

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА»**

**Физико-математический факультет
Кафедра информатики и вычислительной математики**

УТВЕРЖДАЮ
И. о. проректора по УР
М. Х. Чанкаев
«29» апреля 2026 г., протокол № 7

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Методы и средства защиты информации

(наименование дисциплины (модуля))

Направление подготовки

44.03.05 – Педагогическое образование (с двумя профилями подготовки)

(шифр, название направления)

Направленность (профиль) подготовки

Математика и информатика

Квалификация выпускника

бакалавр

Форма обучения

Очная/заочная

Карачаевск, 2026

КОМПЕТЕНЦИИ ПО ДИСЦИПЛИНЕ «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

Код компетенций	Содержание компетенции в соответствии с ФГОС ВО/ОПВО	Индикаторы достижения сформированности компетенций
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Определяет совокупность взаимосвязанных задач и ресурсное обеспечение, условия достижения поставленной цели, исходя из действующих правовых норм. УК-2.2. Оценивает вероятные риски и ограничения, определяет ожидаемые результаты решения поставленных задач. УК-2.3. Использует инструменты и техники цифрового моделирования для реализации образовательных процессов
ОПК-9	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности ОПК-9.2. Демонстрирует способность использовать цифровые ресурсы для решения задач профессиональной деятельности
ПК-1	Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета) ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные

ТЕСТОВЫЙ МАТЕРИАЛ ДЛЯ ДИАГНОСТИКИ ИНДИКАТОРОВ ОЦЕНИВАНИЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ задания	Правильный ответ	Содержание вопроса	Компетенция
I. ЗАДАНИЯ ОТКРЫТОГО ТИПА НА ДОПОЛНЕНИЕ.			
1		Прочитайте текст и запишите правильный ответ. Шифрование — это процесс преобразования информации с использованием _____ для предотвращения несанкционированного доступа.	УК-2
2		Прочитайте текст и запишите правильный ответ. Процесс аутентификации пользователя с использованием пароля или биометрии называется _____.	ОПК-9
3		Прочитайте текст и запишите правильный ответ. _____ — это метод защиты информации, при котором используются различные технологии для блокирования или ограничения доступа к данным.	ПК-1
4		Прочитайте текст и запишите правильный ответ. Защита от несанкционированного изменения данных, их искажения или уничтожения называется _____.	УК-2
II. ЗАДАНИЯ ОТКРЫТОГО ТИПА СВОБОДНОГО ИЗЛОЖЕНИЯ С РАЗВЕРНУТЫМ ОТВЕТОМ.			
5		Прочитайте текст и запишите развернутый ответ. Что такое криптография и какие виды криптографических методов существуют?	УК-2
6		Прочитайте текст и запишите развернутый ответ. Опишите основные способы защиты данных в компьютерных сетях.	ОПК-9
7		Прочитайте текст и запишите развернутый ответ. Что такое резервное копирование (backup) и какие существуют его виды?	ПК-1
8		Прочитайте текст и запишите развернутый ответ. Что такое система управления доступом (СУД)? Приведите примеры механизмов управления доступом.	УК-2

**III. ЗАДАНИЯ ЗАКРЫТОГО ТИПА НА УСТАНОВЛЕНИЕ
ПОСЛЕДОВАТЕЛЬНОСТИ.**

9		Прочитайте текст и установите последовательность шагов процесса шифрования данных: 1. Шифрование исходных данных 2. Генерация ключа 3. Хранение зашифрованных данных 4. Выбор алгоритма шифрования Запишите соответствующую последовательность правильности следования условий в виде цифр слева направо	УК-2
10		Прочитайте текст и установите последовательность этапов оценки рисков в информационной безопасности: 1. Оценка угроз 2. Анализ уязвимостей 3. Определение активов 4. Разработка мер защиты Запишите соответствующую последовательность правильности следования условий в виде цифр слева направо	ОПК-9
11		Прочитайте текст и установите последовательность шагов процесса аутентификации пользователя: 1. Проверка учетных данных 2. Уведомление о неудачной попытке 3. Ввод учетных данных 4. Предоставление доступа Запишите соответствующую последовательность правильности следования условий в виде цифр слева направо	ПК-1
12		Прочитайте текст и установите последовательность шагов в процессе реагирования на инциденты информационной безопасности: 1. Реакция на инцидент 2. Анализ и отчетность 3. Идентификация инцидента 4. Оценка инцидента Запишите соответствующую последовательность правильности	УК-2

		следования условий в виде цифр слева направо	
13		Прочитайте текст и установите последовательность этапов разработки политики безопасности информации: 1. Утверждение и внедрение 2. Анализ текущей ситуации 3. Определение целей и задач 4. Разработка документа Запишите соответствующую последовательность правильности следования условий в виде цифр слева направо	ОПК-9
14		Прочитайте текст и установите последовательность этапов внедрения системы защиты информации: 1. Установка и настройка 2. Оценка потребностей 3. Выбор средств защиты 4. Обучение пользователей Запишите соответствующую последовательность правильности следования условий в виде цифр слева направо	ПК-1

IV. ЗАДАНИЯ ЗАКРЫТОГО ТИПА НА УСТАНОВЛЕНИЕ СООТВЕТСТВИЯ.

15	А	
	Б	
	В	
	Г	
	Д	

Прочитайте текст и установите соответствие				УК-2
Установите соответствие между методами защиты информации и их целями				
А	Обеспечивает доступность данных	1	Шифрование	
Б	Предотвращает несанкционированный доступ	2	Аутентификация	
В	Подтверждает личность пользователя	3	Резервное копирование	
Г	Обеспечивает конфиденциальность данных	4	Биометрия	
Д	Обеспечивает защиту от потери данных	5	Мониторинг безопасности	
Запишите выбранные цифры справа от соответствующих букв				

16	<table><tr><td>А</td><td></td></tr><tr><td>Б</td><td></td></tr><tr><td>В</td><td></td></tr><tr><td>Г</td><td></td></tr><tr><td>Д</td><td></td></tr></table>	А		Б		В		Г		Д		Прочитайте текст и установите соответствие Установите соответствие между типами атак и их характеристиками <table><tr><td>А</td><td>Перехват данных в процессе передачи</td><td>1</td><td>Фишинг</td></tr><tr><td>Б</td><td>Обман с целью получения конфиденциальных данных</td><td>2</td><td>DoS-атака</td></tr><tr><td>В</td><td>Атака, направленная на вывод системы из строя</td><td>3</td><td>SQL-инъекция</td></tr><tr><td>Г</td><td>Вредоносные программы, изменяющие работу системы</td><td>4</td><td>Man-in-the-middle</td></tr><tr><td>Д</td><td>Атака на уязвимость в SQL-базах данных</td><td>5</td><td>Вредоносное ПО</td></tr></table> Запишите выбранные цифры справа от соответствующих букв	А	Перехват данных в процессе передачи	1	Фишинг	Б	Обман с целью получения конфиденциальных данных	2	DoS-атака	В	Атака, направленная на вывод системы из строя	3	SQL-инъекция	Г	Вредоносные программы, изменяющие работу системы	4	Man-in-the-middle	Д	Атака на уязвимость в SQL-базах данных	5	Вредоносное ПО	ОПК-9
А																																	
Б																																	
В																																	
Г																																	
Д																																	
А	Перехват данных в процессе передачи	1	Фишинг																														
Б	Обман с целью получения конфиденциальных данных	2	DoS-атака																														
В	Атака, направленная на вывод системы из строя	3	SQL-инъекция																														
Г	Вредоносные программы, изменяющие работу системы	4	Man-in-the-middle																														
Д	Атака на уязвимость в SQL-базах данных	5	Вредоносное ПО																														
17	<table><tr><td>А</td><td></td></tr><tr><td>Б</td><td></td></tr><tr><td>В</td><td></td></tr><tr><td>Г</td><td></td></tr><tr><td>Д</td><td></td></tr></table>	А		Б		В		Г		Д		Прочитайте текст и установите соответствие Установите соответствие между методами защиты и их категориями. <table><tr><td>А</td><td>Защита от вирусов</td><td>1</td><td>Биометрия</td></tr><tr><td>Б</td><td>Защита сетевого трафика</td><td>2</td><td>Антивирус</td></tr><tr><td>В</td><td>Средство защиты от утечек информации</td><td>3</td><td>Фаервол</td></tr><tr><td>Г</td><td>Средства контроля за доступом</td><td>4</td><td>Криптография</td></tr><tr><td>Д</td><td>Методы защиты передаваемых данных</td><td>5</td><td>Аудит безопасности</td></tr></table> Запишите выбранные цифры справа от соответствующих букв	А	Защита от вирусов	1	Биометрия	Б	Защита сетевого трафика	2	Антивирус	В	Средство защиты от утечек информации	3	Фаервол	Г	Средства контроля за доступом	4	Криптография	Д	Методы защиты передаваемых данных	5	Аудит безопасности	ПК-1
А																																	
Б																																	
В																																	
Г																																	
Д																																	
А	Защита от вирусов	1	Биометрия																														
Б	Защита сетевого трафика	2	Антивирус																														
В	Средство защиты от утечек информации	3	Фаервол																														
Г	Средства контроля за доступом	4	Криптография																														
Д	Методы защиты передаваемых данных	5	Аудит безопасности																														
18	<table><tr><td>А</td><td></td></tr><tr><td>Б</td><td></td></tr><tr><td>В</td><td></td></tr><tr><td>Г</td><td></td></tr><tr><td>Д</td><td></td></tr></table>	А		Б		В		Г		Д		Прочитайте текст и установите соответствие Установите соответствие между типами криптографических алгоритмов с их назначениями. <table><tr><td>А</td><td>Алгоритм хеширования</td><td>1</td><td>RSA</td></tr><tr><td>Б</td><td>Симметричный алгоритм шифрования</td><td>2</td><td>AES</td></tr><tr><td>В</td><td>Алгоритм электронной подписи</td><td>3</td><td>MD5</td></tr><tr><td>Г</td><td>Алгоритм для вычисления контрольной суммы</td><td>4</td><td>HMAC</td></tr><tr><td>Д</td><td>Криптографическая функция для проверки целостности данных</td><td>5</td><td>SHA-256</td></tr></table> Запишите выбранные цифры справа от соответствующих букв	А	Алгоритм хеширования	1	RSA	Б	Симметричный алгоритм шифрования	2	AES	В	Алгоритм электронной подписи	3	MD5	Г	Алгоритм для вычисления контрольной суммы	4	HMAC	Д	Криптографическая функция для проверки целостности данных	5	SHA-256	УК-2
А																																	
Б																																	
В																																	
Г																																	
Д																																	
А	Алгоритм хеширования	1	RSA																														
Б	Симметричный алгоритм шифрования	2	AES																														
В	Алгоритм электронной подписи	3	MD5																														
Г	Алгоритм для вычисления контрольной суммы	4	HMAC																														
Д	Криптографическая функция для проверки целостности данных	5	SHA-256																														

19	<table><tr><td>А</td><td></td></tr><tr><td>Б</td><td></td></tr><tr><td>В</td><td></td></tr><tr><td>Г</td><td></td></tr><tr><td>Д</td><td></td></tr></table>	А		Б		В		Г		Д		Прочитайте текст и установите соответствие Установите соответствие между уровнями защиты и их характеристиками <table><tr><td>А</td><td>Защита данных на уровне оборудования</td><td>1</td><td>Программный уровень</td></tr><tr><td>Б</td><td>Разработка политики безопасности</td><td>2</td><td>Сетевой уровень</td></tr><tr><td>В</td><td>Защита на уровне операционных систем и приложений</td><td>3</td><td>Аппаратный уровень</td></tr><tr><td>Г</td><td>Использование систем контроля доступа и брандмауэров</td><td>4</td><td>Организационный уровень</td></tr><tr><td>Д</td><td>Применение антивирусных и шифровальных программ</td><td>5</td><td>Пользовательский уровень</td></tr></table> Запишите выбранные цифры справа от соответствующих букв	А	Защита данных на уровне оборудования	1	Программный уровень	Б	Разработка политики безопасности	2	Сетевой уровень	В	Защита на уровне операционных систем и приложений	3	Аппаратный уровень	Г	Использование систем контроля доступа и брандмауэров	4	Организационный уровень	Д	Применение антивирусных и шифровальных программ	5	Пользовательский уровень	ОПК-9
А																																	
Б																																	
В																																	
Г																																	
Д																																	
А	Защита данных на уровне оборудования	1	Программный уровень																														
Б	Разработка политики безопасности	2	Сетевой уровень																														
В	Защита на уровне операционных систем и приложений	3	Аппаратный уровень																														
Г	Использование систем контроля доступа и брандмауэров	4	Организационный уровень																														
Д	Применение антивирусных и шифровальных программ	5	Пользовательский уровень																														
20	<table><tr><td>А</td><td></td></tr><tr><td>Б</td><td></td></tr><tr><td>В</td><td></td></tr><tr><td>Г</td><td></td></tr></table>	А		Б		В		Г		Прочитайте текст и установите соответствие Установите соответствие между каждой позицией данной в левом столбце, соответствующей позиции из правого столбца. <table><tr><td>А</td><td>Процесс проверки идентичности пользователя или системы для предоставления доступа к ресурсам.</td><td>1</td><td>Шифрование</td></tr><tr><td>Б</td><td>Создание копий данных для их восстановления в случае потери или повреждения.</td><td>2</td><td>Аутентификация</td></tr><tr><td>В</td><td>Метод преобразования данных в недоступный для чтения формат для защиты информации.</td><td>3</td><td>Контроль доступа</td></tr><tr><td>Г</td><td>Механизм, который определяет, какие пользователи могут получать доступ к определенным ресурсам.</td><td>4</td><td>Резервное копирование</td></tr></table> Запишите выбранные цифры справа от соответствующих букв	А	Процесс проверки идентичности пользователя или системы для предоставления доступа к ресурсам.	1	Шифрование	Б	Создание копий данных для их восстановления в случае потери или повреждения.	2	Аутентификация	В	Метод преобразования данных в недоступный для чтения формат для защиты информации.	3	Контроль доступа	Г	Механизм, который определяет, какие пользователи могут получать доступ к определенным ресурсам.	4	Резервное копирование	ПК-1						
А																																	
Б																																	
В																																	
Г																																	
А	Процесс проверки идентичности пользователя или системы для предоставления доступа к ресурсам.	1	Шифрование																														
Б	Создание копий данных для их восстановления в случае потери или повреждения.	2	Аутентификация																														
В	Метод преобразования данных в недоступный для чтения формат для защиты информации.	3	Контроль доступа																														
Г	Механизм, который определяет, какие пользователи могут получать доступ к определенным ресурсам.	4	Резервное копирование																														

V.1. ЗАДАНИЯ КОМБИНИРОВАННОГО ТИПА С ВЫБОРОМ
ОДНОГО ПРАВИЛЬНОГО ОТВЕТА.

21		Прочитайте текст и выберите правильный ответ Какой алгоритм шифрования является симметричным? a) RSA b) AES c) DSA d) ECC	УК-2
22		Прочитайте текст и выберите правильный ответ Какой из перечисленных методов аутентификации является двухфакторным? a) Пароль + отпечаток пальца b) Пароль c) ПИН-код d) Картридер	ОПК-9
23		Прочитайте текст и выберите правильный ответ Какой из перечисленных методов защиты информации является основной для обеспечения конфиденциальности? a) Шифрование b) Антивирус c) Брандмауэр d) Биометрия	ПК-1
24		Прочитайте текст и выберите правильный ответ Какая из следующих технологий используется для защиты данных при передаче по сети? a) SSL/TLS b) MD5 c) RSA d) Diffie-Hellman	УК-2
25		Прочитайте текст и выберите правильный ответ Какой из алгоритмов шифрования считается наиболее безопасным среди симметричных? a) DES b) AES c) 3DES d) RC4	ОПК-9

26		Прочитайте текст и выберите правильный ответ Какой из следующих методов защиты информации используется для предотвращения несанкционированного доступа к данным? А. Антивирусное программное обеспечение В. Фаервол С. Шифрование данных D. Все вышеперечисленное	ПК-1
V.2. ЗАДАНИЯ КОМБИНИРОВАННОГО ТИПА С ВЫБОРОМ НЕСКОЛЬКИХ ПРАВИЛЬНЫХ ОТВЕТОВ.			
27		Прочитайте текст и выберите правильные ответы Какие из перечисленных методов могут быть использованы для аутентификации пользователя? а) Пароль b) Логин c) Отпечаток пальца d) Секретный вопрос	УК-2
28		Прочитайте текст и выберите правильные ответы Какие из следующих методов защиты информации относятся к криптографической защите? а) Шифрование b) Хеширование c) Электронная подпись d) Антивирус	ОПК-9
29		Прочитайте текст и выберите правильные ответы Какие из перечисленных видов атак являются активными? а) Man-in-the-middle b) Фишинг c) SQL-инъекция d) Оффлайн-атака на хеши	ПК-1
30		Прочитайте текст и выберите правильные ответы Какие из следующих средств могут использоваться для обеспечения безопасности передаваемой информации? а) VPN b) SSL/TLS c) Шифрование d) IDS	УК-2

31		Прочитайте текст и выберите правильные ответы Какие из перечисленных характеристик являются критериями безопасности информации? а) Конфиденциальность б) Доступность в) Интегритет г) Скорость передачи	ОПК-9
32		Прочитайте текст и выберите правильные ответы Какие из следующих методов защиты информации могут быть использованы для обеспечения конфиденциальности данных? а) Шифрование данных б) Аутентификация пользователей в) Фаервол г) Контроль доступа д) Антивирусное программное обеспечение	ПК-1

КЛЮЧИ К ОЦЕНИВАНИЮ.

№ задания	ПРАВИЛЬНЫЙ ОТВЕТ
1	криптографического ключа
2	аутентификацией
3	фаервол (межсетевой экран)
4	целостностью данных
5	Криптография — это наука и искусство защиты информации с помощью математических методов, направленных на обеспечение конфиденциальности, целостности и аутентичности данных. Существует несколько основных видов криптографии: симметричная криптография, асимметричная криптография и хеширование.
6	В компьютерных сетях для защиты данных применяются несколько методов: шифрование данных, аутентификация и авторизация пользователей, межсетевые экраны (фаерволы), системы обнаружения вторжений (IDS/IPS) и VPN (Virtual Private Network) — защищенные каналы связи.
7	Резервное копирование — это процесс создания копий данных, которые могут быть восстановлены в случае их утраты, повреждения или других непредвиденных обстоятельств. Существуют несколько видов резервного копирования: полное, инкрементальное и дифференциальное.
8	Система управления доступом (СУД) — это совокупность средств и методов, обеспечивающих правильный доступ пользователей и систем к ресурсам. Примеры механизмов управления доступом: механизм контроля доступа на основе ролей (RBAC), контроль доступа на основе списков управления доступом (ACL), многофакторная аутентификация (MFA).
9	4 – 2 – 1 – 3
10	3 – 2 – 1 – 4
11	3 – 1 – 4 – 2
12	3 – 4 – 1 – 2
13	3 – 2 – 4 – 1

14	2 – 3 – 1 – 4
15	1 — D, 2 — C, 3 — E, 4 — B, 5 — A
16	1 — B, 2 — C, 3 — E, 4 — A, 5 — D
17	1 — D, 2 — A, 3 — B, 4 — E, 5 — C
18	1 — C, 2 — B, 3 — D, 4 — E, 5 — A
19	1 — C, 2 — D, 3 — A, 4 — B, 5 — E
20	1 – C, 2 – A, 3 – D, 4 - B
21	b) AES
22	a) Пароль + отпечаток пальца
23	a) Шифрование
24	a) SSL/TLS
25	b) AES
26	d) все вышеперечисленное
27	a) Пароль, c) Отпечаток пальца, d) Секретный вопрос
28	a) Шифрование, b) Хеширование, c) Электронная подпись
29	a) Man-in-the-middle, b) Фишинг, c) SQL-инъекция
30	a) VPN, b) SSL/TLS, c) Шифрование
31	a) Конфиденциальность, b) Доступность, c) Интегритет
32	a) Шифрование данных, d) Контроль доступа