Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сочинский государственный университет»

СОГЛАСОВАНО
Декан ФИИЦТ
_____ А.Н. Волков
«10» 04 2023 г.

УТВЕРЖДАЮ
Проректор по УРиКОД
_____ А.В. Иваненко
«10» 04 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Прикладная криптография
(указывается наименование дисциплины по учебному плану)

Шифр и направление подготовки 09.04.03 Прикладная информатика

Квалификация (степень) выпускника магистр
(бакалавр, магистр, и т.п., согласно лицензии)

Профиль подготовки Информационно-аналитическое обеспечение принятия решений
(наименование программы бакалавриата/магистратуры/специалитета)

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

Выпускающая кафедра Информационных технологий и математики
(название)

Кафедра-разработчик рабочей программы Информационных технологий и математики
(название)

Год набора 2023

Семестр	Трудоем-кость (час./зет.)	Лекцион. занятий, (час.)	Практич. занятий, (час.)	Лаборат. занятий, (час.)	СРС, (час.)	КР/КП (час.)	Форма промежуточного контроля (экз./зачет)
3	**108/3**	**28**	**0**	**28**	**52**	**-**	**Зачет**
ИТОГО	**108/3**	**28**	**0**	**28**	**52**		**Зачет**

Сочи 2023 г.

Лист согласования рабочей программы дисциплины «Прикладная криптография»

Рабочую программу составил:
Симаворян С.Ж., к.т.н., доцент кафедры Информационных технологий и математики

РАБОЧАЯ ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА

Заведующий кафедрой _____ Копырин А.С.

Учебно-методическое и информационное обеспечение дисциплины соответствует библиотечному фонду СГУ:

Директор НОБ _____ Онищенко Е.В.

Структура рабочей программы соответствует предъявляемым требованиям.

Отдел качества образования и методического обеспечения _____ Шипранова И.К.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ РПД

Рабочая программа переутверждена на 2024/2025 учебный год, 4 марта 2024г.

В программу внесены дополнения и(или) изменения.

без изменений

Заведующий кафедрой _____ (подпись) Колнрин А.С. (ФИО)

Рабочая программа переутверждена на 20___/20___ учебный год,

В программу внесены дополнения и(или) изменения.

Заведующий кафедрой _____ (подпись) _____ (ФИО)

Рабочая программа переутверждена на 20___/20___ учебный год

В программу внесены дополнения и(или) изменения.

Заведующий кафедрой _____ (подпись) _____ (ФИО)

СОДЕРЖАНИЕ

1 ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Прикладная криптография» является изучение основных подходов, методов и алгоритмов современной криптографии.

Задачи дисциплины:
- изучить основные понятия современной криптографии;
- изучить основные направления криптографии, связанные с обеспечением конфиденциальности взаимодействия пользователей компьютеров и компьютерных сетей;
- изучить основные широко используемые блочные и поточные шифры, криптографические хеш-функции, шифры с открытым ключом и методы цифровой (электронной) подписи;
- изучить отечественные государственные стандарты и зарубежные стандарты в области криптографической защиты информации

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП НАПРАВЛЕНИЯ (СПЕЦИАЛЬНОСТИ)

Дисциплина Прикладная криптография относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Таблица 1 - Дисциплины, участвующие в формировании компетенции

Код и наименование компетенции	**Дисциплины, участвующие в формировании компетенции**
Профессиональные компетенции	
ПК-1 Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Компьютерная безопасность и управление корпоративными информационными системами Поддержка жизненного цикла корпоративных информационных систем Методы и инструментарии конкурентной разведки Когнитивная бизнес-аналитика Теория систем и системный анализ (продвинутый уровень) Проектно-технологическая практика Преддипломная практика

3 ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 2 - Компетенции и индикаторы их достижения

Компетенции и индикаторы их достижения		В результате изучения дисциплины обучающиеся должны:
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	
ПК-1 Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	ПК-1.1 Демонстрирует знание теории систем и системного анализа, теории управления; инструментов и методов оценки качества, надежности и информационной безопасности ИС; устройства и возможностей современных ИС; нормативно-технических документов, описывающие качество, надежности и информационную безопасность ИС	Знать инструменты и методы оценки качества, надежности и информационной безопасности ИС Знать нормативно-технические документы, описывающие качество, надежности и информационную безопасность ИС
	ПК-1.2 Анализирует исходные данные по качеству, надежности и информационной безопасности ИС; планирует, распределяет и контролирует выполнение работ; разрабатывает регламентные документы в области качества, надежности и информационной безопасности	Уметь анализировать исходные данные по качеству, надежности и информационной безопасности ИС Уметь разрабатывать регламентные документы в области качества, надежности и информационной безопасности
	ПК-1.3 Применяет навыки обеспечения соответствия процесса развертывания ИС у заказчика принятым в организации или проекте стандартам и технологиям; навыки разработки и согласования регламентов по управлению качеством, надежностью и информационной безопасностью ИС; навыки выбора и внедрения инструментов и методов контроля качества	Владеть навыками разработки и согласования регламентов по управлению качеством, надежностью и информационной безопасностью ИС

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Тематический план дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 часов

Таблица 3 – Распределение фонда времени по темам

№ раздела темы	Наименование модуля (раздела, темы) дисциплины	Всего часов	Виды учебной нагрузки и их трудоемкость, часы			
			Контактная работа			СРС
			Лекции	Практические занятия	Лабораторные работы	
1	Тема 1. Основные понятия криптографии	6	2	0	2*	2
2	Тема 2. Методы шифрования с закрытым ключом	6	2	0	2*	2
3	Тема 3. Принципы построения блочных шифров с закрытым ключом	8	2	0	2	4
4	Тема 4. Алгоритмы шифрования DES и AES	8	2	0	2*	4
5	Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89	8	2	0	2	4
6	Тема 6. Криптографические хеш-функции	8	2	0	2	4
7	Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1	8	2	0	2	4
8	Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2	8	2	0	2	4
9	Тема 9. Введение в криптографию с открытым ключом	8	2	0	2*	4
10	Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом	8	2	0	2*	4
11	Тема 11. Криптографические алгоритмы с открытым ключом и их использование	8	2	0	2	4
12	Тема 12. Электронно-цифровая подпись	8	2	0	2*	4
13	Тема 13. Совершенно секретные системы	8	2	0	2*	4
14	Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации	8	2	0	2	4
	Зачет					
	ИТОГО	108	28	0	28	52

* ***Лабораторное занятие проводится в форме практической подготовки.***

4.1.1 Лекционные занятия

№ п/п	Наименование темы дисциплины	Краткое содержание
1	Тема 1. Основные понятия криптографии	В данной лекции определяются предмет и задачи криптографии, формулируются основополагающие определения курса и требования к криптографическим системам защиты информации, рассматриваются основные этапы развития криптографии как науки.
2	Тема 2. Методы шифрования с	В этой лекции рассматривается общая схема симметричного

	закрытым ключом	шифрования, а также дается классификация простейших методов симметричного шифрования. Описание каждого из указанных в классификации шифров сопровождается примером.
3	Тема 3. Принципы построения блочных шифров с закрытым ключом	На лекции рассматриваются принципы построения современных блочных алгоритмов: операции, используемые в блочных алгоритмах симметричного шифрования; структура блочного алгоритма; требования к блочному алгоритму шифрования
4	Тема 4. Алгоритмы шифрования DES и AES	На лекции рассматриваются криптографические системы DES и AES
5	Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89	На лекция рассматривается отечественный стандарт на блочный алгоритм шифрования. Подробно рассматривается структура ГОСТ 28147-89, а также режимы шифрования данных с использованием алгоритма криптографического преобразования данных ГОСТ 28147-89.
6	Тема 6. Криптографические хеш-функции	На лекции рассматривается понятие хеш-функции и приводится краткий обзор алгоритмов формирования хеш-функций. Рассматривается возможность использования блочных алгоритмов шифрования для формирования хеш-функции.
7	Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1	Из этой лекции объясняется каким образом осуществляется шифрование при передаче данных в режиме реального времени. Формулируются принципы использования генераторов псевдослучайных ключей при потоковом шифровании.
8	Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2	На лекции рассматриваются алгоритмы генерации псевдослучайных чисел на основе сдвиговых регистров с обратной связью и RC4.
9	Тема 9. Введение в криптографию с открытым ключом	На лекции рассматриваются основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом. Рассматриваются отечественные и зарубежные стандарты на алгоритмы цифровой подписи, применяемые в настоящее время.
10	Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом	На лекции формулируются основные математические понятия и факты, необходимые для дальнейшего изучения криптографии: простые и составные числа; основная теорема арифметики; взаимно простые числа и функция Эйлера; основы арифметики остатков и теории сравнений; малая теорема Ферма; наибольший общий делитель и обобщенный алгоритм Евклида; инверсия по модулю m.
11	Тема 11. Криптографические алгоритмы с открытым ключом и их использование	На этой лекции излагаются наиболее известные криптографические алгоритмы с открытым ключом: RSA, алгоритм Диффи-Хеллмана, алгоритм Эль-Гамаля. Также приводится принцип работы криптографических систем на эллиптических кривых.
12	Тема 12. Электронно-цифровая подпись	На лекции излагаются основные подходы к формированию цифровой подписи на основе различных алгоритмов с открытым ключом. Кроме того, на лекции рассматриваются отечественные и зарубежные стандарты на алгоритмы цифровой подписи, применяемые в настоящее время.
13	Тема 13. Совершенно секретные системы	На этой лекции излагаются основные идеи теории Шеннона (он показал, что теоретически возможны так называемые совершенно секретные криптографические системы, которые не могут быть "взломаны")
14	Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации	На этой лекции сформулированы основные подходы к использования помехоустойчивых кодов и алгоритмов сжатия данных, необходимых на практике.

4.1.2 Практические занятия

В учебном плане отсутствуют

4.1.3 Лабораторные занятия

№ п/п	Наименование темы дисциплины	Краткое содержание
1	Тема 1. Основные понятия криптографии	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №1***. По заданию преподавателя рассматриваются примеры простейших шифров, на основе которых поясняются сформулированные понятия и тезисы на лекции
2	Тема 2. Методы шифрования с закрытым ключом	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №2.*** По заданию преподавателя решаются примеры с конкретными известными в настоящее время шифрами
3	Тема 3. Принципы построения блочных шифров с закрытым ключом	***Лабораторная работа №3.*** По заданию преподавателя на примере построения сети Фейстеля решается задача построения блочных шифров с закрытым ключом
4	Тема 4. Алгоритмы шифрования DES и AES	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №4.*** По заданию преподавателя рассматриваются алгоритмы шифрования DES и AES, "двухкратный DES", атака "встреча посередине" и способы ее устранения. Рассматривается новый стандарт США на блочный шифр – алгоритм Rijndael
5	Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89	***Лабораторная работа №5.*** По заданию преподавателя исследуются основные отличия алгоритмов шифрования по ГОСТ 28147-89 и DES на конкретных примерах
6	Тема 6. Криптографические хеш-функции	***Лабораторная работа №6.*** По заданию преподавателя на занятии приводится краткий обзор алгоритмов формирования хеш-функций и использования блочных алгоритмов шифрования для формирования хеш-функции
7	Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1	***Лабораторная работа №7.*** По заданию преподавателя рассматриваются заданные простейшие генераторы псевдослучайных чисел: линейный конгруэнтный, генератор по методу Фибоначчи с запаздыванием, генератор псевдослучайных чисел на основе алгоритма BBS. Описание каждого из алгоритмов сопровождается примером, в котором поясняются особенности использования того или иного метода генерации псевдослучайных чисел.
8	Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2	***Лабораторная работа №8.*** По заданию преподавателя в этой лабораторной работе изучается механизм использования режимов OFB и CTR блочных шифров для получения псевдослучайных чисел.
9	Тема 9. Введение в криптографию с открытым ключом	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №9.***По заданию преподавателя исследуются особенности применения математических односторонних функций для шифрования, формирования секретных ключей и цифровой подписи на электронных документах.
10	Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №10.*** По заданию преподавателя исследуются алгоритмы шифрования с открытым ключом и алгоритмы симметричного шифрования. Проводится анализ

		и сравнение.
11	Тема 11. Криптографические алгоритмы с открытым ключом и их использование	***Лабораторная работа №11.*** По заданию преподавателя разрабатывается описание и структура каждого из алгоритмов, рассмотренных на лекции подробным примером.
12	Тема 12. Электронно-цифровая подпись	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №12.*** По заданию преподавателя изучаются на конкретных примерах: электронная подпись на основе алгоритма RSA, цифровая подпись на основе алгоритма Эль-Гамаля (принцип создания и проверки подписи), стандарт цифровой подписи DSS, стандарт цифровой подписи ГОСТ Р34.10-94, новый отечественный стандарт ЭЦП «ГОСТ Р34.10-2001», а также вопросы управления открытыми ключами
13	Тема 13. Совершенно секретные системы	***Лабораторное занятие проводиться в форме практической подготовки.*** ***Лабораторная работа №13.*** По заданию преподавателя решаются задачи, в которых рассчитываются энтропия и неопределённость сообщений, норма языка, избыточность сообщений и расстояние единственности шифра.
14	Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации	***Лабораторная работа №14.*** По заданию преподавателя решаются практические задачи передачи информации от абонента к абоненту с моделированием случайных помех на линиях связи, ошибок и сбоёв аппаратуры, частичного разрушение носителей данных и т.д., с помощью алгоритмов комплексного использования различных методов и средств.

4.14. Самостоятельная работа студента

№ п/п	Наименование темы дисциплины	Краткое содержание
1	Тема 1. Основные понятия криптографии	Работа над лекционными и лабораторными занятиями
2	Тема 2. Методы шифрования с закрытым ключом	Работа над лекционными и лабораторными занятиями
3	Тема 3. Принципы построения блочных шифров с закрытым ключом	Работа над лекционными и лабораторными занятиями
4	Тема 4. Алгоритмы шифрования DES и AES	Работа над лекционными и лабораторными занятиями
5	Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89	Работа над лекционными и лабораторными занятиями
6	Тема 6. Криптографические хеш-функции	Работа над лекционными и лабораторными занятиями
7	Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1	Работа над лекционными и лабораторными занятиями
8	Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2	Работа над лекционными и лабораторными занятиями
9	Тема 9. Введение в криптографию с открытым ключом	Работа над лекционными и лабораторными занятиями
10	Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом	Работа над лекционными и лабораторными занятиями
11	Тема 11. Криптографические алгоритмы с открытым ключом и их использование	Работа над лекционными и лабораторными занятиями
12	Тема 12. Электронно-цифровая подпись	Работа над лекционными и лабораторными занятиями
13	Тема 13. Совершенно секретные системы	Работа над лекционными и лабораторными занятиями
14	Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации	Работа над лекционными и лабораторными занятиями

4.1.4 Интерактивные формы занятий

В учебном плане отсутствуют

4.2 Учебно-методическое и информационное обеспечение дисциплины

4.2.1 Литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745 (дата обращения: 06.04.2023).
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019. — 245 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/434104 (дата обращения: 06.04.2023).
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019 (дата обращения 06.04.2023)
4. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487 (дата обращения 06.04.2023)

4.2.2 Современные профессиональные базы данных (СПБД) и информационные справочные системы (ИСС)

Таблица 4 – Перечень современных профессиональных баз данных (СПБД) и информационные справочные системы (ИСС)

№	***Наименование СПБД***
1	Электронная образовательно-информационная среда СГУ. - Режим доступа: http://www.edu.sutr.ru (дата обращения: 29.06.2023)
	Наименование ИСС
1	Пакет бизнес-моделирования “Business Studio”, отечественное ПО
2	Пакет бизнес-моделирования “Elma ECM+”, отечественное ПО
3	Microsoft Visio Professional 2007, 2010, 2013, 2016

4.2.3 Интернет-ресурсы и другие электронные информационные источники

Таблица 5 – Интернет-ресурсы и электронные информационные источники

№	Наименование интернет-ресурсов и электронных информационных источников
1	Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Эр Медиа». – Саратов, 2010 – . – URL: http://www.iprbookshop.ru/ (дата обращения: 29.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
2	Университетская библиотека онлайн : электронно-библиотечная система : сайт / ООО «Нексмедиа». – Москва : Директ-Медиа, 2001 – . – URL: https://biblioclub.ru/index.php?page=book_blocks&view=main_ub (дата обращения:

	29.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
3	Образовательная платформа Юрайт : электронно-библиотечная система : сайт / ООО «Электронное издательство Юрайт». – – Москва, 2020 – . – URL: https://urait.ru/catalog/organization/DE41FE6D-0B08-4394-B225-3DD636CCCE1F (дата обращения: 29.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.
4	eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru/ (дата обращения: 29.06.2023). – Режим доступа: для авториз. пользователей. – Текст : электронный.

4.3 Текущая и промежуточная аттестации по дисциплине

Для оценки сформированности компетенций разрабатываются оценочные средства по дисциплине.

Форма и содержание текущей и промежуточной аттестации по дисциплине раскрывается в фонде оценочных средств, который является отдельным документом.

Оценочные средства по дисциплине содержат:

- материалы для текущего контроля оценки знаний по дисциплине;
- материалы для промежуточного контроля оценки знаний по дисциплине.
- критерии оценивания;
- шкалы оценивания.

Вопросы к промежуточной аттестации:

1. Предмет и задачи криптографии. Основные определения.
2. Требования к криптографическим системам защиты информации.
3. Реализация криптографических методов.
4. Криптографические атаки.
5. Криптографический протокол.
6. Общая схема симметричного шифрования.
7. Методы замены.
8. Одноалфавитная замена.
9. Пропорциональные шифры.
10. Многоалфавитные подстановки.
11. Методы гаммирования.
12. Методы перестановки.
13. Понятие композиционного шифра.
14. Операции, используемые в блочных алгоритмах симметричного шифрования.
15. Структура блочного алгоритма симметричного шифрования.
16. Требования к блочному алгоритму шифрования.
17. Сеть Фейштеля.
18. Шифрование.
19. Расшифрование.
20. Двухкратный DES и атака «встреча посередине».
21. Трехкратный DES.
22. Алгоритм Rijndael.
23. Режимы работы блочных алгоритмов.
24. Структура раунда ГОСТ 28147-89.
25. Процедуры шифрования и расшифрования.
26. Основные режимы шифрования.
27. Отличия алгоритмов шифрования по ГОСТ 28147-89 и DES.
28. Понятие хеш-функции.
29. Использование блочных алгоритмов шифрования для формирования хеш-функции.
30. Обзор алгоритмов формирования хеш-функций.
31. Поточные шифры.
32. Принципы использования генераторов псевдослучайных чисел при потоковом шифровании.

33. Линейный конгруэнтный генератор псевдослучайных чисел
34. Метод Фибоначчи с запаздыванием.
35. Генератор псевдослучайных чисел на основе алгоритма BBS.
36. Генераторы псевдослучайных чисел на основе сдвиговых регистров с обратной связью.
37. Использование режимов OFB и CTR блочных шифров для получения псевдослучайных чисел.
38. Алгоритм RC4.
39. Генераторы настоящих случайных чисел в криптографии.
40. Управление секретными ключами.
41. Предпосылки создания методов шифрования с открытым ключом и основные определения.
42. Односторонние функции.
43. Использование асимметричных алгоритмов для шифрования.
44. Цифровая подпись на основе алгоритмов с открытым ключом.
45. Формирование секретных ключей с использованием асимметричных алгоритмов.
46. Требования к алгоритмам шифрования с открытым ключом.
47. Простые и составные числа.
48. Основная теорема арифметики.
49. Взаимно простые числа и функция Эйлера.
50. Арифметика остатков и теория сравнений.
51. Малая теорема Ферма.
52. Наибольший общий делитель.
53. Обобщенный алгоритм Евклида.
54. Инверсия по модулю m.
55. Алгоритм RSA
56. Основные сведения
57. Шифрование
58. Пример вычислений по алгоритму
59. Вопросы практического использования алгоритма RSA
60. Алгоритм Диффи-Хеллмана.
61. Формирование общего ключа.
62. Вопросы практического использования алгоритма Диффи-Хеллмана.
63. Алгоритм Эль-Гамаля.
64. Шифрование.
65. Криптографические системы на эллиптических кривых.
66. Возможные атаки при использовании алгоритмов асимметричного шифрования.
67. Атака «человек-в-середине».
68. Атака на основе выбранного открытого текста.
69. Электронная подпись на основе алгоритма RSA.
70. Цифровая подпись на основе алгоритма Эль-Гамаля.
71. Принцип создания и проверки подписи.
72. Стандарты на алгоритмы цифровой подписи.
73. Стандарт цифровой подписи DSS.
74. Стандарт цифровой подписи ГОСТ Р34.10-94.
75. Новый отечественный стандарт ЭЦП.
76. Симметричная или асимметричная криптография?
77. Управление открытыми ключами.
78. Основные подходы к измерению информации.
79. Энтропия и неопределенность.
80. Норма языка и избыточность сообщений.
81. Понятие совершенно секретной системы.
82. Расстояние единственности.
83. Проблемы передачи информации и их комплексное решение.
84. Помехоустойчивое кодирование.
85. Принципы сжатия данных.

Нормы оценки знаний предполагают учёт индивидуальных особенностей обучающихся, дифференцированный подход к обучению, проверке знаний, умений, уровня формирования компетенций.

В устных и письменных ответах обучающихся при выполнении практических заданий и расчетов учитываются: глубина знаний, владение необходимыми умениями (в объеме программы), логичность изложения материла, включая обобщения, выводы, соблюдение норм литературной речи, владение навыками и приемами выполнения практических заданий, подтверждение сделанных при решении практических заданий выводов соответствующими нормативными документами, правильность расчета показателей, полнота и правильность раскрытых процедур и действий в предложенном практическом задании.

Шкала оценивания ответов обучающегося при проведении промежуточной аттестации по дисциплине (зачет)

Оценка **«зачтено»** - ответ на вопрос билета полный и правильный, даны правильные ответы на дополнительные вопросы. Изложение материала при ответах на вопрос построено грамотно, в определенной логической последовательности. Обучающийся показывает владение всеми индикаторами достижения компетенций дисциплины.

Оценка **«не зачтено»** - обучающийся не отвечает на вопросы или допускает грубые, существенные ошибки при ответах, Не демонстрирует владения индикаторами достижения компетенций по дисциплине.

5 УСЛОВИЯ ОСВОЕНИЯ И РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1. Методические рекомендации обучающимся по изучению дисциплины

В течение семестра студенты осуществляют учебные действия на лекционных и практических занятиях, усваивают и повторяют основные понятия. Контроль эффективности самостоятельной работы студентов осуществляется путем проверки освоения ими учебных заданий, предусмотренных для самостоятельной отработки.

Преподавание и изучение учебной дисциплины осуществляется в виде лекционных и лабораторных занятий, групповых и индивидуальных форм работы, самостоятельной работы студентов.

Методические рекомендации по подготовке студентов к лабораторным занятиям.

Для лучшего усвоения и закрепления материала по данной дисциплине студентам необходимо научиться работать с литературой. Изучение дисциплины предполагает в том числе отслеживание публикаций в периодических изданиях и работу с Internet.

При подготовке к практическим занятиям студенты должны изучить рекомендованную литературу, ответить на вопросы и выполнить все задания для самостоятельной работы. При подготовке целесообразно на основе изучения рекомендованной литературы выписать в конспект основные категории и понятия по учебной дисциплине, подготовить развернутые планы ответов и краткое содержание выполненных заданий.

Методические рекомендации студентам по организации самостоятельной работы по изучению литературных источников.

При организации самостоятельной работы, следует обратить особое внимание на регулярность изучения литературы. В период изучения литературных источников необходимо так же вести конспект. В случае затруднений необходимо обратиться к преподавателю за разъяснениями.

Методические рекомендации студентам по подготовке к зачету.

При подготовке к зачету следует руководствоваться РПД**.** Студент должен иметь в виду, что некоторые вопросы, имеющиеся в программе, выносятся на самостоятельное изучение.

На зачете студент должен показать знание содержания предмета, терминологии, умение свободно оперировать ею. При подготовке к ответу на зачете студенту разрешено пользоваться рабочей программой дисциплины. Если студент при ответе на вопросы затрудняется с самостоятельным изложением материала, преподаватель имеет право задать ему ряд вопросов, побуждающих и направляющих студентов к полному высказыванию по данной теме, в случае, если ответы на эти вопросы исчерпывают тему, оценка за ответ не снижается. Высказывания студентов должны соответствовать сути вопроса, быть логически выстроенными, доказательно раскрывать отношение отвечающего к излагаемой проблеме, выявлять личную точку зрения на использование тех или иных положений теоретического курса в практической работе.

Промежуточная аттестация может быть выставлена студенту по результатам федерального интернет тестирования (ФЭПО, интернет тренажеры).

5.2.Организация самостоятельной работы студента по дисциплине

Самостоятельная работа студента является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.

Организация самостоятельной работы студентов осуществляется по трем направлениям:

- определение цели, программы, плана задания или работы;
- со стороны преподавателя студенту оказывается помощь в технике изучения материала, подборе литературы для ознакомления;
- контроль усвоения знаний, приобретения навыков по дисциплине.

Мерами по обеспечению выполнения обучающимися всех видов самостоятельной работы являются (указать при наличии ниже перечисленных пунктов):

- обеспечение средствами вычислительной техники, программными средствами;
- обеспечение учебно-методической и справочной литературой всех видов самостоятельной.

Дисциплина обеспечена учебно-методической литературой в объеме, достаточном для проведения всех предусмотренных видов учебных занятий.

Каждый обучающийся по дисциплине должен быть обеспечен учебно-методической литературой.

Проведение всех видов занятий (лекционные, лабораторные и т.д.) при преподавании дисциплины, проведение консультаций, промежуточная и текущая аттестация возможна с применения электронного обучения и дистанционных образовательных технологий.

5.3.Особенности преподавания дисциплины

В целях максимального усвоения дисциплины используются следующие технологии обучения:

- лекция - учебное занятие, составляющее основу теоретического обучения и дающее систематизированные основы научных знаний по дисциплине, раскрывающее состояние и перспективы развития соответствующей области науки и техники, концентрирующее внимание обучающихся на наиболее сложных, узловых вопросах, стимулирующее их познавательную деятельность и способствующее формированию творческого мышления.
- лабораторное занятие - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путем творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности, а также самостоятельное индивидуальное решение практических задач

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

Информационные технологии: использование электронных образовательных ресурсов (электронный конспект, размещенный в локальной сети) при подготовке к лекциям, практическим и лабораторным занятиям.

Проблемное обучение: стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретных задач при выполнении домашних и лабораторных работ.

Контекстное обучение: мотивация студентов к усвоению знаний путем выявления связей между конкретным знанием и его применением для решения профессиональных задач при выполнении домашних заданий.

Обучение на основе опыта: активизация познавательной деятельности студента за счет ассоциации и собственного опыта с предметом изучения при выполнении домашних заданий.

Междисциплинарное обучение: использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи на лекциях и практических занятиях.

5.4.Материально-техническое обеспечение дисциплины

1. Аудитории для проведения занятий лекционного типа
2. Презентационный комплект (ноутбук, проектор, экран)
3. Аудитории для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютеры 14шт. с возможностью подключения к сети «Интернет»)
4. Аудитории для самостоятельной работы (Компьютерный класс. Локальная сеть. Подключение к сети Интернет. Электронные базы данных)

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства*:*

1. Microsoft Windows 7 Professional, 8 Pro, 8.1 Pro, 10 Pro

2. Microsoft Office Professional Plus 2007, 2010, 2013, 2016.

Состав продукта:

Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook, Microsoft Publisher, Microsoft Access, Microsoft OneNote, Microsoft InfoPath.

При организации занятий, текущей и промежуточной аттестации с применением электронного обучения и дистанционных образовательных технологий используются различные электронные образовательные ресурсы и онлайн сервисы, входящие в состав ЭИОС СГУ.

5.5.Методическое обеспечение образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья

Условия организации и содержание обучения и контроля знаний инвалидов и обучающихся с ОВЗ по дисциплине определяются программой дисциплины, адаптированной при необходимости для обучения указанных обучающихся.

Организация обучения, текущей и промежуточной аттестации студентов-инвалидов и студентов с ОВЗ осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Исходя из психофизического развития и состояния здоровья студентов-инвалидов и студентов с ОВЗ, организуются занятия совместно с другими обучающимися в общих группах, используя социально-активные и рефлексивные методы обучения создания комфортного психологического климата в студенческой группе или, при соответствующем заявлении такого обучающегося, по индивидуальной программе, которая является модифицированным вариантом основной рабочей программы дисциплины. При этом содержание программы дисциплины не изменяется. Изменяются, как правило, формы обучения и контроля знаний, образовательные технологии и дидактические материалы.

Обучение студентов-инвалидов и студентов с ОВЗ также может осуществляться индивидуально и/или с применением дистанционных технологий.

Дистанционное обучение обеспечивает возможность коммуникаций с преподавателем, а так же с другими обучаемыми посредством вебинаров (например, с использованием программы Skype) , что способствует сплочению группы, направляет учебную группу на совместную работу, обсуждение, принятие группового решения.

В учебном процессе для повышения уровня восприятия и переработки учебной информации студентов-инвалидов и студентов с ОВЗ применяются мультимедийные и специализированные технические средства приема-передачи учебной информации в доступных формах для студентов с различными нарушениями, обеспечивается выпуск альтернативных форматов печатных материалов (крупный шрифт), электронных образовательных ресурсов в формах, адаптированных к ограничениям здоровья обучающихся, наличие необходимого материально-технического оснащения.

Подбор и разработка учебных материалов производится преподавателем с учетом того, чтобы студенты с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся инвалидов и лиц с ОВЗ фонд оценочных средств по дисциплине, позволяющий оценить достижение ими результатов обучения и уровень сформированности компетенций, предусмотренных учебным планом и рабочей программой дисциплины, адаптируется для обучающихся инвалидов и лиц с ограниченными возможностями здоровья с учетом индивидуальных психофизиологических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.

Приложение к рабочей программе дисциплины

09.04.03 Прикладная информатика (магистратура)
Профиль: « Информационно-аналитическое обеспечение принятия решений»

АННОТАЦИЯ

рабочей программы дисциплины
Прикладная криптография
дисциплина к дисциплинам части учебного плана, формируемой участниками образовательных отношений, .
Очная форма обучения

Общая трудоемкость дисциплины (ЗЕТ / час.)	3/108
Цель изучения дисциплины	изучение основных подходов, методов и алгоритмов современной криптографии.
Содержание дисциплины	Тема 1. Основные понятия криптографии Тема 2. Методы шифрования с закрытым ключом Тема 3. Принципы построения блочных шифров с закрытым ключом Тема 4. Алгоритмы шифрования DES и AES Тема 5. Алгоритм криптографического преобразования данных ГОСТ 28147-89 Тема 6. Криптографические хеш-функции Тема 7. Поточные шифры и генераторы псевдослучайных чисел. Часть 1 Тема 8. Поточные шифры и генераторы псевдослучайных чисел. Часть 2 Тема 9. Введение в криптографию с открытым ключом Тема 10. Основные положения теории чисел, используемые в криптографии с открытым ключом Тема 11. Криптографические алгоритмы с открытым ключом и их использование Тема 12. Электронно-цифровая подпись Тема 13. Совершенно секретные системы Тема 14. Шифрование, помехоустойчивое кодирование и сжатие информации
Формируемые компетенции (коды)	ПК-1
Коды и наименование индикатора достижения компетенции	ПК-1.1 Демонстрирует знание теории систем и системного анализа, теории управления; инструментов и методов оценки качества, надежности и информационной безопасности ИС; устройства и возможностей современных ИС; нормативно-технических документов, описывающие качество, надежности и информационную безопасность ИС; ПК-1.2 Анализирует исходные данные по качеству, надежности и информационной безопасности ИС; планирует, распределяет и контролирует выполнение работ; разрабатывает регламентные документы в области качества, надежности и информационной безопасности; ПК-1.3 Применяет навыки обеспечения соответствия процесса развертывания ИС у заказчика принятым в организации или проекте стандартам и технологиям; навыки разработки и согласования регламентов по управлению качеством, надежностью и информационной безопасностью ИС; навыки выбора и внедрения инструментов и методов контроля качества
Дисциплины, участвующие в формировании компетенции	Компьютерная безопасность и управление корпоративными информационными системами Поддержка жизненного цикла корпоративных информационных систем Методы и инструментарии конкурентной разведки Когнитивная бизнес-аналитика Теория систем и системный анализ (продвинутый уровень) Проектно-технологическая практика Преддипломная практика
Образовательные технологии	Лекция, лабораторная работа; самостоятельная работа студента
Форма промежуточной аттестации	Зачет