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

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.07 «Криптография и сетевая безопасность»

Направление подготовки 01.04.02 Прикладная математика и информатика

Профиль Технологии программирования и разработки информационно-коммуникационных систем

Форма обучения очная

Квалификация магистр

Краснодар 2025

Рабочая программа дисциплины «*Криптография и сетевая безопасность*» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направлению подготовки 01.04.02 Прикладная математика и информатика

Программу составил(и):
Осипян В. О., проф. кафедры анализа данных и искусственного интеллекта, доктор физ.-мат. наук

Рабочая программа дисциплины утверждена на заседании кафедры анализа данных и искусственного интеллекта протокол № 13 от «20» мая 2025г.

Заведующий кафедрой Коваленко А.В.

подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 4 от «23» мая 2025г.

подпись

Председатель УМК факультета Коваленко А.В.

Рецензенты:
Шапошникова Татьяна Леонидовна.

Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Директор института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

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

1. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и задачи дисциплины

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО по направлению подготовки 01.04.02 Прикладная математика и информатика, в рамках которой преподается дисциплина. Преподавание дисциплины Б1.О.07 «Криптография и сетевая безопасность» строится исходя из требуемого уровня базовой подготовки студентов магистратуры, обучающихся по направлению 01.04.02 Прикладная математика и информатика.

В современном мире безопасность информационных систем является важным аспектом стабильной и успешной работы в различных сферах деятельности человека, предприятий, государств, содружеств и т. д.

Конечными целями преподавания дисциплины являются:

– основы обеспечения компьютерной и сетевой безопасности;

− основы безопасности информационных экономических систем предприятия;

− знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных;

− владение основными алгоритмами математики криптографии; − знание и использование различных криптосистем шифрования.

Основа изучения дисциплины Б1.О.07 «Криптография и сетевая безопасность» – реализация требований, установленных Федеральным государственным образовательным стандартом высшего профессионального образования к подготовке студентов бакалавриата, обучающихся по направлению 01.04.02 Прикладная математика и информатика.

1.2 Задачи дисциплины

− научить студентов использовать в своей практической деятельности различные алгоритмы шифрования;

− ознакомить с компьютерными технологиями в области персональной и сетевой безопасности;

− привить студентам умения и навыки самостоятельного изучения специальной литературы по информационной безопасности.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.О.07 «Криптография и сетевая безопасность» относится к обязательной части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

Дисциплина изучается в 1-м семестре и использует разносторонние знания, полученные в предыдущих семестрах. Преподавание дисциплины ведется в виде лекций, лабораторных и самостоятельных занятий. Большая часть лекционного материала дается в интерактивном режиме. Основная цель лабораторных занятий – практическая реализация изученных методов.

Студенты, обучающиеся дисциплине «Криптография и сетевая безопасность» должны владеть навыками логического мышления. Обязательным для них является знание основ безопасности информационных систем. Студент должен уметь использовать навыки работы с алгоритмами защиты информации, технологиями и программами для решения изобретательских и нестандартных задач в области безопасности, в частности безопасности предприятия. Слушатель должен быть ***готов*** использовать знания, полученные в рамках дисциплины «Криптография и сетевая безопасность» в своей практической и научно-теоретической деятельности.

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:

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.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ОПК-1 Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	
ИОПК-1.1 Анализирует проблемы и формулирует задачи исследования. в области фундаментальной и прикладной математики	Знает: -основные теоретические основы криптографии и сетевой безопасности, связанные с математическими понятиями (теория чисел, алгебра, теория групп, теория вероятностей, комбинаторика и теория информации). -современные исследовательские направления и актуальные проблемы в области криптографических алгоритмов и протоколов. -методы анализа сложности и защищенности криптографических систем.
	Умеет -анализировать существующие математические модели и алгоритмы, используемые в криптографии и сетевой безопасности. -выявлять актуальные проблемы и недостатки в существующих методах и протоколах. -формулировать конкретные задачи исследования на основе анализа актуальных проблем и научных данных. -оценивать степень актуальности и практической значимости предстоящего исследования.
	Владеет: -навыками критического анализа проблем, связанных с безопасностью информации, и их формулировки.

	-способностью определять приоритетные направления исследований в области математических основ криптографии и сетевой безопасности.
ИОПК-1.2 Решает актуальные задачи фундаментальной и прикладной математики	Знает -основные математические методы и алгоритмы, применяемые для решения задач криптографии и сетевой безопасности — например, факторизация, дискретный логарифм, криптографические протоколы, теория информации и теория графов. -современные подходы к моделированию и анализу защищенности криптографических систем. -методы численного и теоретического анализа сложности алгоритмов и оценки их стойкости.
	Умеет -применять математические методы при решении конкретных задач, связанных с криптографией и безопасностью сетей. -разрабатывать и реализовывать алгоритмы для решения поставленных задач (например, генерация ключей, создание криптоустойчивых протоколов). -анализировать эффективность, безопасность и надежность криптографических решений. -оценивать риск уязвимостей и эффективности решений на основе математического анализа.
	Владеет -навыками практического применения математических методов для решения актуальных задач в области криптографической защиты информации и сетевой безопасности. -умением самостоятельно интерпретировать результаты математического анализа в контексте безопасности системы. -способностью искать пути улучшения и оптимизации существующих криптографических решений в соответствии с актуальными требованиями.
ОПК-3 Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности	
ИОПК-3.1 Анализирует проблемную область и разрабатывает математические модели для решения прикладных задач профессиональной деятельности	Знает: -основные понятия и требования к моделированию прикладных задач в области информационной безопасности, такие как моделирование угроз, анализ уязвимостей,

	оценка безопасности и эффективности криптографических протоколов. -стандартные математические методы и подходы для построения моделей — например, теория графов, математическая логика, теория вероятностей, теория информации, комбинаторика. -современные криптографические стандарты и протоколы, особенности их уязвимостей и анализа.
	Умеет -анализировать исходные данные прикладной задачи, выделять ключевые параметры и угрозы. -формулировать математическую модель, отражающую сущность и критериографии решения задач безопасности (например, моделирование атак, анализ вероятности уязвимостей). -разрабатывать алгоритмы и методы решения поставленных задач на основе выбранной модели. -оценивать эффективность и безопасность разработанных моделей и решений, интерпретировать полученные результаты.
	Владеет: -навыками профессионального анализа проблемной области и постановки конкретных прикладных задач. -умением разрабатывать адекватные математические модели, учитывающие специфику задач криптографии и сетевой безопасности. -способностью применять разработанные модели для тестирования криптографических протоколов, оценки уязвимостей и нахождения решений. -умением представлять результаты моделирования для последующей оценки и принятия решений специалистами по безопасности.
ИОПК-3.2 Исследует применимость и анализирует эффективность модели для решения прикладных задач профессиональной деятельности	Знает: Основные критерии эффективности криптографических моделей и протоколов. Методы анализа применимости и производительности решений.

	Умеет: Оценивать актуальность модели для конкретных задач в области безопасности. Анализировать эффективность и уязвимости модели на практике.
	Владеет: Навыками тестирования и оценки эффективности разработанных решений и моделей. Умением делать выводы о целесообразности использования модели в профессиональной деятельности.
ИОПК-3.3 Разрабатывает и реализует алгоритмы, структуры данных и программные модули для решения прикладных задач, исходя из требований проекта и особенностей задачи.	Знает: Основные алгоритмы криптографической защиты и принципы их реализации. Структуры данных и программные методы для обеспечения безопасности. Требования к пользовательским и системным криптографическим компонентам.
	Умеет: Анализировать прикладную задачу, выявлять требования безопасности. Проектировать и реализовать алгоритмы и модули, соответствующие поставленной задаче и требованиям проекта. Использовать языки программирования и средства разработки для интеграции криптографических решений.
	Владеет: Навыками написания программных модулей для криптографических приложений. Умением учитывать особенности и ограничения криптографических алгоритмов при кодировании. Способностью тестировать и оптимизировать реализованные криптоалгоритмы и модули.

**Вид индекса индикатора соответствует учебному плану.*

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 трудоемкости дисциплины по видам работ

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

Виды работ		Всего часов	Форма обучения
			очная
			1 семестр(часы)
Контактная работа, в том числе:			**56.3**
Аудиторные занятия (всего):			**56**
занятия лекционного типа			28
лабораторные занятия			28
практические занятия			-
семинарские занятия			-
Иная контактная работа:			**0,3**
Контроль самостоятельной работы (КСР)			
Промежуточная аттестация (ИКР)			0,3
Самостоятельная работа, в том числе:			**97**
Проработка учебного (теоретического) материала			36
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)			36
Подготовка к текущему контролю			36
Контроль:			**26.7**
Подготовка к экзамену			26,7
Общая трудоемкость	**час.**		**180**
	в том числе контактная работа		**26.7**
	зач. ед		**5**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 1семестре (очная форма обучения)

№	Наименование тем		Количество часов			
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Введение в дисциплину	21	4		4	13
2.	Математика криптографии	22	4		4	14
3.	Алгоритмы шифрования	22	4		4	14
4.	Безопасность информационных систем предприятия	22	4		4	14
5.	Алгоритмы реализации электронно-цифровой подписи	22	4		4	14
6.	Безопасность корпоративной сети	22	4		4	14
7.	Безопасность в клиентско-серверных приложений	22	4		4	14
	Итого по разделам:	153	28		28	97
	Промежуточная аттестация (ИКР)	0,3				
	Контроль самостоятельной работы (КСР)					

	Подготовка к экзамену	26,7				
	ИТОГО по дисциплине	**180**				

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1.	Введение в дисциплину	Информационная безопасность ПК/Предприятия– основные понятия; Криптография - основные понятия, стандартные задачи;	Р, К, Т
2.	Математика криптографии	Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Поля Галуа. Простые числа - испытания простоты.	Р, К, Т
3.	Алгоритмы шифрования	Основы современных шифров. Стандарт шифрования с симметричным ключом (DES, AES). Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамаля, эллиптических кривых).	Р, К, Т
4.	Безопасность информационных систем предприятия	Законодательство РФ в области защиты информации, обработки персональных данных, организации безопасности информационных систем на предприятии; Службы контроля исполнения законодательства РФ в области безопасности и алгоритмы взаимодействия с ними предприятия; Организация безопасной информационной системы предприятия	Р, К, Т
5.	Алгоритмы реализации электронно-цифровой подписи	Криптографические хэш-функции; Цифровая подпись; Установление подлинности объекта	Р, К, Т
6.	Безопасность корпоративной сети	Безопасность на транспортном уровне; Безопасность на сетевом уровне;	Р, К, Т
7.	Безопасность в клиентско-серверных приложений	Организация защиты клиентско-серверного приложения; Безопасная аутентификация (API)	Р, К, Т

2.3.2 Занятия семинарского типа

Занятия семинарского типа не предусмотрены учебным планом.

2.3.3 Лабораторные занятия

	Тематика лабораторных работ	Форма текущего контроля
1	3	4

	Тематика лабораторных работ	Форма текущего контроля
1	3	4
1.	Введение в дисциплину	Опрос по теоретическому материалу.
2.	Математика криптографии	Проверка программной реализации рассмотренных алгоритмов
3.	Алгоритмы шифрования	Проверка решений практических задач
4.	Безопасность информационных систем предприятия	Проверка программной реализации рассмотренных алгоритмов
5.	Алгоритмы реализации электронно- цифровой подписи	Проверка программной реализации рассмотренных алгоритмов
6.	Безопасность корпоративной сети	Отчет по лабораторной работе.
7.	Безопасность в клиентско-серверных приложений	Отчет по лабораторной работе.

2.3.4 Курсовые работы – не предусмотрены

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.

№	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 №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 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 №7 от 18.04.2018 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 №7 от 18.04.2018 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 №7 от 18.04.2018 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 №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 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 №7 от 18.04.2018 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 конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В процессе изучения дисциплины лекции, лабораторные занятия, консультации являются ведущими формами обучения в рамках лекционно-семинарской образовательной технологии.

Лекции излагаются в виде презентации с использованием мультимедийной аппаратуры. Данные материалы в электронной форме передаются студентам.

Основной целью лабораторных занятий является разбор практических ситуаций. Дополнительной целью лабораторных занятий является контроль усвоения пройденного материала. На лабораторных занятиях также осуществляется проверка выполнения заданий.

При проведении лабораторных занятий участники закрепляют пройденный материал путем обсуждения вопросов, требующих особого внимания и понимания, отвечают на вопросы преподавателя и других слушателей, осуществляют решения тестов, направленных на повторение лекционного материала и нормативных документов по изучаемой тематике, выполняют решение задач, которые способствуют развитию практических навыков в области изучаемой дисциплины.

В число видов работы, выполняемой слушателями самостоятельно, входят: 1) поиск и изучение литературы по рассматриваемой теме;

2) поиск и анализ научных статей, монографий по рассматриваемой теме; 3) разработка прикладных программ по рассматриваемой теме.

Интерактивные образовательные технологии, используемые в аудиторных занятиях: при реализации различных видов учебной работы (лекций и практических занятий) используются следующие образовательные технологии: дискуссии, презентации, конференции. В сочетании с внеаудиторной работой они создают дополнительные условия формирования и развития требуемых компетенций обучающихся, поскольку позволяют обеспечить активное взаимодействие всех участников. Эти методы способствуют личностно-ориентированному подходу.

Все перечисленные виды и формы учебной работы и текущего контроля направлены на формирование у обучающихся профессиональных компетенций, предусмотренных при планировании результатов обучения по дисциплине и соотнесенных с планируемыми результатами освоения образовательной программы.

Для инвалидов и лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения указанной дисциплины. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Вышеозначенные образовательные технологии дают наиболее эффективные результаты освоения дисциплины с позиций актуализации содержания темы занятия, выработки продуктивного мышления, терминологической грамотности и компетентности обучаемого в аспекте социально-направленной позиции будущего бакалавра, и мотивации к инициативному и творческому освоению учебного материала.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

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

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме коллоквиумов, рефератов и тестовых заданий и **промежуточной аттестации** в форме вопросов и заданий к экзамену.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-1	Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий	Р, К, Т	Вопрос на экзамене 1-10
2	ОПК-2	Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности	Р, К, Т	Вопрос на экзамене 11-20
3	ОПК-3	Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования	Р, К, Т	Вопрос на экзамене 21-30

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

Примерные темы рефератов

1. Основные виды криптографических алгоритмов и их применение в современных информационных систем
2. Протоколы обеспечения конфиденциальности в интернет-банкинге
3. Анализ угроз и методов защиты в сетевых инфраструктурах корпоративных сетей
4. Виды и особенности симметричных и асимметричных шифровальных систем
5. Технологии цифровых подписей и их роль в обеспечении целостности и аутентификации данных
6. Протоколы TLS и SSL: принципы работы и механизмы защиты передаваемой информации
7. Методы обнаружения и предотвращения атак типа «Man-in-the-middle» в сетевых протоколах
8. Введение в постквантовую криптографию: вызовы и перспективы развития
9. Использование систем VPN для обеспечения безопасности удаленного доступа
10. Современные подходы к управлению криптографическими ключами и инфраструктура PKI

Примерные темы для коллоквиумов

1. Основные виды криптографических алгоритмов и их применение в современных информационных систем
2. Протоколы обеспечения конфиденциальности в интернет-банкинге
3. Анализ угроз и методов защиты в сетевых инфраструктурах корпоративных сетей
4. Виды и особенности симметричных и асимметричных шифровальных систем
5. Технологии цифровых подписей и их роль в обеспечении целостности и аутентификации данных
6. Протоколы TLS и SSL: принципы работы и механизмы защиты передаваемой информации
7. Методы обнаружения и предотвращения атак типа «Man-in-the-middle» в сетевых протоколах
8. Введение в постквантовую криптографию: вызовы и перспективы развития

9. Использование систем VPN для обеспечения безопасности удаленного доступа
10. Современные подходы к управлению криптографическими ключами и инфраструктура PKI

Пример тестового задания

Тест по теме "Алгоритмы шифрования"

1. Что такое симметричный шифр?
a) Шифр, использующий один ключ для шифрования и расшифровки
b) Шифр, использующий два ключа: один для шифрования и другой для расшифровки
c) Шифр, основанный на публичных ключах и цифровых сертификатах
d) Алгоритм, использующий один алгоритм без использования ключа

Правильный ответ: a) Шифр, использующий один ключ для шифрования и расшифровки

2. Как называется метод шифрования, при котором используется два ключа — открытый и секретный?
a) Симметричный шифр
b) Асимметричный шифр
c) Хеш-функция
d) Цифровая подпись

Правильный ответ: b) Асимметричный шифр

3. Какой из перечисленных алгоритмов является блочным шифром?
a) RSA
b) AES
c) ElGamal
d) Diffie-Hellman

Правильный ответ: b) AES

4. Что такое потоковый шифр?
a) Алгоритм, шифрующий сообщение блоками фиксированного размера
b) Алгоритм, шифрующий один бит или байт за один цикл, обычно быстрее блочных технологий
c) Метод, использующий цепочки для шифрования больших сообщений
d) Алгоритм, использующий только asymmetric-ключи

Правильный ответ: b) Алгоритм, шифрующий один бит или байт за один цикл, обычно быстрее блочных технологий

5. Как называется знаменитый алгоритм симметричного шифрования, разработанный в 1977 году и широко используемый по сей день?
a) RSA
b) DES
c) AES
d) Blowfish

Правильный ответ: b) DES

6. В чем заключается основное отличие алгоритма AES от DES?
a) AES использует меньше ключей

b) AES работает только в режиме поточного шифра
c) AES использует более длинные ключи и имеет более современную структуру
d) DES более безопасен, чем AES

Правильный ответ: c) AES использует более длинные ключи и имеет более современную структуру

7. Что такое криптостойкость?
a) Способность алгоритма быстро шифровать данные
b) Устойчивость криптографических алгоритмов к атакующим воздействиям
c) Количество ключей, используемых в алгоритме
d) Степень сложности реализации алгоритма

Правильный ответ: b) Устойчивость криптографических алгоритмов к атакующим воздействиям

8. Какой метод шифрования используется в протоколе SSL/TLS для обмена ключами?
a) Симметричное шифрование
b) Асимметричное шифрование с помощью RSA или ECC
c) Хеш-функции
d) Односторонние функции

Правильный ответ: b) Асимметричное шифрование с помощью RSA или ECC

9. Что из перечисленного лучше всего описывает понятие "криптоанализ"?
a) Процесс шифрования данных
b) Анализ криптографической системы с целью поиска уязвимостей или секретных ключей
c) Метод генерации криптографических ключей
d) Протокол обмена ключами

Правильный ответ: b) Анализ криптографической системы с целью поиска уязвимостей или секретных ключей

10. Для каких целей наиболее часто применяется стандартизированный алгоритм AES?
a) Обеспечение конфиденциальности данных и соединений
b) Генерация случайных чисел
c) Аутентификация пользователей
d) Верификация цифровых подписей

Правильный ответ: a) Обеспечение конфиденциальности данных и соединений

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)

1. Что такое криптографический алгоритм и как он обеспечивает безопасность данных?

2. Объясните разницу между симметричным и асимметричным шифрованием.

3. Что такое ключ в криптографии и как он влияет на безопасность системы?

4. Опишите принцип работы блочного шифра и приведите пример алгоритма.

5. Какие основные криптографические протоколы используются для обеспечения конфиденциальности в сети?

6. Что такое хеш-функция и для чего она применяется в сетевой безопасности?

7. Объясните концепцию цифровых подписей и их роль в аутентификации.

8. В чем заключается принцип работы протокола Диффи-Хеллмана?

9. Какие атаки возможны на симметричные шифры и как их избегать?

10. Что такое угроза «Man-in-the-middle» и как ее можно предотвратить?

11. Назовите основные виды криптографических атака и их особенности.

12. Объясните роль сертификатов в инфраструктуре PKI.

13. Что такое протокол SSL/TLS и как он обеспечивает безопасность веб-соединений?

14. В чем заключается принцип работы системы аутентификации по паролю и её уязвимости?

15. Какие методы повышения криптоустойчивости в современных системах криптографии существуют?

16. Что такое криптоанализ и как он влияет на безопасность криптографических алгоритмов?

17. Объясните концепцию многофакторной аутентификации и её преимущества.

18. Назовите виды известных криптографических стандартов, используемых в корпоративных сетях.

19. Что такое протокол обмена ключами и почему он важен в сетевой безопасности?

20. Объясните роль целостности данных и способы её обеспечения в сетевом протоколе.

21. Какие существуют методы защиты от повторных атак (replay attacks)?

22. Что такое VPN и как он обеспечивает безопасную передачу данных?

23. Объясните принципы работы межсетевого экрана (firewall) и его виды.

24. Какие основные виды анонимизации в сетевой безопасности существуют?

25. Что такое атака с отказом в обслуживании (DoS) и как от нее защищаются?

26. В чем заключается суть технологии шифрования на уровне файловой системы?

27. Какие современные методы обнаружения и предотвращения атак используют системы IDS/IPS?

28. Что такое криптографические стандарты и кто их разрабатывает?

29. Объясните принципы цифровой криминалистики и её значимость для сетевой безопасности.

30. Какие перспективные направления развития сетевой криптографии и безопасности?

Критерии оценивания результатов обучения

Оценка	***Критерии оценивания по экзамену***

Высокий уровень «5» (отлично)	студент демонстрирует глубокие и прочные системные знания по изучаемой теме, исчерпывающе, последовательно, грамотно и логически стройно излагает ответ, не затрудняется с ответом при видоизменении вопроса, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.
Средний уровень «4» (хорошо)	студент демонстрирует общие знания по теме семинара, твердо знает материал по теме, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения;
Пороговый уровень «3» (удовлетворительно)	студент демонстрирует фрагментарные представления о содержании изучаемой темы, усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала
Минимальный уровень «2» (неудовлетворительно)	если студент не знает значительной части материала изучаемой темы, допускает существенные ошибки, с большими затруднениями отвечает по заданному вопросу темы;

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. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672 (дата обращения: 26.10.2025).

2. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт,

2025. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568708 (дата обращения: 26.10.2025).

3. Компьютерные сети : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 515 с. — (Высшее образование). — ISBN 978-5-534-21452-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/572239 (дата обращения: 26.10.2025).

4. Маликова, Т. Е. Математические методы и модели в управлении на морском транспорте : учебник для вузов / Т. Е. Маликова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 373 с. — (Высшее образование). — ISBN 978-5-534-04919-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563596 (дата обращения: 26.10.2025).

5. Ip-сети в инфокоммуникационных системах : учебник и практикум для вузов / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 96 с. — (Высшее образование). — ISBN 978-5-534-21454-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/572241 (дата обращения: 26.10.2025).

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

Изучение курса «Безопасность информационных экономических систем» осуществляется в тесном взаимодействии с другими дисциплинами по программированию. Форма и способы изучения материала определяются с учетом специфики изучаемой темы.

Однако во всех случаях необходимо обеспечить сочетание изучения теоретического материала, научного толкования того или иного понятия, даваемого в учебниках и лекциях, с самостоятельной работой студентов, выполнением практических заданий, подготовкой сообщений и докладов.

Лекционное занятие представляет собой систематическое, последовательное, монологическое изложение преподавателем-лектором учебного материала, как правило,

теоретического характера. Такое занятие представляет собой элемент технологии представления учебного материала путем логически стройного, систематически последовательного и ясного изложения с использованием образовательных технологий.

Цель лекции – организация целенаправленной познавательной деятельности обучающихся по овладению программным материалом учебной дисциплины. Чтение курса лекций позволяет дать связанное, последовательное изложение материала в соответствии с новейшими данными науки, сообщить слушателям основное содержание предмета в целостном, систематизированном виде.

Задачи лекции заключаются в обеспечении формирования системы знаний по учебной дисциплине, в умении аргументировано излагать научный материал, в формировании профессионального кругозора и общей культуры, в отражении еще не получивших освещения в учебной литературе новых достижений науки, в оптимизации других форм организации учебного процесса.

Для подготовки к лекциям необходимо изучить основную и дополнительную литературу по заявленной теме и обратить внимание на те вопросы, которые предлагаются к рассмотрению в конце каждой темы. При изучении основной и дополнительной литературы, студент может в достаточном объеме усвоить и успешно реализовать конкретные знания, умения, навыки и компетенции при выполнении следующих условий:

1) систематическая работа на учебных занятиях под руководством преподавателя и самостоятельная работа по закреплению полученных знаний и навыков;

2) добросовестное выполнение заданий преподавателя на практических занятиях; 3) выяснение и уточнение отдельных предпосылок, умозаключений и выводов, содержащихся в учебном курсе; взаимосвязей отдельных его разделов, используемых методов, характера их использования в практической деятельности менеджера;

4) сопоставление точек зрения различных авторов по затрагиваемым в учебном курсе проблемам; выявление неточностей и некорректного изложения материала в периодической и специальной литературе;

5) разработка предложений преподавателю в части доработки и совершенствования учебного курса;

6) подготовка научных статей для опубликования в периодической печати, выступление на научно-практических конференциях, участие в работе студенческих научных обществ, круглых столах и диспутах по антикоррупционным проблемам.

Лабораторные занятия – являются формой учебной аудиторной работы, в рамках которой формируются, закрепляются и представляются студентами знания, умения и навыки, интегрирующие результаты освоения компетенций как в лекционном формате, так в различных формах самостоятельной работы. К каждому занятию преподавателем формулируются практические задания, требования и методические рекомендации к их выполнению, которые представляются в фонде оценочных средств учебной дисциплины.

В ходе самоподготовки к практическим занятиям студент осуществляет сбор и обработку материалов по тематике его исследования, используя при этом открытые источники информации (публикации в научных изданиях, аналитические материалы, ресурсы сети Интернет и т.п.), а также практический опыт и доступные материалы объекта исследования.

Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на практических (семинарских) занятиях.

Самостоятельная работа студентов по дисциплине «Безопасность информационных экономических систем» проводится с целью закрепления и систематизации теоретических знаний, формирования практических навыков по их применению при решении экономических задач в выбранной предметной области. Самостоятельная работа включает: изучение основной и дополнительной литературы, проработка и повторение лекционного материала, материала учебной и научной литературы, подготовку к практическим занятиям, подготовка к разноуровневым задач и заданиям, а также к контролируемой самостоятельной работе

Самостоятельная работа студентов по данному учебному курсу предполагает поэтапную подготовку по каждому разделу в рамках соответствующих заданий:

Первый этап самостоятельной работы студентов включает в себя тщательное изучение теоретического материала на основе лекционных материалов преподавателя, рекомендуемых разделов основной и дополнительной литературы, материалов периодических научных изданий, необходимых для овладения понятийно- категориальным аппаратом и формирования представлений о комплексе теоретического и аналитического инструментария, используемого в рамках данной отрасли знания.

На втором этапе на основе сформированных знаний и представлений по данному разделу студенты выполняют расчетно-графические задания, нацеленные на формирование умений и навыков в рамках заявленных компетенций. На данном этапе студенты осуществляют самостоятельный поиск эмпирических материалов в рамках конкретного задания, обобщают и анализируют собранный материал по схеме, рекомендованной преподавателем, формулируют выводы, готовят практические рекомендации, материалы для публичного их представления и обсуждения.

Под *контролируемой самостоятельной работой (КСР)* понимают совокупность заданий, которые студент должен выполнить, проработать, изучить по заданию под руководством и контролем преподавателя. Т.е. КСР – это такой вид деятельности, наряду с лекциями, лабораторными и практическими занятиями, в ходе которых студент, руководствуясь специальными методическими указаниями преподавателя, а также методическими указаниями по выполнению типовых заданий, приобретает и совершенствует знания, умения и навыки, накапливает практический опыт.

Текущий контроль самостоятельной работы студентов осуществляется еженедельно в соответствие с программой занятий Описание заданий для самостоятельной работы студентов и требований по их выполнению выдаются преподавателем в соответствии с разработанным фондом оценочных средств по дисциплине «Безопасность информационных экономических систем».

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

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

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, ноутбук) и соответствующим программным обеспечением (ПО) Power Point. Ауд 129, А 305-4039л
2.	Лабораторные занятия	Аудитория оснащенная оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. Ауд. 101-102,105,106
3.	Промежуточная аттестация	Аудитория (кабинет Ауд 148-150).
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета. Ауд. 101.

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)	Microsoft Windows 8, 10, Microsoft Office Professional Plus