, 832 с.

3. Емельянов, В. В. Имитационное моделирование систем: учеб. пособие / В. В. Емельянов, С. И. Ясиновский. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2009. - 583с.

4. Карпов, Ю. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5: монография / Ю. Карпов. - СПб. : БХВ- Петербург, 2009. - 390с. + CD.

б) дополнительная литература:

1. Schruben L. Simulation modelling with event graphs. // Communication of the ACM, Vol. 26, N. 11, 1983, P. 957-963.

2. Concepcion A.I., Zeigler B.P. DEVS-formalism: a framework for hierarchical model development. // IEEE trans. on soft. eng. vol.14, n.2, 1987, P. 228-241.
3. Боев В.Д. Моделирование систем. Инструментальные средства GPSS World. - СПб.: БХВ-Петербург, 2004. - 368 с.

в) учебно-методическая литература:

1. Родионов А.С. Имитационное моделирование на ЭВМ. Избранные лекции. Учебное пособие. - Новосибирск: НГУ, 1999. - 84 с.
2.Родионов А.С. Распределенное моделирование цифровых систем связи // Материалы международного семинара «Перспективы развития современных средств и систем телекоммуникаций-99», Хабаровск, 5-10 июля 1999. - Новосибирск, 1999. - С. 105-109.
3.Родионов А.С. О генерации случайных структур сетей // Труды ИВМиМГ СО РАН. Сер. Информатика. Вып. 4., - 2002. - С. 123-137.
4.Rodionov A.S., Choo H., Youn H.Y. “Process simulation using randomized Markov chain and truncated marginal distribution”, Supercomputing, 2002, No. 1, P. 69-85.

## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

| Код компетенции из ФГОС ВО | Наименование компетенции из ФГОС ВО | Планируемые результаты обучения | Процедура освоения |
|---|---|---|---|
| ОК-5 | способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной без- | **Знает:** требования к шифрам и основные характеристики шифров; **Умеет:** применять отечественные и зарубежные стандарты в области криптографических методов компьютерной | - круглый стол |

| | | | |
|---|---|---|---|
| | опасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | безопасности<br>**Владеет:**<br>навыками использования ПЭВМ в анализе простейших шифров | |
| ОПК-7 | способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | **Знает:**<br>основные задачи и понятия криптографии;<br>**Умеет:**<br>использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;<br>**Владеет:**<br>криптографической терминологией; | собеседование, дискуссия |
| ПК-1 | способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | **Знает:**<br>модели шифров и математические методы их исследования;<br>**Умеет:**<br>для проектирования, разработки и оценки защищенности компьютерных систем; | собеседование,дискуссия |

| | | | |
|---|---|---|---|
| | | **Владеет**: навыками математического моделирования в криптографии | |

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

Текущий балл студента по дисциплине состоит из оценок по видам учебной деятельности, включающим: выполнение контрольных и домашних работ, посещение лекционных занятий. Оценки по видам учебной деятельности (максимально100 баллов):
- посещение лекций – 2 балла за каждое занятие (максимально 9 баллов);
- выполнение контрольных работ – 5 баллов за каждую работу (максимально 20 баллов за 4 работы);
- выполнение лабораторных работ – 90 баллов за каждую работу (максимально 80 баллов за 8 работ);
- выполнение семестровой работы – максимально 30 баллов.

Рубежная оценка по дисциплине выставляется в соответствии с результатами тестирования.
Максимально – 100 баллов.

Соотношение между семестровой оценкой успеваемости студента по дисциплине в баллах и их числовыми и буквенными эквивалентами устанавливается согласно таблице.

Перевод баллов из 100-балльной шкалы в числовой и буквенный эквивалент

| **Сумма баллов для дисциплины** | **Оценка** | **Буквенный эквивалент** |
|---|---|---|
| 86 – 100 | 5 | Отлично |
| 66 – 85 | 4 | Хорошо |
| 51 – 65 | 3 | удовлетворительно |

| | | |
|---|---|---|
| 0 – 50 | 2 | неудовлетвори-тельно |

## 8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

### Основная литература

**1.** Гашков, Сергей Борисович. Криптографические методы защиты информации [Текст] : учеб. пособие для студентов вузов, обуч. по направлению "Прикл. мат. и информ." и "Информ. технологии" / Гашков, Сергей Борисович, Э. А. Применко. - М. : Академия, 2010. - 297,[7] с. - (Высшее профессиональное образование. Информационная безопасность)

**2.** Торстейнсон, Питер. Криптография и безопасность в технологии .NET [Текст] / Торстейнсон, Питер, Г. А. Ганеш ; пер. с англ. В.Д.Хорева; под ред. С.М.Молявко. - М. : БИНОМ. Лаб. знаний, 2007. - 479 с. : ил. - (Программисту). - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8 : 380-00.

**3.** Аграновский А.В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2009. — 256 с. — 5-98003-002-6. — Режим па: http://www.iprbookshop.ru/8641.html [Дата обращения 12 июня 2018г]

### Дополнительная литература

1. Расторгуев, Сергей Павлович. Основы информационной безопасности [Текст]: учеб. пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 978-5-7695-3098-2 : 150-70.
2. Ященко,В.В. Варновский, Н.П, Введение в криптографию. Новые математические дисциплины [Текст] : Учебник / В.В.Ященко, Н.П.Варновский, Ю.В.Нестеренко и др.; Под ред. В.В.Ященко. - СПб.: Питер, 2001. - 287 с. - ISBN 5-318-00443-1.
3. Земор Ж. Курс криптографии [Электронный ресурс] / Ж. Земор. — Электрон. текстовые данные. — Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований,

2006. — 256 c. — 5-93972-510-4. — Режим па: http://www.iprbookshop.ru/16547.html [Дата обрашения 12 июня 2018г]

## 9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. eLIBRARY.Ru [ Электронный ресурс]: электронная библиотека / Науч. электр. б-ка.- МОСКВА.1999. – Режим доступа: http//elibrary.ru (дата обращения 15.04.2020). – Яз. рус., англ.\
2. Электронный каталог НБ ДГУ Ru [ Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа: http//elib.dgu.ru. свободный (дата обращения 11.03.2020)
3. Национальный Открытый Университете «ИНТУИТ» [ Электронный ресурс]:электронно-библиотечная система, издательство «Лань» - www.intuit.ru (дата обращения 12.03.2020)

## 10. Методические указания для обучающихся по освоению дисциплины

Практические занятия по дисциплине «Криптографические методы защиты информации» служат для получения практических навыков по применению теоретических знаний, полученных студентами на лекциях, для решения конкретных задач в профессиональной сфере специалистов в области защиты информации.

Решения задач фиксируются с помощью реализованных программ на различных языках программирования(Delphi, Pascal, C, C++) .

Для более полного понимания целей, задач и практических результатов теории систем следует:

1) Ознакомиться с дополнительной литературой, особенно с трудами основоположников.
2) Ознакомиться, хотя бы поверхностно, с другими подходами к построению систем (см. доп. литературу).

3) Попытаться в рамках практических и лабораторных занятий самостоятельно и полностью выполнить все задания.

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

Учебная аудитория, оборудованная мультимедиа проектором. Компьютер под управлением операционной системы Windows 7, 8.0, 8.1, имеющий установленный пакет офисных программ MSOffice 2010, 2013 и Microsoft Visual Studio.

## 12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

а) Мультимедийная аудитория - для лекций;
б) Компьютерный класс, оборудованный для проведения практических работ
средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет – для практических занятий.
Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном. Для проведения практических занятий требуется аудитория на группу студентов, оборудованная интерактивной доской, мультимедийным проектором с экраном. Для проведения практических занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ:
1. Microsoft Office
2. Microsoft Visual Studio.