



**ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
КИЗИЛОРТОВСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ**

Российская Федерация
Республика Дагестан,
368118, г. Кизилорт,
ул. Вишневого, 170.

Тел.: +7(989) 476-00-15
E-mail: omar.g4san@yandex.ru

ОДОБРЕНО
на педагогическом совете № 4
от «16» февраля 2026г.

УТВЕРЖДЕНО
директор ПОАНО «КМК» г. Кизилорт
О.М.Гасанов
Приказ № 32-О
от «16» февраля 2026г.



**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств)**

**для проведения текущего контроля успеваемости, промежуточной
аттестации обучающихся по учебной дисциплине**

ОП.05 Основы информационной безопасности

по специальности 09.02. 11 «Разработка и управление программным
обеспечением»

по программе базовой подготовки

на базе основного общего образования;

форма обучения – очная, очно – заочная, заочная

Квалификация выпускника – программист

Кизилорт 2026



**ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
КИЗИЛЮРТОВСКИЙ МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ**

Российская Федерация
Республика Дагестан,
368118, г. Кизилюрт,
ул. Вишневого, 170.

Тел.: +7(989) 476-00-15
E- mail: omar.g4san@yandex.ru

ОДОБРЕНО
на педагогическом совете № 4
от «16» февраля 2026г.

УТВЕРЖДЕНО
директор ПОАНО «КМК» г. Кизилюрт
О.М.Гасанов _____
Приказ № _____
от «16» февраля 2026г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств)
для проведения текущего контроля успеваемости, промежуточной
аттестации обучающихся по учебной дисциплине

ОП.05 Основы информационной безопасности
по специальности 09.02. 11 «Разработка и управление программным
обеспечением»
по программе базовой подготовки
на базе основного общего образования;
форма обучения – очная, очно – заочная, заочная
Квалификация выпускника – программист

Кизилюрт 2026

Содержание

1. Пояснительная записка.....
2. Перечень компетенций с указанием этапов их формирования в процессе освоения основной образовательной программы.....
3. Описание перечня оценочных средств и критериев оценивания компетенций на различных этапах их формирования.....
4. Оценочные средства характеризующих этапы формирования компетенций при изучении учебной дисциплины.....
5. Критерии и шкала оценивания компетенций на различных этапах их формирования.....
6. Описание процедуры оценивания знаний и умений, характеризующих этапы формирования компетенций.....

1. Пояснительная записка

Оценочные материалы разработаны в форме фонда оценочных средств в соответствии с пунктом 9 статьи 2 Федерального закона от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации» и раздела II Методика расчета и применения аккредитационных показателей по образовательным программам среднего профессионального образования Приказа Министерства просвещения России от 14.04.2023 №272 «Об утверждении аккредитационных показателей, методики расчета и применении аккредитационных показателей по образовательным программам среднего профессионального образования» и пункта 7 Приказа Министерства Просвещения Российской Федерации от 24.08.2022 №762 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».

Фонд оценочных средств (далее – ФОС) предназначены для оценки уровня освоения компетенций на различных этапах их формирования при изучении учебной дисциплины ОП.05 Основы информационной безопасности.

Общие компетенции:

Код компетенции	Формулировка компетенции	Знания, умения
ОК.01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	<p>Умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)</p> <p>Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности</p>
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач про-	<p>Умения: определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска</p>

	фессиональной деятельности	Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	Умения: определять актуальность нормативно-правовой документации в профессиональной деятельности Знания: возможные траектории профессионального развития и самообразования
ОК.09	Пользоваться профессиональной документацией на государственном и иностранном языках	Умения: понимать тексты на базовые профессиональные темы Знания: лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности

Профессиональные компетенции:

Основные виды деятельности	Код и формулировка компетенции	Показатели освоения компетенции
Разработка, администрирование и защита баз	ПК 1.1 Проектировать базы данных.	Умения: проектировать базы данных
		Знания: принципы безопасности хранения данных
	ПК 1.4 Администрировать базы данных	Умения: администрировать базы данных
		Знания: методы защиты баз данных от внешних угроз
	ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации.	Умения: шифровать данные и обеспечивать их конфиденциальность
		Знания: принципы криптографии и методов шифрования данных стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.

		методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2. Перечень компетенций с указанием этапов их формирования в процессе освоения основной образовательной программы

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
1	Тема 1. Введение в информационную безопасность	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
2	Тема 2. Управление безопасностью информации	ОК 02, ОК 03 ПК 1.2, ПК 2.2, ПК 3.2	тест, реферат, устный опрос, практические задачи
3	Тема 3. Криптография	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
4	Тема 4. Защита сетевой инфраструктуры	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
5	Тема 5. Безопасность приложений	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
6	Тема 6. Защита данных	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
7	Тема 7. Безопасность облачных технологий	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
8	Тема 8. Инциденты безопасности	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи

9	Тема 9. Социальная инженерия и человеческий фактор	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи
10	Тема 10. Будущее информационной безопасности	ОК 01, ОК 02, ОК 03 ОК 09 ПК 1.1, ПК 1.4, ПК 1.5	тест, реферат, устный опрос, практические задачи

3. Описание перечня оценочных средств и критериев оценивания компетенций на различных этапах их формирования

№ п/п	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в фонде
1	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов
2	Доклад, сообщение	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы	Темы докладов, сообщений
3	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
4	Тестирование	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
5	4 Разноуровневые задачи и задания	Различают задачи: а) ознакомительного, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) репродуктивного уровня, позволяющие оценивать и диагностировать	Комплект разноуровневых задач и заданий

		<p>умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;</p> <p>в) продуктивного уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения, выполнять проблемные задания.</p>	
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4. Оценочные средства, характеризующие этапы освоения компетенций при изучении учебной дисциплины

Вопросы для устного опроса

1. Что понимается под информационной безопасностью и какие три основных компонента (триада CIA) лежат в ее основе
2. Чем отличаются понятия «угроза», «уязвимость» и «риск» в контексте информационной безопасности
3. Какие виды угроз информационной безопасности существуют и приведите примеры каждой из них
4. Что такое политика информационной безопасности и для чего она необходима в организации
5. Какие этапы включает в себя процесс управления рисками информационной безопасности
6. В чем разница между симметричным и асимметричным шифрованием и приведите примеры алгоритмов для каждого типа
7. Что такое хэш-функция и для каких целей она используется в информационной безопасности
8. Как работает цифровая подпись и какие задачи она решает
9. Что такое инфраструктура открытых ключей и какие компоненты она включает
10. Какие основные меры защиты сетевой инфраструктуры вы знаете
11. Что такое межсетевой экран и как он классифицирует сетевой трафик
12. Для чего используются системы обнаружения и предотвращения вторжений
13. Какие протоколы обеспечивают безопасную передачу данных по сети и в чем их особенности
14. Что такое VPN и как он обеспечивает защиту данных при передаче
15. Какие основные уязвимости веб-приложений входят в список OWASP Top 10
16. Что такое SQL-инъекция и как защититься от данного типа атак
17. Какие методы защиты от межсайтового скриптинга существуют
18. Что такое безопасная разработка программного обеспечения и какие принципы она включает
19. Какие методы защиты данных в состоянии покоя и в состоянии передачи вы знаете
20. Что такое шифрование диска и как оно защищает данные при физическом доступе к устройству
21. Какие методы резервного копирования данных существуют и как они связаны с информационной безопасностью
22. Какие специфические угрозы безопасности существуют для облачных технологий
23. Что такое модель разделения ответственности в облачных сервисах и как она распределяет обязанности между провайдером и клиентом
24. Какие меры безопасности необходимо учитывать при выборе облачного провайдера

25. Что такое инцидент информационной безопасности и какие этапы включает процесс реагирования на инциденты
26. Какие виды социальной инженерии вы знаете и приведите примеры каждой
27. Какие методы защиты от социальной инженерии должен применять ИТ-специалист
28. Как человеческий фактор влияет на уровень информационной безопасности организации
29. Какие современные тренды и технологии формируют будущее информационной безопасности
30. Что такое концепция Zero Trust и в чем заключается ее основной принцип

Указания по выполнению тестовых заданий

Типы заданий	Последовательность действий при выполнении заданий
Тестовые задания на установление соответствия	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответов ожидаются пары элементов. 2. Внимательно прочитать оба списка: Список 1 - вопросы, утверждения, факты, понятия и т.д. Список 2 - утверждение, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы/цифры (в зависимости от задания) вариантов ответов (например, А1 или Б4)
Тестовые задания на установление последовательности	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответов ожидаются последовательность элементов. 2. Внимательно прочитать предложенные варианты ответов. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности без пробелов и знаков препинания (например, БАА или 135)
Тестовые задания с выбором двух (и более) правильных ответов из перечня	<ol style="list-style-type: none"> 1. Внимательно прочитать текст задания и понять, что в качестве ответов ожидаются два и более вариантов ответов, наиболее верных. 2. Внимательно прочитать предложенные варианты ответов. 3. Выбрать два и более вариантов ответов, наиболее верных. 4. Записать только номера/буквы выбранных вариантов ответов.

Тестовые задания на установление соответствия

1. Соотнесите компонент триады CIA с его описанием.

Описание	Термин
А. Информация доступна только авторизованным пользователям	1. Целостность
Б. Информация не может быть изменена несанкционированно	2. Доступность
В. Информация доступна уполномоченным пользователям,	3. Конфиденциальность

когда необходимо	
------------------	--

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

2. Соотнесите тип угрозы с примером.

Описание	Тип угрозы
А. Наводнение в дата-центре	1. Непреднамеренная угроза
Б. Сотрудник случайно удалил важный файл	2. Преднамеренная угроза
В. Хакерская атака на сервер	3. Естественная угроза

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

3. Соотнесите тип шифрования с его характеристикой.

Характеристика	Тип шифрования
А. Используется один ключ для шифрования и расшифрования	1. Хэширование
Б. Используется пара ключей: открытый и закрытый	2. Асимметричное шифрование
В. Необратимое преобразование данных в строку фиксированной длины	3. Симметричное шифрование

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

4. Соотнесите криптографический алгоритм с его типом.

Тип	Алгоритм
А. Симметричное шифрование	1. SHA-256
Б. Асимметричное шифрование	2. RSA
В. Хэш-функция	3. AES

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В	Г

5. Соотнесите свойство цифровой подписи с решаемой задачей..

Обеспечиваемое свойство	Задача цифровой подписи
А. Целостность	1. Подтверждение авторства документа
Б. Неотказуемость	2. Гарантия, что документ не изменен после подписания
В. Аутентификация	3. Документ подписан конкретным лицом

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

6. Соотнесите средство защиты сети с его функцией.

Функция	Средство защиты сети
А. Фильтрация сетевого трафика на основе правил	1. VPN
Б. Обнаружение и сигнализация о подозрительной активности	2. Межсетевой экран (брандмауэр)
В. Создание зашифрованного канала связи через открытую сеть	3. Система обнаружения вторжений (IDS)

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

7. Соотнесите тип уязвимости веб-приложений с ее описанием.

Описание	Уязвимость
А. Внедрение вредоносного кода в запрос к базе данных	1. Межсайтовый скриптинг (XSS)
Б. Внедрение вредоносного скрипта в веб-страницу	2. SQL-инъекция
В. Нарушение контроля доступа, позволяющее получить несанкционированные права	3. Неправильная настройка прав доступа

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б

8. Соотнесите метод защиты данных с его описанием.

Описание	Метод защиты
А. Шифрование всех данных на жестком диске	1. Резервное копирование
Б. Периодическое сохранение копий данных для восстановления	2. Шифрование диска
В. Защита данных при передаче по сети с использованием сертификатов	3. TLS/SSL (HTTPS)

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

9. Соотнесите угрозу безопасности облачных технологий с ее описанием.

Описание	Угроза
А. Потеря доступа к данным из-за сбоя у провайдера	1. Недостаточная изоляция между клиентами
Б. Возможность доступа одного арендатора к данным другого	2. Нарушение доступности
В. Несанкционированный доступ к данным со стороны провайдера	3. Риск конфиденциальности

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

10. Соотнесите компонент инфраструктуры открытых ключей (PKI) с его назначением.

Назначение	Компонент
А. Организация, выпускающая и подтверждающая сертификаты	1. Закрытый ключ
Б. Электронный документ, удостоверяющий принадлежность открытого ключа владельцу	2. Удостоверяющий центр
В. Ключ, который хранится в секрете у владельца	3. Цифровой сертификат

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

11. Соотнесите вид социальной инженерии с его описанием.

Описание	Вид социальной инженерии
А. Злоумышленник выдает себя за сотрудника техподдержки	1. Фишинг
Б. Поддельное электронное письмо с просьбой ввести пароль	2. Претекстинг
В. Оставление зараженного USB-носителя в общедоступном месте	3. Подбрасывание носителя

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

12. Соотнесите этап управления инцидентами с выполняемым действием.

Действие	Этап управления инцидентами
А. Определение факта нарушения безопасности	1. Восстановление
Б. Устранение последствий и возврат к нормальной работе	2. Сдерживание
В. Локализация инцидента и предотвращение распространения	3. Обнаружение

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

13. Соотнесите правило цифровой гигиены с его описанием.

Описание	Правило
А. Использование уникальных сложных комбинаций для каждого сервиса	1. Регулярное обновление ПО
Б. Подтверждение входа через второй канал связи (SMS, приложение-аутентификатор)	2. Использование менеджера паролей
В. Своевременная установка исправлений безопасности	3. Двухфакторная аутентификация

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

14. Соотнесите принцип безопасной разработки с его описанием.

Описание	Принцип
А. Предоставление пользователю минимально необходимых прав для выполнения задач	1. Защита по умолчанию
Б. Безопасность должна быть встроена в продукт, а не добавлена в конце	2. Минимум привилегий
В. Система должна быть защищена даже при возникновении ошибок	3. Безопасность на всех этапах

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

15. Соотнесите тип вредоносного программного обеспечения с его характеристикой.

Характеристика	Тип вредоносного ПО
А. Саморазмножающаяся программа, распространяющаяся через сети	1. Троян
Б. Программа, маскирующаяся под полезное ПО, но выполняющая вредоносные действия	2. Червь
В. Программа, блокирующая доступ к данным с требованием выкупа	3. Вымогатель (Ransomware)

К каждой позиции первого столбца подберите соответствующую позицию второго и запишите его в таблицу выбранные цифры под соответствующими буквами.

А	Б	В

Тестовые задания на установление последовательности

1. Расположите этапы управления рисками информационной безопасности в правильной последовательности:

1. Обработка риска (выбор мер защиты)
2. Идентификация рисков
3. Оценка и анализ рисков

Правильная последовательность: _____

2. Расположите этапы процесса шифрования и расшифрования с использованием симметричного ключа в правильной последовательности:

1. Передача зашифрованного сообщения получателю
2. Шифрование сообщения с использованием секретного ключа
3. Расшифрование сообщения получателем с использованием того же секретного ключа

Правильная последовательность: _____

3. Расположите этапы работы цифровой подписи в правильной последовательности:

1. Получатель расшифровывает подпись открытым ключом отправителя
2. Отправитель создает хэш документа
3. Отправитель шифрует хэш своим закрытым ключом (создает подпись)
4. Получатель сравнивает полученный хэш с вычисленным хэшем документа

Правильная последовательность: _____

4. Расположите этапы настройки VPN-соединения в правильной последовательности:

1. Установка VPN-клиента на устройство пользователя
2. Аутентификация пользователя (логин, пароль, сертификат)
3. Установка зашифрованного туннеля между клиентом и сервером
4. Настройка параметров подключения (адрес сервера, протокол)

Правильная последовательность: _____

5. Расположите этапы реагирования на инцидент информационной безопасности в правильной последовательности:

1. Восстановление систем и возврат к нормальной работе
2. Обнаружение инцидента
3. Сдерживание и локализация инцидента
4. Расследование и анализ причин

Правильная последовательность: _____

6. Расположите этапы атаки SQL-инъекции в правильной последовательности:

1. Злоумышленник вводит вредоносный SQL-код в поле ввода на веб-странице
2. Приложение некорректно обрабатывает введенные данные
3. Злоумышленник получает несанкционированный доступ к базе данных или извлекает информацию

Правильная последовательность: _____

7. Расположите этапы фишинговой атаки в правильной последовательности:

1. Жертва переходит по ссылке и вводит свои учетные данные на поддельном сайте
2. Злоумышленник создает поддельное письмо, имитирующее официальное сообщение
3. Злоумышленник использует полученные данные для несанкционированного доступа
4. Письмо отправляется потенциальным жертвам

Правильная последовательность: _____

8. Расположите этапы создания резервной копии данных в правильной последовательности:

1. Выбор метода резервного копирования (полное, инкрементное, дифференциальное)
2. Определение критически важных данных для резервирования
3. Настройка расписания автоматического резервного копирования
4. Проверка целостности и восстановление тестовой копии

Правильная последовательность: _____

9. Расположите этапы безопасной разработки программного обеспечения (SDLC) в правильной последовательности:

1. Тестирование безопасности (статическое, динамическое)
2. Проектирование с учетом угроз (threat modeling)
3. Сбор и анализ требований безопасности
4. Развертывание и мониторинг безопасности в эксплуатации

Правильная последовательность: _____

10. Расположите этапы атаки социальной инженерии методом претекстинга в правильной по-

следовательности:

1. Злоумышленник собирает информацию о жертве (имя, должность, внутренние процессы)
2. Злоумышленник связывается с жертвой, представляясь сотрудником техподдержки или коллегой
3. Жертва под давлением или обманом предоставляет конфиденциальную информацию (пароль, доступ)
4. Злоумышленник использует полученные данные для доступа к системам

Правильная последовательность: _____

11. Расположите этапы внедрения системы управления доступом на основе ролей (RBAC) в правильной последовательности:

1. Назначение пользователям соответствующих ролей
2. Определение ролей в организации
3. Назначение разрешений (прав доступа) каждой роли

Правильная последовательность: _____

12. Расположите этапы проверки подлинности с использованием двухфакторной аутентификации в правильной последовательности:

1. Система запрашивает второй фактор (код из приложения, SMS)
2. Пользователь вводит логин и пароль (первый фактор)
3. Пользователь вводит код второго фактора
4. Система предоставляет доступ после успешной проверки обоих факторов

Правильная последовательность: _____

13. Расположите этапы процесса управления уязвимостями в правильной последовательности:

1. Устранение или снижение рисков (установка патчей, настройка защиты)
2. Обнаружение и идентификация уязвимостей (сканирование, тестирование)
3. Приоритизация уязвимостей на основе критичности
4. Оценка и подтверждение устранения уязвимостей

Правильная последовательность: _____

14. Расположите этапы создания цифрового сертификата в инфраструктуре открытых ключей (PKI) в правильной последовательности:

1. Формирование запроса на сертификат (CSR) с открытым ключом
2. Генерация пары ключей (открытый и закрытый) пользователем
3. Выпуск и подпись цифрового сертификата удостоверяющим центром
4. Установка сертификата на устройство пользователя

Правильная последовательность: _____

15. Расположите этапы реализации концепции Zero Trust в организации в правильной последовательности:

1. Постоянный мониторинг и проверка каждого запроса доступа
2. Сегментация сети и разделение ресурсов
3. Внедрение многофакторной аутентификации для всех пользователей
4. Определение всех пользователей, устройств и ресурсов

Правильная последовательность: _____

Тестовые задания с выбором двух (и более) правильных ответов из перечня

1. Какие три компонента составляют классическую триаду информационной безопасности (CIA)?
 1. Конфиденциальность
 2. Скорость доступа
 3. Целостность
 4. Доступность
 5. Экономическая эффективность

2. Какие из перечисленных угроз относятся к категории естественных (природных) угроз информационной безопасности?
 1. Хакерская атака
 2. Землетрясение
 3. Наводнение
 4. Ошибка системного администратора
 5. Пожар в дата-центре

3. Какие из перечисленных алгоритмов относятся к симметричному шифрованию?
 1. RSA
 2. AES
 3. 3DES
 4. ECC
 5. Blowfish

4. Какие из перечисленных алгоритмов относятся к хэш-функциям?
 1. MD5
 2. RSA
 3. SHA-256
 4. AES
 5. SHA-1

5. Какие задачи решает использование цифровой подписи?
 1. Шифрование больших объемов данных
 2. Подтверждение авторства документа
 3. Обеспечение целостности документа
 4. Увеличение скорости передачи данных
 5. Обеспечение неотказуемости (невозможность отказа от авторства)

6. Какие из перечисленных средств используются для защиты сетевой инфраструктуры?
 1. Межсетевой экран (брандмауэр)
 2. Антивирусное ПО на рабочей станции
 3. Система обнаружения вторжений (IDS)
 4. VPN (виртуальная частная сеть)
 5. Текстовый редактор

7. Какие из перечисленных уязвимостей входят в OWASP Top 10 для веб-приложений?
 1. SQL-инъекция

2. Недостаточная мощность процессора
 3. Межсайтовый скриптинг (XSS)
 4. Неправильная настройка прав доступа
 5. Отсутствие резервного копирования
8. Какие методы защиты данных в состоянии покоя (на диске) вы знаете?
1. Шифрование диска (BitLocker, LUKS)
 2. Регулярное резервное копирование
 3. Использование VPN
 4. Установка межсетевого экрана
 5. Шифрование отдельных файлов и папок
9. Какие из перечисленных угроз характерны для облачных технологий?
1. Недостаточная изоляция между арендаторами
 2. Потеря данных из-за сбоя провайдера
 3. Повышенная скорость работы
 4. Риск несанкционированного доступа со стороны провайдера
 5. Автоматическое обновление ПО
10. Какие этапы входят в процесс реагирования на инциденты информационной безопасности?
1. Обнаружение инцидента
 2. Разработка нового программного обеспечения
 3. Сдерживание и локализация
 4. Расследование и анализ
 5. Восстановление систем
11. Какие из перечисленных методов относятся к социальной инженерии?
1. Фишинг
 2. SQL-инъекция
 3. Претекстинг (предлог)
 4. Подбрасывание носителя (USB-ловушка)
 5. DDoS-атака
12. Какие факторы аутентификации используются в многофакторной аутентификации?
1. То, что вы знаете (пароль, PIN-код)
 2. То, что вы имеете (смарт-карта, токен)
 3. То, чем вы являетесь (биометрия)
 4. То, где вы находитесь (геолокация)
 5. То, что вы любите (предпочтения)
13. Какие из перечисленных правил относятся к цифровой гигиене ИТ-специалиста?
1. Использовать один и тот же пароль для всех сервисов
 2. Включить двухфакторную аутентификацию
 3. Регулярно обновлять программное обеспечение
 4. Использовать менеджер паролей
 5. Записывать пароли на стикере и клеить на монитор
14. Какие принципы безопасной разработки программного обеспечения (DevSecOps) являются ключевыми?
1. Безопасность встраивается на всех этапах разработки
 2. Тестирование безопасности проводится только перед релизом
 3. Автоматизация проверок безопасности
 4. Использование принципа наименьших привилегий
 5. Безопасность — ответственность только специалистов по ИБ

15. Какие виды вредоносного программного обеспечения (ВПО) относятся к категории «само распространяющихся»?

1. Троян
2. Червь
3. Вымогатель (Ransomware)
4. Сетевой червь
5. Кейлоггер

16. Какие меры защиты от SQL-инъекций являются эффективными?

1. Использование параметризованных запросов
2. Валидация и экранирование пользовательского ввода
3. Отключение межсетевого экрана
4. Использование хранимых процедур
5. Установка антивируса на сервер баз данных

17. Какие компоненты входят в инфраструктуру открытых ключей (PKI)?

1. Удостоверяющий центр (CA)
2. Регистрационный центр (RA)
3. База данных паролей
4. Список отозванных сертификатов (CRL)
5. Антивирусный сервер

18. Какие из перечисленных протоколов обеспечивают безопасную передачу данных по сети?

1. HTTPS
2. FTP
3. SSH
4. TLS/SSL
5. HTTP

19. Какие элементы должны содержаться в политике информационной безопасности организации?

1. Правила парольной политики
2. Список запрещенных действий сотрудников
3. Личные предпочтения руководителя
4. Ответственность за нарушение требований безопасности
5. План эвакуации при пожаре

20. Какие концепции и технологии формируют будущее информационной безопасности?

1. Zero Trust (нулевое доверие)
2. Искусственный интеллект и машинное обучение для обнаружения атак
3. Отказ от аутентификации
4. Security as a Service (SECaaS)
5. Использование только симметричного шифрования

Практические задания

Задание 1. Опишите способ перевода шестнадцатеричного числа в двоичное. Число EE816 переведите в двоичную систему счисления.

Задание 2. Опишите способ перевода восьмеричного числа в двоичное. Число 5318 перевести в двоичную систему счисления.

- Задание 3.** Перевести данные числа из двоичной системы счисления в десятичную и наоборот. 1001110011_2 , 10110101_2
- Задание 4.** Перевести данные числа из восьмеричной системы счисления в десятичную и наоборот. 671_8 , 250_8
- Задание 5.** Перевести данные числа из шестнадцатеричной системы счисления в десятичную и наоборот. $41A_{16}$, $1C2_{16}$
- Задание 6.** Перевести данные числа из двоичной системы счисления в восьмеричную и наоборот. 100000110_2 , 110011101_2
- Задание 7.** Перевести данные числа из двоичной системы счисления в шестнадцатеричную и наоборот. 11110001001_2 , 10101011101_2
- Задание 8.** Перевести данные числа из восьмеричной системы счисления в шестнадцатеричную и наоборот. 52_8 , 324_8
- Задание 9.** Перевести данные числа из двоичной системы счисления в десятичную и наоборот. 1001000_2 , 1111100111_2
- Задание 10.** Перевести данные числа из восьмеричной системы счисления в десятичную и наоборот. 164_8 , 255_8
- Задание 11.** Перевести данные числа из шестнадцатеричной системы счисления в десятичную и наоборот. 118_{16} , $2B_{16}$
- Задание 12.** Перевести данные числа из двоичной системы счисления в восьмеричную и наоборот. 1010001100_2 , 100000101_2
- Задание 13.** Перевести данные числа из двоичной системы счисления в шестнадцатеричную и наоборот. 10110001011_2 , 11101011001_2
- Задание 14.** Перевести данные числа из восьмеричной системы счисления в шестнадцатеричную и наоборот. 413_8 , 670_8
- Задание 15.** Перевести данные числа из двоичной системы счисления в десятичную и наоборот. 1100000000_2 , 1101011111_2
- Задание 16.** Перевести данные числа из восьмеричной системы счисления в десятичную и наоборот. 273_8 , 156_8
- Задание 17.** Перевести данные числа из шестнадцатеричной системы счисления в десятичную и наоборот. $11B_{16}$, $10A_{16}$
- Задание 18.** Перевести данные числа из двоичной системы счисления в восьмеричную и наоборот. 1010001100_2 , 100000101_2
- Задание 19.** Перевести данные числа из двоичной системы счисления в шестнадцатеричную и наоборот. 10110001000_2 , 11000000000001_2
- Задание 20.** Перевести данные числа из восьмеричной системы счисления в шестнадцатеричную и наоборот. 1017_8 , 661_8
- Задание 21.** Перевести данные числа из двоичной системы счисления в десятичную и наоборот. 1100001001_2 , 1100100101_2
- Задание 22.** Перевести данные числа из восьмеричной системы счисления в десятичную и наоборот. 105_8 , 357_8
- Задание 23.** Перевести данные числа из шестнадцатеричной системы счисления в десятичную и наоборот. 334_{16} , AC_{16}
- Задание 24.** Перевести данные числа из двоичной системы счисления в восьмеричную и наоборот. 1111110110_2 , 11001100_2
- Задание 25.** Перевести данные числа из двоичной системы счисления в шестнадцатеричную и наоборот. 10111000_2 , 110001111_2
- Задание 26.** Перевести данные числа из восьмеричной системы счисления в шестнадцатеричную и наоборот. 112_8 , 61_8
- Задание 27.** Перевести данные числа из двоичной системы счисления в десятичную и наоборот. 1101010001_2 , 100011100_2
- Задание 28.** Создайте презентацию-приглашение из 4-5 слайдов о научно-практической студенческой конференции. Выполните для одного слайда эффекты анимации для всех его объектов. Скройте один из слайдов. Просмотрите презентацию, покажите скрытый слайд.
- Задание 29.** Создайте презентацию учебника по медицинской информатике (5-7 слайдов). Уста-

новите различные варианты переходов слайдов. Для маркированных списков создайте эффекты анимации.

Задание 30. В два столбца электронной таблицы введите 10 четных и 10 нечетных чисел (соответственно 1 и 2 столбец), в третьем столбце просчитайте посредством формул их произведение за вычетом числа из первого столбца, в четвертом – разность их кубов.

Задание 31. Для решения практического задания по одной из дисциплин, вам нужно провести подробный анализ существующей литературы. Дисциплина на ваш выбор. Для поиска информации используйте сеть Интернет

Задание 32. Вы получили новый компьютер со склада. Компьютер предназначен для работы с больничной документацией (электронного документооборота в больнице нет) и для доступа в Интернет. Какой минимальный набор программ вы установите? Приведите примеры программ, которые распространяются бесплатно или условно бесплатно (свободное программное обеспечение).

Ключи к ответам тестовых заданий

Ключи к ответам тестовых заданий на установление соответствия:

Ответы:

Установление соответствия

1.

A	Б	В
3	1	2

2.

A	Б	В
3	1	2

3.

A	Б	В
3	2	1

4.

A	Б	В
3	2	1

5.

A	Б	В
2	1	3

6.

A	Б	В
2	3	1

7.

A	Б	В

8.

A	Б	В
2	1	3

9.

A	Б	В
2	1	3

10.

A	Б	В
2	3	1

11.

A	Б	В

12.	2	1	3
	А	Б	В
	3	1	2
13.	А	Б	В
	2	3	1
14.	А	Б	В
	2	3	1
15.	А	Б	В
	2	1	3

Ключи к ответам тестовых заданий на установление последовательности

- 1) 2, 3, 1
- 2) 2, 1, 3
- 3) 2, 3, 1, 4
- 4) 1, 4, 2, 3
- 5) 2, 3, 4, 1
- 6) 1, 2, 3
- 7) 2, 4, 1, 3
- 8) 2, 1, 3, 4
- 9) 3, 2, 1, 4
- 10) 1, 2, 3, 4
- 11) 2, 3, 1
- 12) 2, 1, 3, 4
- 13) 2, 3, 1, 4
- 14) 2, 1, 3, 4
- 15) 4, 2, 3, 1

Ключи к ответам тестовых заданий с выбором двух и более правильных ответов из перечня

- 1) 1, 3, 4
- 2) 2, 3, 5
- 3) 2, 3, 5
- 4) 1, 3, 5
- 5) 2, 3, 5
- 6) 1, 3, 4
- 7) 1, 3, 4
- 8) 1, 2, 5
- 9) 1, 2, 4
- 10) 1, 3, 4, 5
- 11) 1, 3, 4
- 12) 1, 2, 3
- 13) 2, 3, 4
- 14) 1, 3, 4
- 15) 2, 4
- 16) 1, 2, 4
- 17) 1, 2, 4
- 18) 1, 3, 4
- 19) 1, 2, 4

5. Критерии и шкала оценивания компетенций на различных этапах их формирования

КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ ОТВЕТОВ НА УСТНЫЕ ВОПРОСЫ

№ п/п	Критерии оценивания	Шкала оценивания
1.	1) полно и аргументированно отвечает по содержанию задания; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3) излагает материал последовательно и правильно.	отлично
2.	студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет.	хорошо
3.	ставится, если студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.	удовлетворительно
4.	студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.	неудовлетворительно

КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ

№ п/п	тестовые нормы: % правильных ответов	Шкала оценивания
1	85-100 %	отлично
2	70-84%	хорошо
3	51-69%	удовлетворительно
4	менее 50%	неудовлетворительно

КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ РЕФЕРАТА, СООБЩЕНИЯ

№ п/п	Критерии оценивания	Шкала оценивания
1.	ответ аргументирован, обоснован и дана самостоятельная оценка изученного материала	отлично
2.	ответ аргументирован, последователен, но допущены некоторые неточности	хорошо
3.	ответ является неполным и имеет существенные логические несоответствия	удовлетворительно
4.	в ответе отсутствует аргументация, тема не раскрыта	неудовлетворительно

**КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ КОНТРОЛЬНЫХ ВОПРОСОВ
ПО ТЕМАТИКЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

№ п/п	Критерии оценивания	Шкала оценивания
1	<p>Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал различной литературы, правильно обосновывает принятое нестандартное решение, владеет разносторонними навыками и приемами</p>	«отлично» / зачтено
	<p>выполнения практических задач по формированию общепрофессиональных компетенций.</p>	
2	<p>Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, а также имеет достаточно полное представление о значимости знаний по дисциплине.</p>	«хорошо» / зачтено
3	<p>Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает сложности при выполнении практических работ и затрудняется связать теорию вопроса с практикой.</p>	«удовлетворительно» / зачтено
4	<p>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, неуверенно отвечает, допускает серьезные ошибки, не имеет представлений по методике выполнения практической работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по данной дисциплине.</p>	«неудовлетворительно»/ незачтено

КРИТЕРИИ И ШКАЛА ОЦЕНИВАНИЯ УРОВНЕЙ ОСВОЕНИЯ КОМПЕТЕНЦИЙ

Шкала оценивания	Уровень освоения компетенции	Критерии освоения компетенции
зачтено	высокий	студент, овладел элементами компетенции «знать», «уметь», проявил всесторонние и глубокие знания программного материала по дисциплине, освоил основную и дополнительную литературу, обнаружил творческие способности в понимании, изложении и практическом использовании усвоенных знаний.
зачтено	базовый	студент овладел элементами компетенции «знать» и «уметь», проявил полное знание программного материала по дисциплине, освоил основную рекомендованную литературу, обнаружил стабильный характер знаний и умений и проявил способности к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.
зачтено	нормативный	студент овладел элементами компетенции «знать», проявил знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, изучил основную рекомендованную литературу, допустил неточности в ответе на экзамене, но в основном обладает необходимыми знаниями для их устранения при корректировке со стороны экзаменатора.
незачтено	компетенции не сформированы	студент не овладел ни одним из элементов компетенции, обнаружил существенные пробелы в знании основного программного материала по дисциплине, допустил принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Шкала оценивания	Уровень освоения компетенции	Критерии освоения компетенции
отлично	высокий	студент, овладел элементами компетенции «знать», «уметь», проявил всесторонние и глубокие знания программного материала по дисциплине, освоил основную и дополнительную литературу, обнаружил творческие способности в понимании, изложении и практическом использовании усвоенных знаний.
хорошо	базовый	студент овладел элементами компетенции «знать» и «уметь», проявил полное знание программного материала по дисциплине, освоил основную рекомендованную литературу, обнаружил стабильный характер знаний и умений и проявил способности к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.
удовлетворительно	нормативный	студент овладел элементами компетенции «знать», проявил знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, изучил основную рекомендованную литературу, допустил неточности в ответе на экзамене, но в основном обладает необходимыми знаниями для их устранения при корректировке со стороны экзаменатора.
неудовлетворительно	компетенции не сформированы	студент не овладел ни одним из элементов компетенции, обнаружил существенные пробелы в знании основного программного материала по дисциплине, допустил принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

6. Описание процедуры оценивания знаний и умений, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующих этапы формирования компетенций по дисциплине, осуществляется в ходе текущего и промежуточного контроля. Текущий контроль организуется в формах: устного опроса (беседы, индивидуального опроса), защиты рефератов, сообщений; тестирования.

Промежуточная аттестация осуществляется в форме дифференцированного зачета. Каждая форма промежуточного контроля должна включать в себя вопросы, позволяющие оценить уровень освоения студентами знаний.

Процедура оценивания компетенций обучающихся основана на следующих принципах: периодичности проведения оценки, многоступенчатости оценки по устранению недостатков, единства используемой технологии для всех обучающихся, выполнения условий сопоставимости результатов оценивания, соблюдения последовательности проведения оценки.

Краткая характеристика процедуры реализации текущего контроля и промежуточной аттестации для оценки компетенций обучающихся включает:

сообщение - продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Подготовка осуществляется во внеурочное время. В оценивании результата наравне с преподавателем могут принимать участие студенты группы.

устный опрос – устный опрос по основным терминам может проводиться в начале/конце лекционного или практического занятия в течении 15-20 мин. Либо устный опрос проводится в течение всего практического занятия по заранее выданной тематике.

тестовые задания – позволяют оценить уровень знаний студентами теоретического материала по дисциплине. Осуществляется на бумажных носителях по вариантам.

реферат - продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Защита реферата проводится на занятии.

Изложенное понимание реферата как целостного авторского текста определяет критерии его оценки: новизна текста; обоснованность выбора источника; степень раскрытия сущности вопроса; соблюдения требований к оформлению.

Новизна текста: а) актуальность темы исследования; б) новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); в) умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; г) явленность авторской позиции, самостоятельность оценок и суждений; д) стилевое единство текста, единство жанровых черт.

Степень раскрытия сущности вопроса: а) соответствие плана теме реферата; б) соответствие содержания теме и плану реферата; в) полнота и глубина знаний по теме; г) обоснованность способов и методов работы с материалом; е) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме).

Обоснованность выбора источников: а) оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования (в т.ч. журнальные публикации последних лет, интернет-ресурсы и т.д.).

Соблюдение требований к оформлению: а) насколько верно оформлены ссылки на используемую литературу, список литературы; б) оценка грамотности и культуры изложения.

Дифференцированный зачет проводится в срок согласно графику учебного про-

цесса.