

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ

Проректор по учебной работе,
качеству образования – первый
проректор

Хагуров Т.А.

подпись

«02» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ФТД.В.01 «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ
ИНФОРМАЦИИ»

Направление

подготовки/специальность 10.04.01 Информационная безопасность

Направленность (профиль) / специализация Безопасность компьютерных систем

Форма обучения очная

Квалификация магистр

Краснодар
2026

Рабочая программа дисциплины «Методы и средства криптографической защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 «Информационная безопасность»

Программу составила:

О.В. Руденко, доцент кафедры вычислительных технологий, кандидат технических наук



Рабочая программа дисциплины «Методы и средства криптографической защиты информации» утверждена на заседании кафедры вычислительных технологий протокол № 11 «14» мая 2026 г.

И. о. заведующего кафедрой (разработчика) Приходько Т.А.

фамилия, инициалы



подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 3 «15» мая 2026 г.

Председатель УМК факультета Добровольская Н.Ю.

фамилия, инициалы



подпись

Рецензенты:

Схаляхо Ч.А., доцент КВВУ им. С.М. Штеменко, кандидат физико-математических наук, доцент

Гаркуша О.В. доцент кафедры информационных технологий ФБГОУ ВПО «Кубанский государственный университет», кандидат физико-математических наук, доцент

1. Цели и задачи освоения дисциплины (модуля)

1.1 Цель освоения дисциплины

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

1.2 Задачи дисциплины

Основные задачи освоения дисциплины:

- формирование целостного представления о современных организационных, технических, алгоритмических и других методах и средствах защиты компьютерной информации, используемых в современных криптосистемах, знакомство с законодательством и стандартами в этой области.

В результате освоения дисциплины студент должен:

Знать:

- правовые основы защиты компьютерной информации,
- математические основы криптографии
- организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях,
 - стандарты, модели и методы шифрования,
 - методы идентификации пользователей,
 - основы инфраструктуры систем, построенных с использованием публичных и секретных ключей.

Уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах,
 - проводить сравнительный анализ, выбирать методы и средства,
 - оценивать уровень защиты информационных ресурсов в прикладных системах;

Иметь навыки (приобрести опыт):

- передачи конфиденциальной информации по каналам связи,
- установления подлинности передаваемых сообщений и хранимой информации (документов, баз данных)
- выбирать методы и средства защиты информации.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Курс «Методы и средства криптографической защиты информации» относится к части, формируемой участниками образовательных отношений блока ФТД Факультативы.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по дисциплинам: «Алгебра», «Дискретная математика», «Теория графов и ее приложения», «Комбинаторный анализ», «Безопасность операционных систем», «Теория алгоритмов и вычислительных процессов», «Программирование в компьютерных сетях», «Криптографические протоколы», с которыми дисциплина связана логически и содержательно-методически.

Дисциплина предшествует изучению дисциплин: «Безопасные методы извлечения информации из сетевых источников», «Разработка и реализация проектов в сфере информационной безопасности».

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 универсальных/ общепрофессиональных/ профессиональных компетенций (УК/ОПК/ПК):

Код и наименование индикатора*	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1 Способен осуществлять экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	
ПК-1.1. Знает методы, применяемые при исследовании криптографических и технических систем и средств обеспечения информационной безопасности	Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах.
ПК-1.2. Умеет проводить экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	Умеет применять математические методы при исследовании криптографических алгоритмов
ПК-1.3. Владеет практическими навыками представления результатов экспериментальных исследований в области криптографических и технических систем и средств обеспечения информационной безопасности.	Владеет методиками оценки эффективности реализации систем защиты информации и навыками работы с программными средствами общего и специального назначения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)
			8
Контактная работа, в том числе:			
Аудиторные занятия (всего):		36	36
Занятия лекционного типа		18	18
Лабораторные занятия		18	18
Занятия семинарского типа (семинары, практические занятия)		—	—
		—	—
Иная контактная работа:			
Контроль самостоятельной работы (КСР)			
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе:		35,8	35,8
Курсовая работа		—	—
Проработка учебного (теоретического) материала		10	10
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		20	20
Реферат		—	—
Подготовка к текущему контролю		15,8	15,8
Контроль:		зачет	зачет
Подготовка к экзамену		-	-
Общая трудоёмкость	час.	72	72
	в том числе контактная работа	36,2	36,2
	зач. ед.	2	2

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре (очная форма).

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.	26	6	–	6	14
2	Криптографические методы защиты информации в компьютерных системах и сетях	26	6	–	6	14
3	Стохастические методы защиты информации	19,8	6	–	6	7,8
4	Подготовка к экзамену					
5	ИКР	0,2				
6	КСР					
7	Общая трудоемкость по дисциплине:	72	18	–	18	35,8

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

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела(темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1	Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.	Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов. Архитектура системы безопасности операционных систем.	ЛР
2	Криптографические методы защиты информации в компьютерных системах и сетях.	Управление ключами. Время жизни ключей. Виды ключевой информации. Распределение ключей. Сертификация ключей. Причины ненадежности криптосистем. Человеческий фактор. Особенности реализации. Типичные ошибки пользователей. Применение нестойких криптоалгоритмов (КА). Неправильное применение КА. Ошибки в реализации КА. Криптография как математическая наука vs криптография как инженерная дисциплина. Криптография как часть системы обеспечения безопасности информации (ОБИ). Философия проектирования систем ОБИ. Противоборствующее окружение. Параноидальная модель. Модель информационного противоборства. Информационная безопасность государства. Программные средства скрытого информационного воздействия(ПССИВ). Виды ПССИВ. Компьютерные вирусы (КВ).	ЛР

3	Стохастические методы защиты информации	Основы теории генераторов псевдослучайных чисел(ГПСЧ). Требования к качественным ГПСЧ. Классификация ГПСЧ, ориентированных на использование в задачах криптографической защиты информации. Структура ГПСЧ. Типы используемых нелинейных функций. Блочные и поточные ГПСЧ.ГПСЧ на основе односторонних функций. ГПСЧ на регистрах сдвига с линейными и нелинейными обратными связями. ГПСЧ И.А. Кулакова.	ЛР
---	---	--	----

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	Наименование лабораторных работ	Форма текущего контроля
1	Локальный администратор безопасности, центр аутентификации, диспетчер учетных записей, монитор безопасности.	ЛР
2	Механизм контроля доступа. Безопасность серверов SMB, RAS, IIS.	ЛР
3	Защищенные сетевые протоколы (SSL, TSL, IPsec и др.). Система аудита.	ЛР
4	ГПСЧ, функционирующие в конечных полях.	ЛР
5	Криптографические основы блокчейн технологий. Блокчейн-системы первого и второго поколений.	ЛР
6	Криптосистема RSA, режим шифрования со сцеплением блоков.	ЛР
7	Ранцевая криптосистема на основе вычислений в конечных полях.	ЛР
8	Стохастические методы в парольных системах разграничения доступа. Одноразовые пароли. Вероятностное шифрование.	ЛР
9	Криптопротоколы Zero Knowledge Proofs. Logic Encryption.	ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Индивидуальное задание	Источники основной и дополнительной литературы

Учебно-методические материалы для самостоятельной работы обучающихся и 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, применяемые при освоении дисциплины (модуля)

Программа дисциплины предусматривает использование в учебном процессе следующих образовательных технологий: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

- Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.
- Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.
- Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.
- Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:
- Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.
- Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.
- Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.
- Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.
- Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.
- Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.
- Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеперечисленных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

- работа в малых группах (команде) - совместная деятельность студентов в группе под

руководством лидера, направленная на решение общей задачи путём творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

- проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;
- анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;
- развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

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

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.

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

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Методы и средства криптографической защиты информации».

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (экзамен в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на экзамене (для выявления знания и понимания теоретического материала дисциплины).

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.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1.	Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.	ПК-1	ЛР	Вопросы 1-7
2.	Криптографические методы защиты информации в компьютерных системах и сетях	ПК-1	ЛР	Вопросы 8-35
3.	Стохастические методы защиты	ПК-1	ЛР	Вопрос 36-47

	информации			
--	------------	--	--	--

Показатели, критерии и шкала оценки сформированных компетенций

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: удовлетворительно /зачтено)				
на пороговом уровне:				
1	ПК-1.1. Знает методы, применяемые при исследовании криптографических и технических систем и средств обеспечения информационной безопасности	Проводит единичные исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 1-2
2	ПК-1.2. Умеет проводить экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	Умеет составлять научные отчёты и обзоры по результатам выполнения исследований.	опрос по теме, лабораторная работа	Вопросы на зачет 8-11
3	ПК-1.3. Владеет практическими навыками представления результатов экспериментальных исследований в области криптографических и технических систем и средств обеспечения информационной безопасности.	Владеет некоторыми методиками оценки эффективности реализации систем защиты информации и навыками работы с программными средствами общего и специального назначения.	опрос по теме, лабораторная работа	Вопросы на зачет 15,17
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: хорошо /зачтено)				
на базовом уровне:				
4	ПК-1.1. Знает методы, применяемые при исследовании криптографических и технических систем и средств обеспечения информационной безопасности	Проводит основные исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 3-5
5	ПК-1.2. Умеет проводить экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	Умеет составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 12-14

6	ПК-1.3. Владеет практическими навыками представления результатов экспериментальных исследований в области криптографических и технических систем и средств обеспечения информационной безопасности	Владеет методиками оценки эффективности реализации систем защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 19-30
Соответствие освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: отлично /зачтено)				
на продвинутом уровне:				
7	ПК-1.1. Знает методы, применяемые при исследовании криптографических и технических систем и средств обеспечения информационной безопасности	Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 16,18
8	ПК-1.2. Умеет проводить экспериментальные исследования в области криптографических и технических систем и средств обеспечения информационной безопасности	Умеет составлять научные отчеты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах.	опрос по теме, лабораторная работа	Вопросы на зачет 31-38
9	ПК-1.3. Владеет практическими навыками представления результатов экспериментальных исследований в области криптографических и технических систем и средств обеспечения информационной безопасности	Владеет методиками оценки эффективности реализации систем защиты информации и навыками работы с программными средствами общего и специального назначения.	опрос по теме, лабораторная работа	Вопросы на зачет 39-41

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

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1	1	Локальный администратор безопасности, центр аутентификации, диспетчер учетных записей, монитор безопасности. (ПК-1)
2		Механизм контроля доступа. Безопасность серверов SMB, RAS, IIS. (ПК-1)
3		Защищенные сетевые протоколы (SSL, TLS, IPsec и др.). Система аудита. (ПК-1)
4	2	ГПСЧ, функционирующие в конечных полях. (ПК-1)
5		Криптографические основы блокчейн технологий. Блокчейн-системы первого и второго поколений. (ПК-1)
6		Криптосистема RSA, режим шифрования со сцеплением блоков.

		(ПК-1)
7	3	Ранцевая криптосистема на основе вычислений в конечных полях. (ПК-1)
8		Стохастические методы в парольных системах разграничения доступа. Одноразовые пароли. Вероятностное шифрование. (ПК-1)
9		Криптопротоколы Zero Knowledge Proofs. Logic Encryption. (ПК-1)

Отчет должен содержать:

- постановку задачи;
- краткое описание проделанной работы;
- список использованной литературы.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

1. Протокол классической ЭП. (ПК-1)
2. Атака на схему ЭП, основанная на парадоксе дней рождения. (ПК-1)
3. Симметричный протокол аутентификации удаленных абонентов Нидхем-Шнеллера. (ПК-1)
4. Асимметричный протокол аутентификации удаленных абонентов Диффи-Хеллмана. (ПК-1)
5. Протоколы разделения секрета. (ПК-1)
6. Протоколы доказательства с нулевым разглашением знаний. (ПК-1)
7. Схема Kerberos. (ПК-1)
8. Причины трудоемкости решения задач защиты информации. (ПК-1)
9. Примеры уязвимости IT-технологий. (ПК-1)
10. Источники угроз кибербезопасности. (ПК-1)
11. Ошибки, сделанные в области кибербезопасности в ближайшем прошлом. Пути исправления ситуации. (ПК-1)
12. Процессный подход к решению задач защиты информации (ЗИ). (ПК-1)
13. Стохастические методы ЗИ. (ПК-1)
14. Особенности криптографии как науки. Задачи ЗИ, решаемые криптографическими методами. (ПК-1)
15. Основы криптологии. Криптография и криптоанализ. Основные термины. Правило Керхгофса. Требования к качественному шифру. (ПК-1)
16. Методы оценки стойкости шифров. Полиномиальные и экспоненциальные алгоритмы. (ПК-1)
17. Классификация шифров. (ПК-1)
18. Модель криптосистемы (КС) с секретным ключом. Основные проблемы. (ПК-1)
19. Совершенно секретный шифр. (ПК-1)
20. Схема гаммирования, ее свойства. (ПК-1)
21. Блочные и поточные шифры. (ПК-1)
22. S-блоки. SP-сеть. Сеть Фейстеля. Рассеивание и перемешивание информации. Основы дифференциального криптоанализа. (ПК-1)
23. Идея криптоалгоритма (КА) AES-128. Архитектура Квадрат. (ПК-1)
24. Идея КА Кузнечик. XSL-шифры. (ПК-1)
25. Режимы использования блочных шифров. (ПК-1)
26. Криптографические методы контроля целостности информации. (ПК-1)
27. Поточные шифры А5 и PIKE. (ПК-1)
28. Поточный шифр RC4. (ПК-1)
29. Хеш-функции, требования к качественной хеш-функции. (ПК-1)
30. Модель КС с открытым ключом. (ПК-1)
31. Односторонняя функция. Односторонняя функция с секретом. (ПК-1)
32. Криптосистема RSA. Пример. (ПК-1)

33. Ранцевая КС. Пример. (ПК-1)
34. Протокол выработки общего секретного ключа Диффи-Хеллмана. Пример. (ПК-1)
35. Идея электронной подписи (ЭП). Пример. (ПК-1)
36. Биткоин. Блокчейн. Публичный блокчейн. Как построить блокчейн у себя на ноутбуке или смартфоне. (ПК-1)
37. Алгоритм работы системы Биткоин. Формат транзакций. (ПК-1)
38. Механизмы консенсуса блокчейн-систем. (ПК-1)
39. Причины ненадежности криптосистем. (ПК-1)
40. Управление ключами. Человеческий фактор. Особенности конкретной реализации КА. (ПК-1)
41. Парольные системы разграничения доступа. (ПК-1)

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

4.2.1 Методические рекомендации к сдаче экзамена

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на экзамене (для выявления знания и понимания теоретического материала дисциплины).

4.2.2 Критерии оценивания результатов обучения

Методические рекомендации, определяющие процедуры оценивания лабораторных работ.

Задание считается выполненным, если предоставлен исходный текст программы, который содержит не более 3 синтаксических ошибок, логика работы программы эффективна, программа работает на любых входных данных.

Методические рекомендации, определяющие процедуры оценивания на экзамене

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

5. Перечень основной и дополнительной учебной литературы, необходимой

для освоения дисциплины (модуля)

5.1 Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии .NET : руководство / П. Торстейнсон, Г. А. Ганеш ; перевод с англ. В. Д. Хорева под редакцией С. М. Молявко. - 5-е изд. (эл.). - Москва : Лаборатория знаний, 2024. - 482 с. - URL: <https://e.lanbook.com/book/418025> (дата обращения: 17.01.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-93208-734-3. - Текст : электронный.

2. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Юрайт, 2022. - 473 с. - URL: <https://urait.ru/bcode/489242> (дата обращения: 26.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474-3. - Текст : электронный.

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL: <https://urait.ru/bcode/489919> (дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный.

5.2 Дополнительная литература:

1. Нечаев, Василий Ильич. Элементы криптографии : основы теории защиты информации : учебное пособие / В. И. Нечаев ; под ред. В. А. Садовниченко. - М. : Высшая школа, 1999. - 109 с. : ил. - (Высшая математика). - Библиогр.: с. 104-106. - ISBN 5060036448 : 38 р. - Текст : непосредственный. (40 экз. в библиотеке КубГУ).
2. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Лань, 2022. - 400 с. - URL: <https://e.lanbook.com/book/210746> (дата обращения: 18.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-1116-0. - Текст : электронный.
3. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стереотипное. - Москва : Горячая линия-Телеком, 2017. - 230 с. - <https://e.lanbook.com/book/111097>. - Текст : электронный.

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

Профессиональные базы данных:

1. Scopus <http://www.scopus.com/>
2. ScienceDirect <https://www.sciencedirect.com/>
3. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
4. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
5. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
6. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ)) <https://rusneb.ru/>
7. Президентская библиотека им. Б.Н. Ельцина <https://www.prilib.ru/>
8. База данных CSD Кембриджского центра кристаллографических данных (CCDC) <https://www.ccdc.cam.ac.uk/structures/>
9. Springer Journals: <https://link.springer.com/>
10. Springer Journals Archive: <https://link.springer.com/>
11. Nature Journals: <https://www.nature.com/>
12. Springer Nature Protocols and Methods:

<https://experiments.springernature.com/sources/springer-protocols>

13. Springer Materials: <http://materials.springer.com/>
14. Nano Database: <https://nano.nature.com/>
15. Springer eBooks (i.e. 2020 eBook collections): <https://link.springer.com/>
16. "Лекториум ТВ" <http://www.lektorium.tv/>
17. 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. КиберЛенинка <http://cyberleninka.ru/>;
2. Американская патентная база данных <http://www.uspto.gov/patft/>
3. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
4. Федеральный портал "Российское образование" <http://www.edu.ru/>;
5. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru/>;
6. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/> .
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" <https://pushkininstitute.ru/>;
8. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
9. Служба тематических толковых словарей <http://www.glossary.ru/>;
10. Словари и энциклопедии <http://dic.academic.ru/>;
11. Образовательный портал "Учеба" <http://www.ucheba.com/>;
12. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--plai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Электронный каталог Научной библиотеки КубГУ <http://megapro.kubsu.ru/MegaPro/Web>
2. Электронная библиотека трудов ученых КубГУ <http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6>
3. Среда модульного динамического обучения <http://moodle.kubsu.ru>
4. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://infoneeds.kubsu.ru/>
5. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
6. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
7. 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)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите ЛР студент должен ответить на несколько вопросов из лекционной части курса.

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 (модулю)

7.1 Перечень информационных технологий

- Проверка домашних заданий и консультирование посредством электронной почты.
- Использование электронных презентаций при проведении лекций и практических занятий.

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения

1. Visual Studio Code, версия 1.52+.
2. Visual Studio 19 и выше.
3. Программы для демонстрации и создания презентаций.

8. Материально-техническое обеспечение по дисциплине (модулю)

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
3.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
4.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
5.	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.

Примечание: конкретизация аудиторий и их оснащение определяется ОПОП.