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.
«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.04 Основы информационной безопасности

Направление
подготовки/специальность 01.03.02 Прикладная математика и информатика

Направленность (профиль) /
специализация Программирование и информационные технологии

Форма обучения Очная

Квалификация Бакалавр

Краснодар 2025

Рабочая программа дисциплины Основы информационной безопасности составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 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 № 9 от 06.05.2025 г.

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

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 4 от 23.05.2025 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».

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

1 Цели и задачи изучения дисциплины (модуля)

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 (модуля) в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к обязательной части Блока 1 "Дисциплины (модули)" учебного плана.

Входными знаниями для освоения данной дисциплины являются знания, умения и навыки, полученные студентами в процессе изучения дисциплин

- 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 (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора*	Результаты обучения по дисциплине
УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	
Знать ИУК-3.1 (Зн.1) Проблемы подбора эффективной команды ИУК-3.3 (Зн.3) Основы стратегического управления человеческими ресурсами, нормативные правовые акты, касающиеся организации и осуществления профессиональной деятельности ИУК-3.4 (Зн.4) Модели организационного поведения, факторы формирования организационных отношений ИУК-3.5 (Зн.5) Стратегии и принципы командной работы, основные характеристики организационного климата и взаимодействия людей в организации	Уметь ИУК-3.13 (06.001 D/03.06 У.3) Осуществлять осуществлять социальное взаимодействие, коммуникации с заинтересованными сторонами Владеть ИУК-3.15 (В.1) Организацией и управлением командным взаимодействием в решении поставленных целей ИУК-3.18 (В.4) Составлением деловых писем с целью организации и сопровождения командной работы
ПК-4 Способен активно участвовать в разработке системного и прикладного программного обеспечения	
Знать ИПК-4.1 (06.001 D/03.06 Зн.1) Принципы построения архитектуры системного и прикладного программного обеспечения и	Уметь ИПК-4.10 (06.001 D/03.06 У.1) Использовать существующие типовые решения и шаблоны

Код и наименование индикатора*	Результаты обучения по дисциплине
виды архитектуры системного и прикладного программного обеспечения ИПК-4.5 (06.015 В/16.5 Зн.3) Архитектура, устройство и функционирование вычислительных систем используемых в разработке системного и прикладного программного обеспечения ИПК-4.7 (06.016 А/06.6 Зн.1) Возможности ИС, предметная область системное и прикладное программное обеспечение ИПК-4.8 (06.016 А/30.6 Зн.1) Управление рисками проекта при разработке системного и прикладного программного обеспечения ИПК-4.9 (06.016 А/30.6 Зн.2) Возможности ИС, методы разработки прикладного программного обеспечения	проектирования системного и прикладного программного обеспечения ИПК-4.12 (06.016 А/30.6 У.2) Планировать работы в проектах разработки системного и прикладного программного обеспечения Владеть ИПК-4.17 (06.016 А/30.6 Тд.1) Качественный анализ рисков при разработке системного и прикладного программного обеспечения
ПК-8 Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции	
Знать ИПК-8.2 (06.016 А/30.6 Зн.1) Управление рисками проекта, способы планирования необходимых ресурсов и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции ИПК-8.3 (40.001 А/02.5 Зн.3) Методы, этапы и средства планирования и организации исследований и разработок ИПК-8.4 (06.015 В/16.5 У.1) Устанавливать программное обеспечение	Уметь ИПК-8.5 (06.016 А/06.6 У.1) Разрабатывать документы, составлять соответствующие технические описания и инструкции ИПК-8.6 (06.016 А/30.6 У.2) Планировать работы в проектах, необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий ИПК-8.7 (40.001 А/02.5 У.2) Оформлять результаты научно-исследовательских и опытно-конструкторских работ, составлять соответствующие технические описания и инструкции Владеть ИПК-8.9 (06.016 А/06.6 Тд.1) Подготовка договоров в проектах в соответствии с типовой формой, составление соответствующих технических описаний и инструкций ИПК-8.12 (40.001 А/02.5 Др.2 Тд.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, планирование необходимых ресурсов и этапов выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции

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

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

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зачетных единиц (108 часов), их распределение по видам работ представлено в таблице

Виды работ	Всего часов	Семестры (часы)
		7
Контактная работа, в том числе:	**72,2**	**72,2**
Аудиторные занятия (всего):	**68**	**68**

Занятия лекционного типа		34	34
Лабораторные занятия		34	34
Практические занятия			
Иная контактная работа:		**4,2**	**4,2**
Контроль самостоятельной работы (КСР)		4	4
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:		**35,8**	**35,8**
Самостоятельная работа		35,8	35,8
Подготовка к текущему контролю			
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час,**	**108**	**108**
	в том числе контактная работа	**72,2**	**72,2**
	зач, ед	**3**	**3**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) 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**				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) 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 шифров перестановки: маршрутные и геометрические 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. 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. Практические аспекты использования шифрсистем с открытым ключом. Алгоритмы цифровых подписей. Общие положения. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи. 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. Системы, совмещающие конфиденциальность и аутентификацию на одном ключе: CCM, OCB.	Тестирование, написание реферата (по желанию)

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

Семинарские занятия не предусмотрены учебным планом.

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены учебным планом.

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

№	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 18.05.2023 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №9 от 06.05.2025 г.
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 №9 от 06.05.2025 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 №9 от 06.05.2025 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 №9 от 06.05.2025 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 №9 от 06.05.2025 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №9 от 06.05.2025 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 №9 от 06.05.2025 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,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

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,
– в форме аудиофайла.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

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, 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.

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

4. 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 зачёту.

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.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	Знать ИУК-3.1 (Зн.1) Проблемы подбора эффективной команды ИУК-3.3 (Зн.3) Основы стратегического управления человеческими ресурсами, нормативные правовые акты, касающиеся организации и осуществления профессиональной деятельности ИУК-3.4 (Зн.4) Модели организационного поведения, факторы формирования организационных отношений ИУК-3.5 (Зн.5) Стратегии и принципы командной работы, основные характеристики организационного климата и взаимодействия людей в организации Уметь ИУК-3.13 (06.001 D/03.06 У.3) Осуществлять осуществлять социальное взаимодействие, коммуникации с заинтересованными сторонами Владеть ИУК-3.15 (В.1) Организацией и управлением командным взаимодействием в решении поставленных целей ИУК-3.18 (В.4) Составлением деловых писем с целью организации и сопровождения командной работы	опрос	Вопрос на зачет 1-20
2	ПК-4 Способен активно участвовать в разработке системного и прикладного программного обеспечения	Знать ИПК-4.1 (06.001 D/03.06 Зн.1) Принципы построения архитектуры системного и прикладного программного обеспечения и виды архитектуры системного и прикладного программного обеспечения ИПК-4.5 (06.015 B/16.5 Зн.3) Архитектура, устройство и функционирование вычислительных систем используемых в разработке системного и прикладного программного обеспечения ИПК-4.7 (06.016 A/06.6 Зн.1) Возможности ИС, предметная область системное и прикладное программное обеспечение ИПК-4.8 (06.016 A/30.6 Зн.1) Управление рисками проекта при разработке системного и прикладного программного обеспечения ИПК-4.9 (06.016 A/30.6 Зн.2) Возможности ИС, методы разработки	опрос	Вопрос на зачет 21-35

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
		прикладного программного обеспечения Уметь ИПК-4.10 (06.001 D/03.06 У.1) Использовать существующие типовые решения и шаблоны проектирования системного и прикладного программного обеспечения ИПК-4.12 (06.016 A/30.6 У.2) Планировать работы в проектах разработки системного и прикладного программного обеспечения Владеть ИПК-4.17 (06.016 A/30.6 Тд.1) Качественный анализ рисков при разработке системного и прикладного программного обеспечения		
3	ПК-8 Способен планировать необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции	Знать ИПК-8.2 (06.016 A/30.6 Зн.1) Управление рисками проекта, способы планирования необходимых ресурсов и этапы выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции ИПК-8.3 (40.001 A/02.5 Зн.3) Методы, этапы и средства планирования и организации исследований и разработок ИПК-8.4 (06.015 B/16.5 У.1) Устанавливать программное обеспечение Уметь ИПК-8.5 (06.016 A/06.6 У.1) Разрабатывать документы, составлять соответствующие технические описания и инструкции ИПК-8.6 (06.016 A/30.6 У.2) Планировать работы в проектах, необходимые ресурсы и этапы выполнения работ в области информационно-коммуникационных технологий ИПК-8.7 (40.001 A/02.5 У.2) Оформлять результаты научно-исследовательских и опытно-конструкторских работ, составлять соответствующие технические описания и инструкции Владеть ИПК-8.9 (06.016 A/06.6 Тд.1) Подготовка договоров в проектах в соответствии с типовой формой, составление соответствующих технических описаний и инструкций ИПК-8.12 (40.001 A/02.5 Др.2 Тд.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и	опрос	Вопрос на зачет 36-49

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
		многообразие актуальных способов решения задач, планирование необходимых ресурсов и этапов выполнения работ в области информационно-коммуникационных технологий, составлять соответствующие технические описания и инструкции		

Контроль знаний студентов на всех этапах осуществляется путем тестирования. Время проведения тестирования составляет, как правило, 30 мин. Ниже приведен пример демо-версии теста.

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. Вычислить (11010110) ⊕ (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

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. Алгоритм 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

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 конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная 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

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

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

5.2. Периодическая литература

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

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

Электронно-библиотечные системы (ЭБС):

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

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action

10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

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

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

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

6. Методические указания для обучающихся по освоению дисциплины (модуля)

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 5 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».
6. Анализ качества генерации псевдослучайной последовательности.

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

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

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Учебные аудитории для проведения занятий лекционного типа (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 10/11, пакет Microsoft Office, среды программирования MS Visual Studio) (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).

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

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Операционная система Windows 10/11, пакет Microsoft Office
Помещение для самостоятельной работы обучающихся (ауд 102а)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Операционная система Windows 10/11, пакет Microsoft Office