Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования «Северо-Осетинский государственный университет

имени Коста Левановича Хетагурова»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«**Криптография и защита информации**»

Направление подготовки:

**01.03.02 Прикладная математика и информатика**

Профиль: **«Программирование, анализ данных**

**и математическое моделирование»**

Квалификация (степень) выпускника – бакалавр

Форма обучения очная

Год начала подготовки 2024

Владикавказ

2024

Рабочая программа

*обсуждена и утверждена* на заседании кафедры алгебры и анализа (протокол № 5 от 14.02.2024 г.);

*одобрена* советом факультета математики и компьютерных наук (протокол № 6 от 01.03.2024 г.);

*утверждена* в составе Основной профессиональной образовательной программы понаправлению подготовки 01.03.02 «Прикладная математика и информатика», профиль: «Программирование, анализ данных и математическое моделирование», год начала подготовки 2024 (решение ученого совета от 28.03.2024, протокол № 8).

Составитель: старший преподаватель кафедры алгебры и анализа Дряева Р.Ю.

**1. Структура и общая трудоемкость дисциплины**

Общая трудоемкость дисциплины составляет 3 з.е. (108 ч.).

|  | форма обучения |
| --- | --- |
| Курс | 4 |
| Семестр | 8 |
| Лекции | 10 |
| Практические занятия | 8 |
| Лабораторные занятия | - |
| Консультации |  |
| Итого аудиторных занятий | 18 |
| Самостоятельная работа | 90 |
| Курсовая работа | - |
| Зачет | + |
| Экзамен | - |
| Общее количество часов | 108 |

**2. Цели изучения дисциплины**

Целями освоения дисциплины (модуля) «Криптография и защита информации» является изучение основных принципов обеспечения информационной безопасности на основе организационных, инженерно-технических и правовых методов защиты информации в автоматизированных системах. В рамках курса рассматриваются как теоретические, так и практические аспекты информационной безопасности автоматизированных систем.

Практические работы в компьютерных классах служат для индивидуальной работы студентов над учебными задачами с целью выработки и закрепления практических навыков защиты информации.

**3. Место дисциплины в структуре ОПОП:**

Б1.В.ДВ.04.01. Блок 1. Дисциплины (модули). Часть, формируемая участниками образовательных отношений.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса математических дисциплин и общего курса информатики, а также в результате освоения дисциплин: «Информационные технологии в профессиональной деятельности», «Линейная алгебра», «Алгебра и теория чисел», «Математический анализ», «Теория вероятностей и математическая статистика».

**4. Требования к результатам освоения дисциплины**

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);

Способен проводить научно-исследовательские разработки по отдельным разделам темы в области прикладной математики и информационных технологий (ПК-1);

Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники (ПК-2).

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

| **Компетенции** | **Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП** | | |
| --- | --- | --- | --- |
| **Код и формулировка** | **Знать:** | **Уметь** | **Владеть:** |
| УК-1  Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | современные технические и программные средства взаимодействия с ЭВМ;  методы и средства обеспечения информационной безопасности компьютерных систем; основные стандарты в области инфокоммуникационных систем и технологий; | инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; настраивать конкретные конфигурации операционных систем;  настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;  применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей | навыками работы с различными операционными системами и их администрирования; |
| ПК-1  Способен проводить научно-исследовательские разработки по отдельным разделам темы в области прикладной математики и информационных технологий | Способен проводить научно-исследовательские разработки по отдельным разделам темы в области прикладной математики и информационных технологий | использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры; | средствами администрирования сетевых программно-аппаратных комплексов защиты информации; средствами администрирования систем обнаружения компьютерных атак |
| ПК-2  Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники | технологии обнаружения компьютерных атак и их возможности;  основные уязвимости и типовые атаки на современные компьютерные системы;  возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;  методы защиты компьютерных сетей | выполнять функции администратора безопасности защищенных компьютерных систем;  выполнять настройку защитных механизмов сетевых программно-аппаратных средств | средствами и системами аудита информационной безопасности;  методикой проведения аудита информационной безопасности |

**5. Содержание и учебно-методическая карта дисциплины**

| **№ темы** | **Наименование тем (вопросов), изучаемых по данной дисциплине** | **Занятия** | | **Самостоятельная работа студентов** | | **Формы контроля** | **Литература** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **л** | **пр.** | **Содержание** | **Часы** |
|  | Основные понятия криптографии и теория сложности  Понятие и сущность защиты информации. Базовые термины и определения, применяемые в области информационной безопасности. | 2 | 2 | дискретное логарифмирование  Функции межсетевых экранов. Системы защиты на базе межсетевых экранов | 30 | Опрос | [1-6] |
|  | Криптографические протоколы  Технологические и эксплуатационные уязвимости программно-аппаратного обеспечения АС. Основные типы информационных вторжений | 2 | 2 | математика разделения  секрета  Организация виртуальных частных сетей. Достоинства применения технологии VPN. | 30 | Доклад | [1-6] |
|  | Функции хеширования  Американский стандарт шифрования данных DES, отечественный стандарт шифрования данных ГОСТ 28147-89. Правило стойкости шифра Керкхоффа. Понятие раскрытия криптосистемы. Частотный анализ. Метод полного перебора. Атака по ключам. | 2 | 2 | компьютер и криптография  Классификация классических вирусов. Антивирусные программы. Методы обнаружения вирусов. | 30 | Доклад | [1-6] |
|  | Алгоритмические  проблемы теории чисел  Законодательные и правовые основы защиты информации. Руководящие документы ФСТЭК (Гостекомиссии РФ) по защите информации. | 2 | 2 |  |  |  | [1-6] |
|  | Система RSA  Понятие риска, подходы к обоснованию проекта подсистемы обеспечения безопасности. Положения основных моделей безопасности компьютерных систем: дискреционного, мандатного и ролевого разграничении доступа | 2 |  |  |  |  | [1-6] |
|  | **Итого** | 10 | 8 |  | 90 |  |  |

**6. Образовательные технологии**

Согласно учебному плану при преподавании дисциплины используются традиционные образовательные технологии: лекции, практические (семинарские) занятия и самостоятельная работа студентов. Также при проведении занятий и самостоятельной работе студентов могут быть использованы:

**–** *интерактивные технологии* («мозговой штурм», дебаты, презентационный метод, работа в парах, работа в группах, деловая игра);

**–** *технологии контекстного обучения* **–** система дидактических форм, методов и средств, направленная на моделирование содержания будущей профессиональной деятельности специалиста (анализ конкретных ситуаций, методы работы с информационными базами данных, деловая игра и др.);

– *технологии электронного обучения* (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов СОГУ.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте или с использованием ЭИОС СОГУ.

**7. Учебно-методическое обеспечение самостоятельной работы**

Самостоятельная работа проводится с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

– углубления и расширения теоретических знаний;

– формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развития исследовательских навыков и умений.

По дисциплине предусмотрены следующие виды самостоятельной работы студентов:

– самостоятельное повторение и изучение теоретического материала;

– выполнение домашних заданий;

– подготовка доклада/конспекта по теме, вынесенной на самостоятельное изучение;

– подготовка к выполнению практических работ;

– подготовка к промежуточной аттестации (зачету);

Содержание, трудоемкость и формы контроля внеаудиторной самостоятельной работы содержатся в разделе 5.

**8. Оценочные средства для текущего контроля успеваемости,**

**рубежной и промежуточной аттестации по итогам освоения дисциплины**

Основными *формами текущего контроля* по дисциплине являются:

– устный опрос на лекции или практическом занятии;

– доклад / конспект по теме, вынесенной на самостоятельное изучение;

– проверка домашних заданий, практических работ.

Форма *рубежного контроля:* тест.

Формы *промежуточной аттестации:* зачет.

**8.1. Формы контроля и критерии оценивания**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Этап** | **Форма**  **контроля** | **Критерии оценивания (процент от максимального кол-ва баллов)** | | | |
| **86-100 %** | **71–85%** | **50–70%** | **Менее 50%** |
| **отлично / зачет** | **хорошо / зачет** | **удовлетворительно / зачет** | **неудовлетворительно / незачет** |
| *1. Текущий контроль (max 20 баллов за один модуль)* | | | | | |
|  |  | 15–17 баллов | 12–14 баллов | 8–11 баллов | 0–7 баллов |
|  | Текущая работа в течение модуля  (мах 17б.) | Студент активно работает на занятиях, превосходно выполняет все задания преподавателя. | Студент активно работает на занятиях, хорошо выполняет задания преподавателя. | Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя. | Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя. |
|  |  | 3 балла | 2 балла | 1 балл | 0 баллов |
|  | Реферат /  доклад / конспект  (мах 3б.) | Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения. | Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения. | Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения. | Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения. |
| *2. Рубежный контроль (15 б. за один модуль)* | | | | | |
|  | тест /  контрольная работа | Количество баллов за выполнение каждого задания указываются в тесте / контрольной работе. | | | |
| *3. Промежуточная аттестация по дисциплине (max число баллов – в соответствии с действующим локальным нормативным актом)* | | | | | |
|  |  | Критерии оценивания (процент от максимального кол-ва баллов) | | | |
|  |  | 86–100 % | 71–85 % | 50–70 % | 0–49 % |
|  | Зачет /  Экзамен | Дан полный, развернутый ответ на поставленный вопрос. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. | Дан полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью «наводящих» вопросов преподавателя. | Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции. | Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины. |

Пересчет полученной суммы баллов по дисциплине в оценку производится в соответствии с действующим локальным нормативным актом.

**8.2. Примерный вариант рубежной контрольной работы (теста) (30 баллов)**

**Каждое задание оценивается в 2 балла**

Используя теорему Эйлера и алгоритм быстрого возведения в степень, найти

+5

4

1

Решить систему сравнений

+75

101

201

Зашифровать сообщение «Шифр Цезаря» с использованием ключа k=3

+ЫлчуЩзкгув

ЬмшфЪилдфг

ЪкцтШжйвтб

Зашифровать сообщение «Мало иметь хороший ум, главное – хорошо его применять» с помощью таблицы Вижинера и ключа «Рене Декарт»

+эещумсптмзяхьэмоюм, уюржыуи – ъщрякяйруухумхапчй

эещумсптмзяхьэмоюм, уюржыки – ъщрякяйруухулхапчй

эещумсптмзяхьэноюм, уюржыки – ъщряряйруухумхапчй

Зашифровать сообщение m=7, с помощью алгоритма RSA, если e=3,n=55

+13

5

11

Зашифровать сообщение m=RSA, с помощью алгоритма RSA, если e=7,n=33

+6131

5462

6452

В криптосистеме Хилла с инволютивной над матрицей

зашифруйте слово ROSE

+KRUS

SASN

KRIS

Зашифруйте слово STUDENTcпомощью модулярного шифра

+FILMPQL

FILMTOL

FILMTQL

Хеш-функция определяется как результат выполнения побитовой операции «сумма по модулю 2» для всех байтов сообщения. Длина хеш-кода 8 бит. Вычислите хеш- функцию для 10 96 ВЕ

+38

11

36

Зашифровать сообщение ПРИНЦИПЫМЕТОДОВШИФРОВАНИЯ с помощью перестановки 436215

+НИИРПЦЕМОЫПТШВФОДИАВИОРН\_ \_ \_ \_я\_

НИИРПЦЕМОЫПШТВФОДИАВИОРН\_ \_ \_ \_я\_

НИИПРЦЕМОЫПТШВФОДИАВИОРН\_ \_ \_ \_я\_

Первый байт фрагмента текста имеет вид В6,на него накладывается по модулю 2 4-х битовая гамма 0111. Что получится после шифрования?

+С1

C2

C6

Выберите правильное определение термина «криптоанализ»

+криптоанализ-это наука о преодолении криптографической защиты информации

 криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи

криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия

Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон?

 электронная цифровая подпись

+протокол

хэш-функция

Расшифруйте сообщение ЕВВФМШБЬШ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯОтвет запишите заглавными русскими буквами без пробелов

+СООБЩЕНИЕ

Гарантирование невозможности несанкционированного изменения информации - это:

+обеспечение целостности

обеспечение конфиденциальности

 обеспечение аутентификации

**8.3. Вопросы к зачету**

1. Понятие защиты информации. Основные определения в области защиты информации.
2. Аспекты защиты информации: правовая, организационная инженерно-техническая.
3. Понятие уязвимости. Распространенные типы уязвимостей.
4. Понятие угрозы безопасности. Классификация угроз.
5. Понятие сетевой атаки. Классификация сетевых атак.
6. Основные понятия в области криптографии. Классификация криптографических алгоритмов.
7. Блочные шифры. Принцип работы шифра ГОСТ 28147-89.
8. Поточные шифры. Понятие синхронных и асинхронных шифров.
9. Криптографические хеш-функции. Примеры алгоритмов.
10. Криптосистемы с открытым ключом. Криптосистема RSA.
11. Электронная цифровая подпись. Принцип работы. Примеры алгоритмов.
12. Понятие риска в области информационной безопасности. Управление рисками.
13. Понятие политики безопасности. Основные типы политик безопасности.
14. Понятие политики безопасности. Модель Харрисона-Руззо-Ульмана.
15. Понятие политики безопасности. Модель Белла-Лападула.
16. Понятие политики безопасности. Ролевое разграничение доступа.
17. Основные компоненты системы безопасности Windows и их функции.
18. Основные информационные объекты системы безопасности Windows (идентификатор безопасности, маркер доступа, дескриптор безопасности и т.д.) и их назначение.
19. Понятие компьютерного вируса. Классификация вирусов. Троянские программы и сетевые черви.
20. Понятие компьютерного вируса. Классификация вирусов по особенностям работы. Основные методы обнаружения вирусов.

**9. Учебно-методическое и информационное обеспечение дисциплины**

**а) основная литература:**

1. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Министерство науки и высшего образования РФ, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 77 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=499598>  – Библиогр. в кн. – ISBN 978-5-9275-2501-0. – Текст : электронный.
2. Лапонина, О.Р. Межсетевые экраны : учебное пособие / О.Р. Лапонина. – 2-е изд., исправ. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=429093>  – Текст : электронный.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=429035>  – Текст : электронный.
4. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428820>  – Текст : электронный.

**б) дополнительная литература:**

1. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=480636>  – Библиогр.: с. 213. – Текст : электронный.
2. Пилиди, В.С. Математические основы защиты информации : учебное пособие : [16+] / В.С. Пилиди ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 309 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=577894> – Библиогр.: с. 301. – ISBN 978-5-9275-3363-3. – Текст : электронный.

**в) Профессиональные базы данных и другие интернет-ресурсы:**

– ЭБС «Научная электронная библиотека eLibrary.ru» (<http://www.elibrary.ru>);

– ЭБС «Университетская библиотека onLine» (<http://www.biblioclub.ru>);

– ЭБС «Юрайт» (<http://www.urait.ru/>);

– Универсальная база данных «ИВИС» ([htpps:/eivis.ru/](about:blank));

– ИС «Национальнаяэлектронная библиотека (НЭБ)»(<https://rusneb.ru/>).

**10. Материально-техническое обеспечение дисциплины**

Для проведения лекционных и практических занятий используются:

– учебные аудитории для проведения лекционных занятий, занятий семинарского типа, текущего контроля, промежуточной аттестации, оборудованные аудиторной мебелью, доской (меловой, маркерной или интерактивной), компьютером или ноутбуком с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду СОГУ, мультимедийным проектором, экраном;

– компьютерный класс (корпус 10, ауд. №505, 506, 600, 601, 605, 606), оборудованный аудиторной мебелью, доской (меловой, маркерной или интерактивной), компьютерами или ноутбуками с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СОГУ, мультимедийным проектором, экраном.

*Лицензионное программное обеспечение:*

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ».

*Перечень ПО в свободном доступе:* Kaspersky Free; WinRar; Google Chrome; Yandex Browser; Opera Browser; Acrobat Reader; MOODLE; LaTeX; системы компьютерной алгебры SciLab и Maxima, WplframAlpha.

Помещение для самостоятельной работы студентов: Зал электронных ресурсов Научной библиотеки СОГУ (корпус 6, кабинет № 1.8), укомплектован специализированной мебелью (рабочие места студентов), необходимыми техническими средствами обучения: компьютеры, принтер, возможность подключения к сети «Интернет», доступ в электронную информационно-образовательную среду СОГУ.