МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«26» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки **01.03.02 Прикладная математика и информатика**

Направленность (профиль) Математические и информационные технологии в цифровой экономике

Программирование и информационные технологии

Математическое моделирование в естествознании и технологиях

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2023

Рабочая программа дисциплины «Основы информационной безопасности» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.02 Прикладная математика и информатика.

Программу составил: Савин В.Н.,
к.т.н., доцент кафедры прикладной математики

Рабочая программа дисциплины «Основы информационной безопасности» утверждена на заседании кафедры прикладной математики
протокол № 10 от 18.05.2023 г.

И.о. заведующего кафедрой, к.ф.-м.н.,
А.В. Письменский

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 5 от 19.05.2023 г.

Председатель УМК факультета компьютерных технологий и прикладной математики
А.В. Коваленко, д.ф.-м.н, к.э.н., доцент

Рецензенты:

Шапошникова Татьяна Леонидовна.
Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Зав. каф. физики института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.
Доктор техничеметодских наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки «Прикладная информатика», в рамках которой преподается дисциплина.

Целью дисциплины «Основы информационной безопасности» является развитие логического мышления, овладение основными методами обеспечения информационной безопасности, в том числе криптографических, умение самостоятельно расширять знания в области обеспечения информационной безопасности.

1.2 Задачи дисциплины

- изучение основных понятий и методов решения типовых задач информационной безопасности;
- овладение практическими навыками в реализации информационной безопасности.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к части, формируемой участниками образовательных отношений (Б1.В) учебного плана.

Для изучения данной учебной дисциплины (модуля) студент должен владеть обязательным минимумом содержания математической части ООП для данного направления:

знать/понимать

- основные понятия и методы математического анализа, аналитической геометрии, линейной алгебры, принципы алгоритмизации и программирования;

уметь

- применять математические методы для решения практических задач;
- составлять алгоритмы и компьютерные программы;

владеть

- методами решения алгебраических уравнений, аналитической геометрии, теории вероятностей;
- инструментальными средствами программирования.

Вышеуказанные знания, умения и навыки формируются предшествующими дисциплинами:

- Алгебра и аналитическая геометрия.
- Математический анализ.
- Основы программирования.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

- Новые информационные технологии в экономике.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных компетенций (ОПК):

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
1.	УК-2 Способен определять круг	- основные требования,	обоснованно выбрать	методами анализа существующих

№ п.п.	Код и наименование компетенции	Индикаторы достижения компетенции		
		знает	**умеет**	**владеет**
	задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	предъявляемые к криптографических системам: конфиденциальность, целостность, доступность	криптографический метод, разработать алгоритм решения поставленной задачи в рамках теоретического и экспериментального исследования;	алгоритмов шифрования
2.	ОПК-1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	- вычислительные методы в алгебре; - методы приближенного вычисления сеточных функций;	понимать принципы работы современных информационных технологий и программных средств, в которых применяются численные методы	вычислительным и методами решения задач линейной алгебры, оптимизационных задач для функции одной и нескольких переменных, методами дискретной математики и функционального анализа
3.	ПК-3 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов	- криптографические методы защиты информации	составить и отладить программу на алгоритмическом языке (Паскаль / C++/ Phyton/ Julia) для решения несложных криптографических задач	инструментарием разработки программной реализации вычислительных алгоритмов

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Трудоемкость, часов
		7 семестр
Контактная работа, в том числе:		**72,2**
Аудиторные занятия:		**68**
Занятия лекционного типа (Л)		34
Занятия семинарского типа (семинары, практические занятия) (ПЗ)		–
Лабораторные работы (ЛР)		34
Иная контактная работа:		**4,2**
Контроль самостоятельной работы (КСР)		4
Промежуточная аттестация (ИКР)		0,2
Самостоятельная работа, в том числе:		**35.8**
Курсовой проект (КП), курсовая работа (КР)		–
Проработка учебного (теоретического) материала (ПМ)		20
Подготовка к текущему контролю (ПТК)		15,8
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		–
Реферат (Р)		–
Контроль: подготовка к зачету		–
Общая трудоемкость	**час.**	**108**
	зач. ед.	**3**

2.2 Структура учебной дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов, *тем*	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Введение в основы информационной безопасности	6	2	-	2	2
	1. Исторический обзор применения средств сокрытия информации. История криптографии.	*6*	*2*	-	*2*	*2*
2.	Основные классы шифров и их свойства	16	6	-	6	4
	1. Шифры перестановки.	*6*	*2*	-	*2*	*2*
	2. Блочные шифры замены	*10*	*4*	-	*4*	*2*
3.	Надёжность шифров	12	4	-	4	4
	Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Практически стойкие шифры.	*12*	*4*	-	*4*	*4*
4.	Методы синтеза и анализа симметричных шифрсистем	20	8	-	8	4
	1. Управление открытыми ключами.	*10*	*4*	-	*4*	*2*
	2 Методы анализа криптографических алгоритмов.	*10*	*4*	-	*4*	*2*
5.	Методы синтеза и анализа асимметричных криптосистем	20	8	-	8	4
	1 Системы шифрования с открытым ключом.	*10*	*4*	-	*4*	*2*

	2 Алгоритмы идентификации на основе асимметричных криптосистем.	*10*	*4*	-	*4*	*2*
6.	Хеш-функции и их криптографические приложения	14	6	-	6	2
	Хеш-функции и аутентификация сообщений. Общие сведения о хеш-функциях.	*14*	*6*	-	*6*	*2*
	ИТОГО по разделам дисциплины:	**88**	**34**	**0**	**34**	**20**
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	15,8				
	Общая трудоемкость по дисциплине	**108**				

Сокращения: Л – лекции, ПЗ – практические занятия, ЛР – лабораторные работы, СРС – самостоятельная работа студентов.

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Введение в основы информационной безопасности	Исторический обзор применения средств сокрытия информации. Открытые сообщения и их характеристики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста. Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы	Тестирование, написание реферата (по желанию)

2.	Основные классы шифров и их свойства	1. Шифры перестановки. Разновидности шиф- ров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана 2. Блочные шифры замены Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES (RIJNDAEL).	Тестирование, написание реферата (по желанию)
3.	Надёжность шифров	Основы теории К. Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры. Вопросы имитозащиты. Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации. Помехоустойчивость шифров. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.	Тестирование, написание реферата (по желанию)

4.	Методы синтеза и анализа симметричных шифрсистем	1. Управление открытыми ключами. Принципы построения криптографических алгоритмов. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Режимы использования блочных шифров и их особенности. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров. Строение поточных шифрсистем. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Генераторы на основе линейных регистров сдвига. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Алгоритм Берлекемпа-Месси. Методы усложнения ЛРП Фильтрующие и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига. 2 Методы анализа криптографических алгоритмов. Подходы к анализу алгоритмов шифрования. Классификация методов анализа криптографических алгоритмов. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы. Особенности криптоанализа алгоритмов блочного шифрования. Особенности анализа программных реализаций криптографических алгоритмов.	Тестирование, написание реферата (по желанию)

5.	Методы синтеза и анализа асимметричных криптосистем	1 Системы шифрования с открытым ключом Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA. Практи ческие аспекты использования шифрсистем с открытым ключом. Алгоритмы цифровых под-писей. Общие положения. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой под-писи. 2 Алгоритмы идентификации на основе асимметричных криптосистем. Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением. Алгоритмы распределения ключей Алгоритмы передачи ключей(с использованием и без использования цифровой подписи).Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.	Тестирование, написание реферата (по желанию)
6.	Хеш-функции и их криптографические приложения	Хеш-функции и их криптографические приложения Хеш-функции и аутентификация сообщений. Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции. Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC. Конструкции MAC на основе симметричного шифрования. Система CBC-MAC. Основы анализа CBC-MAC: атака на основе наличия коллизий, использование CBC-MAC для аутентификации сообщений переменной длины. Другие системы: EMAC, XOR-MAC, PCS-MAC. Системы, совмещающие конфиденциальность и аутентификацию на одном ключе: CCM, OCB.	Тестирование, написание реферата (по желанию)

2.3.2 Занятия семинарского типа

Семинарские занятия не предусмотрены учебным планом.

2.3.3 Лабораторные занятия

№	Наименование раздела	Содержание раздела (номера и наименования лабораторных работ)	Форма текущего контроля
1	2	3	4

1.	Введение в основы информационной безопасности	Методика исследования свойств открытого текста по повторяемости и чередованию гласных и согласных букв (Markov, TextStat) Генераторы случайных последовательностей Линейный конгруэнтный метод Метод вычетов. Генератор псевдослучайных чисел согласно ГОСТ Р 34.11-94	Защита ЛР
2.	Основные классы шифров и их свойства	Моделирование полиномиального шифрования с помощью программы Cycle. Моделирование алгоритма IDEA с помощью программы IDEA (IdeaPro).	Защита ЛР
3.	Надёжность шифров	Тестирование алгоритмов шифрования с помощью системы CAP (CryptographicAnalysisProgram).	Защита ЛР
4.	Методы синтеза и анализа симметричных шифрсистем	Моделирование процесса шифрования и дешифрования для симметричного алгоритма шифрования DES с помощью программы DES	Защита ЛР
5.	Методы синтеза и анализа асимметричных криптосистем	SimpleNumber. Алгоритм Евклида, простые числа и тест Миллера-Рабина. RSA. Алгоритмы дискретного логарифмирования	Защита ЛР
6.	Хеш-функции и их криптографические приложения	Моделирование хеш-функций SHA1, MD4, MD5, с использованием программы HASH.	Защита ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены учебным планом.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающегося по дисциплине

Целью самостоятельной работы студента является углубление знаний, полученных в результате аудиторных занятий. Вырабатываются навыки самостоятельной работы. Закрепляются опыт и знания, полученные во время лабораторных занятий. Ниже представлен перечень учебно-методических материалов, которые помогают обучающемуся организовать самостоятельное изучение тем (вопросов) дисциплины по всем видам СРС.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка и повторение лекционного материала, материала учебной и научной литературы, подготовка к семинарским занятиям	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
2	Подготовка к лабораторным занятиям	Методические указания по выполнению лабораторных работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
3	Подготовка к решению задач и тестов	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
4	Подготовка докладов	Методические указания для подготовки эссе, рефератов, курсовых работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
5	Подготовка к решению расчетно-графических заданий (РГЗ)	Методические указания по выполнению расчетно-графических заданий, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.
6	Подготовка к текущему контролю	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №10 от 15.05.2019 г.

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 расширен и конкретизирован в зависимости от контингента обучающихся.

3 Образовательные технологии

Лекционные материалы реализуются с помощью электронных презентаций. При реализации учебной работы по дисциплине «Основы информационной безопасности» используются следующие образовательные технологии:

- интерактивная подача материала с мультимедийной системой;
- разбор конкретных исследовательских задач.

Объем интерактивных занятий – 18% от объема аудиторных занятий

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
7	*Л*	Интерактивная подача материала с мультимедийной системой. Обсуждение сложных и дискуссионных вопросов.	*10*
	ЛР	Компьютерные занятия в режимах взаимодействия «преподаватель - студент».	*2*
ИТОГО			*12*

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4 Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Основы информационной безопасности».

Оценочные средства включает контрольные материалы для проведения текущего контроля в форме тестовых заданий для защиты лабораторных работ, промежуточной аттестации в форме вопросов и заданий к экзамену.

В качестве оценочных средств, используемых для текущего контроля успеваемости, предлагается перечень вопросов по выполненным лабораторным работам, которые прорабатываются в процессе освоения курса. Данный перечень охватывает все основные разделы курса, включая знания, получаемые во время самостоятельной работы. Кроме того, важным элементом технологии является самостоятельное решение студентами и сдача индивидуальных проектных заданий в конце курса. Студент демонстрирует свое решение преподавателю, отвечает на дополнительные вопросы.

4.1.1 Примерные задания для защиты лабораторных работ

1 Для заданного n найти функцию Эйлера: 1) 13; 2) 17; 3) 25; 4) 34; 5) 165; 6) 98.

2 Для заданного n найти все первообразные корни: 1) 5; 2) 7; 3) 10; 4) 13; 5) 14; 6) 17.

3 Вычислить хеш-образ.

4.1.2 Примерные задания для тестирования учащихся

Контроль знаний студентов на всех этапах осуществляется путем компьютерного тестирования. Время проведения тестирования составляет, как правило, 30 мин. Ниже приведены примеры демо-версий тестов.

Бланк заданий

1. Шифрование – это…
=а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
в) удобная среда для вычисления конечного пользователя
г) способ скрытой передачи информации

2. Алфавит в криптографии – это…
а) последовательность букв языка
=б) конечное множество используемых для кодирования информации знаков
в) буквы текста
г) допустимый набор сообщений для кодирования

3. Электронной подписью называется…
а) файл с отсканированной подписью
=б) присоединяемое к тексту его криптографическое преобразование
в) текст
г) зашифрованный текст.

4. Чем отличается блок-схема алгоритма ГОСТ-89 от блок-схемы DES-алгоритма
а) наличием закрытого ключа
=б) отсутствием начальной перестановки и числом циклов шифрования
в) длиной ключа
г) методом шифрования

5.Какие из методов относятся к шифрованию с открытым ключом?
=а) RSA.
б) Кузнечик.
=в) схема Эль-Гамаля.
г) DES.

6. Какую секретную информацию хранит Windows
а) объём оперативной памяти
=б) пароли для доступа в Интернет
=в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
г) версия БИОС

7. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
=а) знание алгоритма шифрования не должно влиять на надежность защиты
б) секретность обеспечивается сокрытием факта передачи информации
=в) структурные элементы алгоритма шифрования должны быть неизменными
=г) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

8. Какие методы шифрования считаются устаревшими
=а) Цезаря
б) RSA
в) AES
=г) однозначной замены

9. (11010110) $\oplus$ (01101011)
=10111101

10. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования?
=1

11. Вычислите 4*32 по модулю 43
=42

12. Соотнесите название методов и их классификацию
DES =симметричная система шифрования
Схема Эль-Гамаля = симметричная система шифрования
SHA-2= метод хеширования

13. Раскрытие ключа шифрования не является проблемой для [1] шифрования
= асимметричного
симметричного
вероятностного

14. Для подтверждения целостности сообщения используется [1] .
= электронная подпись
копирование
симметричное шифрование

4.2 Фонд оценочных средств для проведения промежуточной аттестации

4.2.1 Примерный перечень вопросов к зачёту.

1. Исторический обзор. Открытые сообщения и их характеристики
2. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки.
3. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста.
4. Основы теории К.Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры.
5. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование.
6. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.
7. Шифры перестановки. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки.
8. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены.
9. Схема Фейстеля и не-Фейстеля
10. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы,
11. Криптоанализ шифра Виженера. Тесты У.Фридмана.
12. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры.
13. Криптоалгоритм DES.
14. Криптоалгоритм ГОСТ-28147-89.
15. Криптоалгоритм ГОСТ Р 34.12 -2015 «Кузнечик».
16. Криптоалгоритм ГОСТ Р 34.12 -2015 «Магма».
17. Криптоалгоритм RIJNDAEL (AES).

18. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры.
19. Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки.
20. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации.
21. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.
22. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Режимы использования блочных шифров и их особенности.
23. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров. Строение поточных шифрсистем.
24. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
25. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел.
26. Генераторы на основе линейных регистров сдвига.
27. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Алгоритм Берлекемпа-Месси.
28. Методы усложнения ЛРП. Фильтрующие и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига.
29. Подходы к анализу алгоритмов шифрования. Классификация методов анализа криптографических алгоритмов. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы.
30. Особенности криптоанализа алгоритмов блочного шифрования. Особенности анализа программных реализаций криптографических алгоритмов.
31. Тесты чисел на простоту, причина появления, классификация.
32. Основные принципы построения асимметричных криптосистем. Стойкость.
33. Практические аспекты использования шифрсистем с открытым ключом.
34. Алгоритмы цифровых подписей. Общие положения. Цифровые подписи на основе шифрсистем с открытым ключом. ГОСТ Р 34.10-2012
35. Открытое шифрование и электронная подпись.
36. Основные результаты статьи У. Диффи и М. Хеллмана.
37. Однонаправленные функции, построение однонаправленных функций с секретами. Система RSA. Использование алгоритма Евклида для расчета секретного ключа d.
38. Алгоритма цифровой подписи Эль-Гамаля, преимущества по сравнению с методом RSA, недостатки.
39. Проблема дискретного логарифмирования, аутентификация.
40. Система открытого шифрования RSA, атаки на RSA.
41. Система электронной подписи Эль-Гамаля (EGSA - ElGamal Signature Algorithm)
42. Система открытого шифрования Эль-Гамаля.
43. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи.
44. Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции.
45. Хеш-функции семейства "Стрибог ГОСТ Р 34.11– 2012 г.
46. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
47. Стандарт GSM, механизмы безопасности.
48. Теорема Левина-Кука «P=NP?», влияние на криптографию.

49. Квантовые алгоритмы шифрования

4.2.2 Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает стандартные методы решений в теории чисел, допускает незначительные ошибки; студент умеет правильно объяснять изученный материал, иллюстрируя его примерами задач.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры по изученной теме, довольно ограниченный объем знаний программного материала. Отметка «не зачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

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 дополнен и конкретизирован в зависимости от контингента обучающихся.

5 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература

1. Фомичев, В. М. Криптография — наука о тайнописи: учебное пособие / В. М. Фомичев. - Москва : Прометей, 2020. - 66 с. - ISBN 978-5-00172-040-9. - Текст : электронный. - Режим доступа: https://znanium.com/read?id=389799

2. Бабаш, А. В. Криптографические методы защиты информации.Т.1:Уч.-метод.пос./Бабаш А. В., 2-е изд. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 413 с.: - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=334834

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература

3. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст: электронный. - Режим доступа: https://znanium.com/read?id=416723

6 Методические указания для обучающихся по освоению дисциплины

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

По желанию студента предлагается написание реферата на выбранную им тему (по согласованию с преподавателем). Для написания реферата необходимо подобрать литературу. Общее количество литературных источников, включая тексты из Интернета, (публикации в журналах), должно составлять не менее 10 наименований. Учебники, как правило, в литературные источники не входят.

Рефераты выполняют на листах формата А4. Страницы текста, рисунки, формулы нумеруют, рисунки снабжают порисуночными надписями. Текст следует печатать шрифтом №14 с интервалом между строками в 1,5 интервала, без недопустимых сокращений. В конце реферата должны быть сделаны выводы.

В конце работы приводят список использованных источников.

Реферат должен быть подписан студентом с указанием даты ее оформления.

Работы, выполненные без соблюдения перечисленных требований, возвращаются на доработку.

Выполненная студентом работа определяется на проверку преподавателю в установленные сроки. Если у преподавателя есть замечания, работа возвращается и после исправлений либо вновь отправляется на проверку, если исправления существенные, либо предъявляется на ее защите.

Примерные темы рефератов:

1. Анализ одного из законов по информационной безопасности.
2. Симметричные шифры
3. Анализ уязвимостей RSA.
4. Угрозы безопасности, связанные с квантовыми компьютерами.
5. Анализ криптостойкости алгоритма «Кузнечик».

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 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

7.1 Перечень информационно-коммуникационных технологий

– Проверка домашних заданий и консультирование посредством ЭИОС, электронной почты и социальной сети «ВКонтакте».

– Использование электронных презентаций при проведении лекционных и лабораторных занятий.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

1. Операционная система MS Windows.
2. Интегрированное офисное приложение MS Office.
3. Система программирования MS Visual Studio или Delphi.

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

1. Портал CrypTool (CTP) https://www.cryptool.org/. Его цель - повысить осведомленность и интерес к криптотехнологиям для всех. Проект CT разрабатывает самые распространенные в мире бесплатные программы электронного обучения в области криптографии и криптоанализа. Все учебные программы в проекте CT имеют открытый исходный код и доступны бесплатно.
2. Википедия, свободная энциклопедия – Wikipedia [Электронный ресурс]. - URL: http://ru.wikipedia.org.
3. Электронная библиотека КубГУ [Электронный ресурс]. - URL: http://www.kubsu.ru/ru/node/1145.
4. Электронная библиотечная система eLIBRARY.RU [Электронный ресурс]. - URL: http://www.elibrary.ru.
5. Профессиональная база данных zbMath [Электронный ресурс]. - URL: https://zbmath.org/.

8 Материально-техническое обеспечение по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), соответствующим программным обеспечением, а также необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307)
2.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью, техническими средствами обучения (современными ПЭВМ на базе процессоров Intel или AMD, объединёнными локальной сетью) с выходом в глобальную сеть Интернет, а также современным лицензионным программным обеспечением (операционная система Windows 8/10, пакет Microsoft Office, среды программирования MS Visual Studio и Delphi) (аудитории: 101, 102, 105, 106, 107, А301а)

3.	Групповые (индивидуальные) консультации	Аудитория для семинарских занятий, групповых и индивидуальных консультаций, укомплектованные необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131)
4.	Текущий контроль, промежуточная аттестация	Аудитория для семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованная необходимой мебелью (доска, столы, стулья) (аудитории: 129, 131, 133, А305, А307, 147, 148, 149, 150, 100С, А3016, А512), компьютерами с лицензионным программным обеспечением и выходом в интернет (аудитории: 106, 106а. А301)
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети Интернет, программой экранного увеличения, обеспеченный доступом в электронную информационно-образовательную среду университета, необходимой мебелью (доска, столы, стулья) (аудитория 102а, читальный зал).