МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный университет»
(ФГБОУ ВО «КубГУ»)

Факультет компьютерных технологий и прикладной математики
Кафедра информационных технологий


РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
**Б1.О.01 «КРИПТОГРАФИЯ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»**

Направление подготовки 02.04.02 Фундаментальная информатика и информационные технологии
(код и наименование направления подготовки/специальности)

Направленность (профиль) "Интеллектуальные системы и технологии "
(наименование направленности (профиля) специализации)

Программа подготовки академическая
(академическая /прикладная)

Форма обучения очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника магистр
(бакалавр, магистр, специалист)

Краснодар 2022

Рабочая программа дисциплины Б1.О.01 - Криптография и сетевая безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии»

Программу составил(и):

В.О. Осипян, проф., доктор физ.-мат. наук _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины «Криптография и сетевая безопасность» утверждена на заседании кафедры анализа данных и искусственного интеллекта№10 от «18» мая 2022 г.

Заведующий кафедрой (разработчика)

А.В. Коваленко подпись

---

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики, протокол №6 от «25 » мая 2022 г.

Председатель УМК факультета _____ А.В. Коваленко

Рецензенты:
Бегларян М. Е., зав. кафедрой социально-гуманитарных и естественнонаучных дисциплин СКФ ФГБОУВО «Российский государственный университет правосудия», канд. физ.-мат. наук, доцент

Рубцов Сергей Евгеньевич, кандидат физико-математических наук, доцент кафедры математического моделирования ФГБГОУ «КубГУ»

# 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

## 1.1. Цель освоения дисциплины

Цели изучения дисциплины «Криптография и сетевая безопасность» определены федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению 02.04.02 Фундаментальная информатика и информационные технологии направленность (профиль) " Интеллектуальные системы и технологии " в рамках которой преподается дисциплина.

## 1.2. Задачи дисциплины

Основной задачей освоения дисциплины является овладение студентами знаниями и практическими навыками, необходимыми для проектирования и разработки безопасных информационных систем и и криптографических систем защиты информации.

## 1.3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Криптография и сетевая безопасность» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана. Для изучения дисциплины необходимо знание материала университетского курса по алгебре, дискретной математике и криптографии.. Знания, получаемые при изучении дисциплины «Криптография и сетевая безопасность», используются при изучении таких дисциплин учебного плана магистра как «Интеллектуальные информационные системы и технологии», «Спецсеминар», «Методы извлечения информации из сетевых источников», «Вероятностные модели компьютерных сетей», научно-исследовательская работа, технологическая(проектно-технологическая) практика.

## 1.4. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Процесс освоения дисциплины направлен на формирование следующих компетенций:

| Код и наименование индикатора* | Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))* |
|---|---|
| **ОПК-1. Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.** | |
| ОПК-1.1. Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций. | Знает основы построения математических моделей систем защищенной передачи информации. |
| ОПК-1.2. Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты. | Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты как основы построения криптографических алгоритмов. |
| ОПК-1.3. Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности. | Имеет практический опыт работы с решением задач теории чисел, статистического анализа, дискретной математики. |
| **ОПК-2. Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.** | |
| ОПК-2.1. Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включенного в Единый Реестр Российских программ. | Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО по защите информации, включенного в Единый Реестр Российских программ. |
| ОПК-2.2. Умеет анализировать типовые языки программирования, составлять программы. | Умеет анализировать типовые языки программирования и выбирать наилучший для реализации конкретного алгоритмы защиты информации, составлять программы безопасной передачи и хранения данных. |
| ОПК-2.3. Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов коммуникации. | Имеет практический опыт решения задач анализа, интеграции программного обеспечения сетевой безопасности в действующие информационные и программные системы, анализа типов коммуникации. |
| **ОПК-3. Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования.** | |

| Код и наименование индикатора* | Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))* |
|---|---|
| ОПК-3.1. Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей. | Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей систем безопасности данных |
| ОПК-3.2. Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем. | Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем с учетом требований к безопасности информации |
| ОПК-3.3. Имеет практический опыт применения разработки программного обеспечения и тестирования программных продуктов. | Имеет практический опыт применения разработки программного обеспечения, реализующего или использующего современные криптографические протоколы |

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 2.1. Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 5 зач.ед. (180 часов), их распределение по видам работ представлено в таблице (для студентов ОФО)

| Вид работы | Всего часов | Форма обучения | | | |
|---|---|---|---|---|---|
| | | Очная | | очно-заочная | заочная |
| | | 1 семестр (часы) | X семестр (часы) | X семестр (часы) | X курс (часы) |
| **Контактная работа в том числе:** | 36,3 | 36,3 | | | |
| **Аудиторные занятия (всего):** | 36 | 36 | | | |
| В том числе: | | | | | |
| Занятия лекционного типа | 18 | 18 | | | |
| Занятия семинарского типа (семинары, практ. занятия) | | | | | |
| Лабораторные занятия | 18 | 18 | | | |
| **Иная контрольная работа** | 0,3 | 0,3 | | | |
| Контроль самостоятельной работы | | | | | |
| Промежуточная аттестация (ИКР) | 0,3 | 0,3 | | | |
| **Самостоятельная работа, в том числе** | 108 | 108 | | | |
| В том числе: | | | | | |
| Курсовая работа | | | | | |
| *Проработка учебного (теоретического) материала* | 40 | 40 | | | |
| *Выполнение индивидуальных заданий (подготовка сообщений, презентаций)* | 50 | 50 | | | |
| *Реферат* | | | | | |
| *Подготовка к текущему* | 18 | 18 | | | |

| Вид работы | | Всего часов | Форма обучения | | | |
|---|---|---|---|---|---|---|
| | | | Очная | | очно-заочная | заочная |
| | | | 1 семестр (часы) | X семестр (часы) | X семестр (часы) | X курс (часы) |
| *контролю* | | | | | | |
| **Контроль:** | | 35,7 | 35,7 | | | |
| Подготовка к экзамену | | 35,7 | 35,7 | | | |
| Общая трудоемкость | в час | 180 | 180 | | | |
| | в т.ч. контактная работа | 36,3 | 36,3 | | | |

**2.2. Содержание дисциплины:**

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в _1__семестре *(очная форма)*

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | | Внеаудиторная работа |
| | | | Л | ПЗ | ЛР | СРС |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. | Базовые понятия и история развития информационной безопасности. | 22 | 2 | | 2 | 18 |
| 2. | Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем. | 22 | 2 | | 2 | 18 |
| 3. | Шифры замены. Шифры перестановки. Шифры гаммирования. | 22 | 2 | | 2 | 18 |
| 4. | Блочные системы шифрования. | 26 | 4 | | 4 | 18 |
| 5. | Поточные системы шифрования. | 26 | 4 | | 4 | 18 |
| 6. | Идентификация. Цифровые подписи. | 26 | 4 | | 4 | 18 |
| | ИТОГО по разделам дисциплины | 144 | 18 | | 18 | 108 |
| | Контроль самостоятельной работы (КСР) | | | | | |
| | Промежуточная аттестация (ИКР) | 0,3 | | | | |
| | Подготовка к текущему контролю | 35,7 | | | | |
| | Общая трудоемкость по дисциплине | 180 | | | | |

Примечание: Л – лекции, КСР – контрольные и самостоятельные работы, ЛР – лабораторные занятия, СРС – самостоятельная работа студента, Д-доклад, РГЗ – расчетно-графическое задание.

## 2.3. Содержание разделов дисциплины:

### 2.3.1. Занятия лекционного типа

| № | Наименование раздела | Содержание раздела | Форма текущего контроля |
|---|---|---|---|
| 1 | 1 | 3 | 4 |
| 1. | Базовые понятия и история развития информационной безопасности. | Защита информации. Угрозы информационной безопасности. Угрозы информационной безопасности. | ЛР |
| 2. | Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем. | Конечные поля. Характеристика поля. Мультипликативная группа конечного поля. Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности. | ЛР |
| 3. | Шифры замены. Шифры перестановки. Шифры гаммирования. | Математическая модель шифра замены. Классификация шифров замены. Поточные шифры простой замены. Криптоанализ поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Дисковые многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки. Элементы криптоанализа шифров перестановки. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы. | ЛР |
| 4. | Блочные системы шифрования. | Блочные системы шифрования. Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования | ЛР |
| 5. | Поточные системы шифрования. | Поточные системы шифрования. Шифрсистема А5. ШифрсистемаГиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа—Месси. Методы анализа поточных шифров. | ЛР |
| 6. | Идентификация. Цифровые подписи. | Идентификация. Фиксированные пароли. Парольные фразы. Атаки на фиксированные пароли. Одноразовые пароли. Протоколы с нулевым разглашением. Атаки на протоколы идентификации. Цифровые подписи. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи. | ЛР |

### 2.3.2. Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

**3-й семестр**

| № | Наименование лабораторных работ | Форма текущего контроля |
|---|---|---|
| 1 | 2 | 3 |

| | | |
|---|---|---|
| 1. | Основные шифры, Стойкость шифров. | Защита ЛР |
| 2. | Конечные поля. Характеристика поля. Мультипликативная группа конечного поля. Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем. Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности. | Защита ЛР |
| 3. | Математическая модель шифра замены. Поточные шифры простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки. Табличное гаммирование. | Защита ЛР |
| 4. | Американский стандарт шифрования данных DES и его модификации. | Защита ЛР |
| 5. | Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования | Защита ЛР |
| 6. | Поточные системы шифрования. | Защита ЛР |
| 7. | Линейные регистры сдвига. Методы анализа поточных шифров. | Защита ЛР |
| 8. | Идентификация. Фиксированные пароли. Парольные фразы. | Защита ЛР |
| 9. | Цифровые подписи. Одноразовые цифровые подписи. | Защита ЛР |

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

### 2.3.3. Примерная тематика курсовых работ (проектов)

Курсовые проекты не предусмотрены

## 2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

| № | Вид СРС | Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Работа с лекционным материалом | Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 |
| 2. | Изучение теоретического материала к лабораторным занятиям | Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1 |
| 3. | Подготовка к зачету | Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. |

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

## 3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ, ПРИМЕНЯЕМЫЕ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

| Семестр | Вид занятия | Используемые интерактивные образовательные технологии | Количество часов |
|---|---|---|---|
| 1 | ЛР | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации. | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| | | ПО для работы с криптографическими системами защиты информации | 2 |
| *Итого:* | | | 16 |

## 4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Криптография и сетевая безопасность».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, доклада-презентации по проблемным темам разделов дисциплины, разно уровневых заданий и промежуточной аттестации в форме вопросов и заданий к экзамену.

**Структура оценочных средств для текущей и промежуточной аттестации**

| № п/п | Код и наименование индикатора | Результаты обучения | Наименование оценочного средства | |
|---|---|---|---|---|
| | | | Текущий | Промежуточная |

| | | | контроль | аттестация |
|---|---|---|---|---|
| 1 | ОПК-1.1. Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций. | Знает основы построения математических моделей систем защищенной передачи информации. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 2 | ОПК-1.2. Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты. | Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты как основы построения криптографических алгоритмов. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 3 | ОПК-1.3. Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности. | Имеет практический опыт работы с решением задач теории чисел, статистического анализа, дискретной математики. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 4 | ОПК-2.1. Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включенного в Единый Реестр Российских программ. | Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО по защите информации, включенного в Единый Реестр Российских программ. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 5 | ОПК-2.2. Умеет анализировать типовые языки программирования, составлять программы. | Умеет анализировать типовые языки программирования и выбирать наилучший для реализации конкретного алгоритмы защиты информации, составлять программы безопасной передачи и хранения данных. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 6 | ОПК-2.3. Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов коммуникации. | Имеет практический опыт решения задач анализа, интеграции программного обеспечения сетевой безопасности в действующие информационные и программные системы, анализа типов коммуникации. | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 7 | ОПК-3.1. Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей. | Знает методы теории алгоритмов, методы системного и прикладного программирования, основные положения и концепции в области математических, информационных и имитационных моделей систем безопасности данных | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 8 | ОПК-3.2. Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем. | Умеет соотносить знания в области программирования, интерпретацию прочитанного, определять и создавать информационные ресурсы глобальных сетей, образовательного контента, средств тестирования систем с учетом требований к безопасности информации | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |
| 9 | ОПК-3.3. Имеет практический опыт применения разработки программного обеспечения и тестирования программных продуктов. | Имеет практический опыт применения разработки программного обеспечения, реализующего или использующего современные | опрос по теме, лабораторная работа | Вопросы на экзамен 1-35 |

| | | | | |
|---|---|---|---|---|
| | | криптографические протоколы | | |

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

Индивидуальные задачи (выполняются студентами самостоятельно и предоставляются в письменном виде).

1. Алгоритм DES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
2. Алгоритм A5. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
3. Алгоритм Feal. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
4. Алгоритм Crypto1. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
5. Алгоритм IDEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Dragon. Реализовать в виде программного приложения с оконным интерфейсом.
6. Алгоритм ГОСТ 94. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
7. Алгоритм Mickey. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Safer64. Реализовать в виде программного приложения с оконным интерфейсом.
8. Алгоритм Mosqito. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC5-64. Реализовать в виде программного приложения с оконным интерфейсом.
9. Алгоритм Rabbit. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
10. Алгоритм Loki 91. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC4. Реализовать в виде программного приложения с оконным интерфейсом.
11. Алгоритм CAST256. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
12. Алгоритм SEAL. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
13. Алгоритм AES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
14. Алгоритм GMR. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
15. Алгоритм Wake. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
16. Алгоритм Trivium. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным

интерфейсом.

17. Алгоритм Skipjack. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

18. Алгоритм Vest. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

19. Алгоритм Frog. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

20. Алгоритм VMPC. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

21. Алгоритм Serpent. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

22. Алгоритм Oryx. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

23. Алгоритм TEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

24. Алгоритм Salsa20. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

25. Алгоритм Mars. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

26. Алгоритм Mugi. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

27. Алгоритм Blowfish. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

28. Алгоритм Pike. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

29. Алгоритм ГОСТ 2012. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

Алгоритм DSA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

**Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)**

Перечень вопросов, которые выносятся на экзамен.

1. Группа. Подгруппа.
2. Группа постановок.
3. Кольцо. Идеалы. Классы вычетов.
4. Кольца полиномов.
5. Конечные поля.
6. Кольцо вычетов.
7. Алгоритмы умножения, обращения, вычисления НОД.
8. Извлечение корней в конечном поле.
9. Вычисление символа Якоби. Проверка на простоту.
10. Основные понятия и определения криптографической защиты информации.
11. Шифрование.

12. Аутентификация.
13. Система RSA. Детерминированные методы разложения.
14. Система RSA. Вероятностные методы разложения.
15. Дискретное логарифмирование в конечном поле. Задача Диффи-Хеллмана.
16. Шифрование с открытым ключом для группы вычислимого порядка.
17. Шифрование с открытым ключом для группы трудновычислимого порядка.
18. Цифровая подпись на группе трудновычислимого порядка.
19. Цифровая подпись на группе вычислимого порядка.
20. Схемы предъявления битов. Криптографические протоколы доказательства с нулевым разглашением.
21. Криптографические протоколы передачи информации со стиранием. Криптографический протокол разделения секрета.
22. Криптографические протоколы управления ключами. Временная метка.
23. Основные понятия классической криптографии. Шифры замены и перестановки. Блочные шифры.
24. Режимы шифрования.
25. Шифр DES.
26. Шифр FEAL.
27. Шифр IDEA.
28. Шифр ГОСТ 28147-89.
29. Шифр RC5.
30. Шифр Blowfish.
31. Шифр SAFER.
32. Шифр AES.
33. Шифр MD5.
34. Шифр ГОСТ Р 34.11-94.
35. Хэш-функция. Хэширование.

**Критерии оценивания результатов обучения**

| Оценка | Критерии оценивания по экзамену |
|---|---|
| Высокий уровень «5» (отлично) | оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы. |
| Средний уровень «4» (хорошо) | оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки. |
| Пороговый уровень «3» (удовлетворительно) | оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. |
| Минимальный уровень «2» (неудовлетворительно) | оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. |

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

## 5. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

### 5.1. Учебная литература

#### 5.1.1. Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : 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. - http://biblioclub.ru/index.php?page=book&id=438331.

2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016.

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1

4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

5.1.2. **Дополнительная литература**:

1. Басалова, Г.В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233689

2. Сергеева, Ю.С. Защита информации. Конспект лекций [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : А-Приор, 2011. – https://biblioclub.ru/index.php?page=book_red&id=72670&sr=1

3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – https://biblioclub.ru/index.php?page=book_red&id=480637&sr=1

5.1.3. Учебно-методическая литература

1. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1

2. Бабенко, Л.И. Параллельные алгоритмы для решения задач защиты информации / Л.И. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Москва : Издательство Горячая линия-Телеком, 2014. - https://e.lanbook.com/reader/book/63228/#1

**5.2. Периодическая литература**

1. Автоматика и вычислительная техника.
2. Реферативный журнал ВИНИТИ
3. Базы данных компании «Ист Вью» http://dlib.eastview.com
4. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

**5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы**

**Электронно-библиотечные системы (ЭБС):**

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

**Профессиональные базы данных:**

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

**Информационные справочные системы:**

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

**Ресурсы свободного доступа:**

1. Американская патентная база данных http://www.uspto.gov/patft/

2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety
15. Philology.ru [Электронный ресурс]: [филологический портал]. - Режим доступа:– http://www.philology.ru/, свободный (дата обращения: 2.02.2017) (библиотека филологических текстов (монографий, статей, методических пособий).
16. Языкознание.ру [Электронный ресурс] : [образовательный портал]. – Режим доступа:– http://yazykoznanie.ru, свободный (дата обращения: 2.02.2017) (ресурс для изучающих различные лингвистические дисциплины).
17. Linguists [Электронный ресурс]: [образовательный портал]. – Режим доступа: http://linguists.narod.ru, свободный (дата обращения: 12.02.2017) (Ресурсы для переводчиков и лингвистов, содержит список других сетевых ресурсов).
18. Лингвистика для школьников [Электронный ресурс]: [образовательный сайт]. – Режим доступа: –http://lingling.ru/, свободный (дата обращения: 2.02.2017).
19. COGNITIV [Электронный ресурс]: [образовательный портал]. – Режим доступа: http://cognitiv.narod.ru, свободный (дата обращения: 5.01.2017) (Сайт для ученых-языковедов всех специальностей (обмен новейшей информацией в области лингвистики; обсуждение фундаментальных и прикладных проблем языкознания, а также вопросов взаимоотношения языка, культуры и общества).
20. Лингвистический энциклопедический словарь [Электронный ресурс]: [он- лайн-словарь]. – Режим доступа: http://lingvisticheskiy-slovar.ru/, свободный (дата обращения: 17.01.2017).
21. Linguistics Dictionary Glossary Terms Lexicon Online [Электронный ресурс]: [образовательный ресурс]. – Режим доступа: http://www.glossary.sil.org/, свободный (дата обращения: 12.02.2017) (глоссарий, содержащий более 950 лингвистических терминов с перекрестными ссылками и списком источников (SIL International).

**Собственные электронные образовательные и информационные ресурсы КубГУ:**

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

## 6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (модуля)

Для освоения учебного материала студенту необходимо ознакомиться со структурой курса и методикой овладения материалом. Весь курс построен от простого к сложному и каждая его тема основана на материалах предыдущих тем. В это связи студенту необходимо не терять логику

курса и строго ей следовать. В лекционном материале даются, как правило, теоретические сведения, которые раскрываются на практических примерах. Для закрепления теоретических знаний студент получает индивидуальное задание к циклу лабораторных работ, который охватывает весь теоретический материал. Каждая лабораторная работы защищается по мере выполнения. Таким образом, выполняя весь цикл лабораторных работ, студент получает и осваивает знания в соответствии с компетенциями курса. По выступлениям на круглом столе с преподавателем согласовывается тема выступления и готовится само выступление. Во время текущей аттестации могут проводиться контрольные опросы по начитанному теоретическому и практическому материалу.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

| Наименование специальных помещений | Оснащенность специальных помещений | Перечень лицензионного программного обеспечения |
|---|---|---|
| Учебные аудитории для проведения занятий лекционного типа (ауд. 129, 131, А305). | Мебель: учебная мебель<br>Технические средства обучения: проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) | PowerPoint, доступ к Microsoft Teams |
| Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации ауд. 129, 131, А305 | Мебель: учебная мебель<br>Технические средства обучения: экран, компьютер<br>Оборудование: кондиционер | PowerPoint, доступ к Microsoft Teams |
| Учебные аудитории для проведения лабораторных работ. Лаборатория (ауд. 102-106, А301-303). | Мебель: учебная мебель<br>Технические средства обучения: экран, проектор, компьютер<br>Оборудование: | системы программирования на языках высокого уровня, сетевой доступ к ресурсам, в частности C++, Object Pascal и пр. с возможностью многопользовательской работы |

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

| Наименование помещений для самостоятельной работы обучающихся | Оснащенность помещений для самостоятельной работы обучающихся | Перечень лицензионного программного обеспечения |
|---|---|---|
| Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки) | Мебель: учебная мебель<br>Комплект специализированной мебели: компьютерные столы<br>Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в | Доступ печатным и электронным информационным ресурсам |

| Наименование помещений для самостоятельной работы обучающихся | Оснащенность помещений для самостоятельной работы обучающихся | Перечень лицензионного программного обеспечения |
|---|---|---|
| | электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi) | |
| Помещение для самостоятельной работы обучающихся (ауд. 146 ) | Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi) | системы программирования на языках C++ и Object Pascal с возможностью многопользовательской работы |