

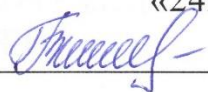
Министерство образования Ростовской области
государственное бюджетное профессиональное образовательное учреждение
Ростовской области
«Белокалитвинский гуманитарно-индустриальный техникум»
(ГБПОУ РО «БГИТ»)

Приложение 4.25
к ОПОП по специальности
09.02.11 «Разработка и управление
программным обеспечением»

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ
для проведения процедуры оценки уровня освоения обучающимися
ФГОС СПО по учебной дисциплине
ОП.05 Основы информационной безопасности
специальность 09.02.11 Разработка и управление программным
обеспечением

г. Белая Калитва
2025 г.

Рассмотрена
на заседании цикловой комиссии
специальности 09.02.11 Разработка и
управление программным обеспечением
Протокол № 4
от «23» декабря 2025г.
Председатель ЦК
 Комиссарова И.В.

УТВЕРЖДАЮ
Заместитель директора по УМР
«24» декабря 2025 г.
 Г. В. Шматко

Комплект оценочных средств разработан в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.11 «Разработка и управление программным обеспечением», утверждённым приказом Министерства просвещения Российской Федерации от 24 февраля 2025 г. № 138; Рабочей программой по учебной дисциплине ОП.05 Основы информационной безопасности и Методическими рекомендациями по формированию комплекта оценочных материалов образовательной программы среднего профессионального образования.

Организация – разработчик: государственное бюджетное профессиональное образовательное учреждение Ростовской области «Белокалитвинский гуманитарно-индустриальный техникум»

Разработчик:

Комиссарова Ирина Викторовна – преподаватель высшей категории.

СОДЕРЖАНИЕ

1	Спецификация комплекта оценочных средств.	4
1.1	Назначение комплекта оценочных средств.	4
1.2	Общее количество тестовых заданий.	4
1.3	Распределение тестовых заданий по компетенциям и дисциплинам ...	5
1.4	Типы, уровни сложности и время выполнения тестовых заданий.....	7
1.5	Система оценивания выполнения тестовых заданий.....	9
1.6	Описание дополнительных материалов и оборудования, необходимых для выполнения тестовых заданий.....	11
1.7	Продолжительность выполнения.....	12
1.8	Инструкция по организации и проведению тестирования.....	12
2	Тестовые задания	14
2.1	Вариант 1	14
2.2	Вариант 2	20
2.3	Вариант 3	26
2.4	Вариант 4	32
3	Ключи к оцениванию тестовых заданий	38

1. Спецификация комплекта оценочных средств.

1.1. Назначение комплекта оценочных средств.

Оценка уровня сформированности компетенций у обучающихся по дисциплине ОП.05 Основы информационной безопасности для специальности 09.02.11.

1.2. Общее количество тестовых заданий.

Количество заданий в комплекте оценочных материалов

Код компетенции	Наименование компетенции	Количество заданий
ОК 01	Выбирать способы решения задач профессиональной деятельности	4
ОК 02	Осуществлять поиск, анализ и интерпретацию информации	8
ОК 03	Планировать и реализовывать собственное профессиональное развитие	8
ОК 04	Осуществлять профессиональную деятельность в условиях обновления её целей, содержания, смены технологий	12
ОК 05	Организовывать собственную деятельность	8
ОК 09	Использовать информационные технологии в профессиональной деятельности	8
ПК 1.5	Участвовать в обеспечении информационной безопасности	12
ПК 2.4	Выполнять работы по проектированию, модификации, тестированию и отладке программного обеспечения	8
ПК 3.5	Участвовать в сопровождении программного обеспечения	12
ПК 4.4	Обеспечивать безопасность функционирования программного обеспечения	10

Всего заданий в комплекте: 80 заданий (4 варианта × 20 заданий)

1.3.Распределение тестовых заданий по компетенциям и дисциплинам

Распределение заданий по компетенциям и дисциплинам

Код компетенции	Наименование компетенции	Наименование индикаторов сформированности компетенции	Наименование дисциплины/ модуля/ практики	Семестр	Номер задания
ОК 01	Выбирать способы решения задач профессиональной деятельности	Способность анализировать виды угроз информационной безопасности	ОП.05 Основы информационной безопасности	4	3, 13, 18
ОК 02	Осуществлять поиск, анализ и интерпретацию информации	Умение классифицировать угрозы, уязвимости и риски ИБ	ОП.05 Основы информационной безопасности	4	1, 7, 11, 12, 14, 15, 18, 20
ОК 03	Планировать и реализовывать собственное профессиональное развитие	Способность применять методы управления рисками ИБ	ОП.05 Основы информационной безопасности	4	2, 8, 16, 17
ОК 04	Осуществлять профессиональную деятельность в условиях обновления её целей, содержания, смены технологий	Владение современными методами защиты информации	ОП.05 Основы информационной безопасности	4	4, 9, 14, 19
ОК 05	Организовывать собственную деятельность	Способность применять криптографические методы защиты	ОП.05 Основы информационной безопасности	4	5, 10, 20
ОК 09	Использовать информационные технологии в	Умение использовать инструменты анализа безопасности	ОП.05 Основы информационной безопасности	4	6, 12, 17

	профессиональной деятельности				
ПК 1.5	Участвовать в обеспечении информационной безопасности	Способность применять методы и средства защиты информации	ОП.05 Основы информационной безопасности	4	1, 5, 8, 12, 15, 18
ПК 2.4	Выполнять работы по проектированию, модификации, тестированию и отладке программного обеспечения	Умение выявлять уязвимости в программном коде	ОП.05 Основы информационной безопасности	4	3, 9, 15, 19
ПК 3.5	Участвовать в сопровождении программного обеспечения	Способность проводить аудит безопасности	ОП.05 Основы информационной безопасности	4	2, 6, 10, 13, 17
ПК 4.4	Обеспечивать безопасность функционирования программного обеспечения	Владение методами реагирования на инциденты ИБ	ОП.05 Основы информационной безопасности	4	4, 7, 11, 14, 16, 20

1.4. Типы, уровни сложности и время выполнения тестовых заданий

Распределение заданий по типу и уровням сложности

Код компетенции	Индикаторы сформированности компетенции	Номер задания	Тип задания	Уровень сложности и задания	Время выполнения (мин)
ОК 1	Способность анализировать виды угроз информационной безопасности	3, 13, 18	Выбор одного правильного ответа с обоснованием	Б	7, 4, 4
ОК 2	Умение классифицировать угрозы, уязвимости и риски ИБ	1, 7, 11, 14, 15	Установление соответствия, Установление последовательности, Установление соответствия, Выбор всех правильных ответов с обоснованием, Открытый вопрос (написание кода)	Б, Б, Б, П, В	5, 6, 5, 8, 12
ОК 3	Способность применять методы управления рисками ИБ	2, 8, 16	Установление последовательности, Выбор одного правильного ответа с обоснованием, Установление соответствия	Б, Б, Б	6, 4, 5
ОК 4	Владение современными методами защиты информации	4, 9, 19	Выбор всех правильных ответов с обоснованием, Выбор всех правильных ответов с обоснованием, Выбор всех правильных ответов с обоснованием	П, П, П	8, 7, 7
ОК 5	Способность применять криптографические методы защиты	5, 10, 20	Открытый вопрос, Открытый вопрос, Открытый вопрос (анализ кода)	П, П, В	10, 10, 12

ОК 9	Умение использовать инструменты анализа безопасности	6, 12, 17	Установление соответствия, Установление последовательности, Установление последовательности	Б, Б, Б	5, 6, 6
ПК 1.5	Способность применять методы и средства защиты информации	1, 5, 8, 12, 18	Установление соответствия, Открытый вопрос, Выбор одного правильного ответа с обоснованием, Установление последовательности, Выбор одного правильного ответа с обоснованием	Б, П, Б, Б, Б	5, 10, 4, 6, 4
ПК 2.4	Умение выявлять уязвимости в программном коде	3, 9, 15, 19	Выбор одного правильного ответа с обоснованием, Выбор всех правильных ответов с обоснованием, Открытый вопрос (написание кода), Выбор всех правильных ответов с обоснованием	Б, П, В, П	7, 7, 12, 7
ПК 3.5	Способность проводить аудит безопасности	2, 6, 10, 13, 17	Установление последовательности, Установление соответствия, Открытый вопрос, Выбор одного правильного ответа с обоснованием, Установление последовательности	Б, Б, П, Б, Б,	6, 5, 10, 4, 6
ПК 4.4	Владение методами реагирования на инциденты ИБ	4, 7, 11, 14, 16, 20	Выбор всех правильных ответов с обоснованием,	П, Б, Б, П, Б, В	8, 6, 5, 8, 5, 12

			Установление последовательности, Установление соответствия, Выбор всех правильных ответов с обоснованием, Установление соответствия, Открытый вопрос (анализ кода)		
--	--	--	--	--	--

1.5. Система оценивания выполнения тестовых заданий

Система оценивания заданий

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/ характеристика правильности ответа)
1	За каждый правильный элемент соответствия - 0.5 балла. Всего 4 соответствия.	0-2 балла. Полный балл - все 4 соответствия установлены верно
2	За правильную последовательность - 2 балла. За 1 ошибку - 1 балл. За 2 и более ошибок - 0 баллов	0-2 балла
3	За правильный ответ - 1 балл. За правильное обоснование - 1 балл	0-2 балла
4	За каждый правильный ответ - 0.5 балла. За правильное обоснование - 1 балл. Максимум за задание - 3 балла	0-3 балла
5	По 1 баллу за каждый из 4 принципов безопасного хранения паролей. За полный, развернутый ответ - дополнительно 1 балл	0-5 баллов
6	За каждый правильный элемент соответствия - 0.5 балла. Всего 3 соответствия	0-1.5 балла
7	За правильную последовательность - 2 балла. За 1 ошибку - 1 балл. За 2 и более ошибок - 0 баллов	0-2 балла
8	За правильный ответ - 1 балл. За правильное обоснование - 1 балл	0-2 балла
9	За каждый правильный ответ - 0.5 балла. За правильное обоснование - 1 балл. Максимум за задание - 3 балла	0-3 балла

10	По 1 баллу за каждый из 5 этапов аудита безопасности. За полный, структурированный ответ - дополнительно 1 балл	0-6 баллов
11	За каждый правильный элемент соответствия - 0.5 балла. Всего 3 соответствия	0-1.5 балла
12	За правильную последовательность - 2 балла. За 1 ошибку - 1 балл. За 2 и более ошибок - 0 баллов	0-2 балла
13	За правильный ответ - 1 балл. За правильное обоснование - 1 балл	0-2 балла
14	За каждый правильный ответ - 0.5 балла. За правильное обоснование - 1 балл. Максимум за задание - 3 балла	0-3 балла
15	Критерии: работает корректно - 2 балла, проверяет все условия - 2 балла, правильный синтаксис - 1 балл, комментарии - 1 балл	0-6 баллов
16	За каждый правильный элемент соответствия - 0.5 балла. Всего 3 соответствия	0-1.5 балла
17	За правильную последовательность - 2 балла. За 1 ошибку - 1 балл. За 2 и более ошибок - 0 баллов	0-2 балла
18	За правильный ответ - 1 балл. За правильное обоснование - 1 балл	0-2 балла
19	За каждый правильный ответ - 0.5 балла. За правильное обоснование - 1 балл. Максимум за задание - 3 балла	0-3 балла
20	Критерии: выявление уязвимости - 2 балла, предложение исправления - 2 балла, правильность исправления - 2 балла	0-6 баллов

Максимальное количество баллов – 54.

Оценка «5» (отлично) соответствует результатам, содержащим 48 – 54 баллов (90-100%).

Оценка «4» (хорошо) — 37 – 47 баллов (70-89%).

Оценка «3» (удовлетворительно) — 27 – 36 баллов (50-69%).

Оценка «2» (неудовлетворительно) — менее 27 баллов (менее 50 %).

Примечания по оцениванию:

Задания на соответствие (1, 6, 11, 16): оцениваются по 0.5 балла за каждый правильный элемент

Задания на последовательность (2, 7, 12, 17): оцениваются целиком за правильный порядок

Задания с выбором одного ответа (3, 8, 13, 18): раздельное оценивание ответа и обоснования

Задания с выбором нескольких ответов (4, 9, 14, 19): учитывается как правильность выбора, так и обоснование

Открытые теоретические вопросы (5, 10): оцениваются по полноте и правильности ответа

Задания с написанием/анализом кода (15, 20): оцениваются по функциональности, правильности и безопасности решения

Рекомендации по проверке:

Частично правильные ответы оцениваются пропорционально их полноте

При наличии грубых ошибок в обосновании, даже при правильном ответе, баллы снижаются

Критерии оценивания открытых вопросов должны быть доведены до обучающихся перед выполнением работы.

1.6. Описание дополнительных материалов и оборудования, необходимых для выполнения тестовых заданий

Код компетенции	Наименование компетенции	Дополнительные материалы и оборудование
ОК 01	Выбирать способы решения задач профессиональной деятельности	Бланки ответов, черновики, ручки
ОК 02	Осуществлять поиск, анализ и интерпретацию информации	Бланки заданий, бланки ответов, черновики
ОК 03	Планировать и реализовывать собственное профессиональное развитие	стандартные условия
ОК 04	Осуществлять профессиональную деятельность в условиях обновления её целей, содержания, смены технологий	стандартные условия
ОК 05	Организовывать собственную деятельность	Бланки ответов, черновики
ОК 09	Использовать информационные технологии в профессиональной деятельности	стандартные условия
ПК 1.5	Участвовать в обеспечении информационной безопасности	стандартные условия

ПК 2.4	Выполнять работы по проектированию, модификации, тестированию и отладке программного обеспечения	стандартные условия
ПК 3.5	Участвовать в сопровождении программного обеспечения	стандартные условия
ПК 4.4	Обеспечивать безопасность функционирования программного обеспечения	стандартные условия

1.7.Продолжительность выполнения

Общее время, отведенное на выполнение задания, не более двух академических часов.

Распределение времени рекомендуется следующим образом:

Тип задания	Количество заданий в варианте	Примерное время на задание	Общее время
Установление соответствия	4	5–6 минут	20–24 мин
Установление последовательности	4	6 минут	24 мин
Выбор одного ответа с обоснованием	4	4–7 минут	16–28 мин
Выбор всех правильных ответов с обоснованием	4	7–8 минут	28–32 мин
Открытый теоретический вопрос	2	10 минут	20 мин
Написание / анализ кода	2	12 минут	24 мин
Итого	20	—	≈ 90 мин

При необходимости допускается увеличение времени до 120 минут для обучающихся с особыми образовательными потребностями.

1.8.Инструкция по организации и проведению тестирования

Действия преподавателя во время проведения тестирования:

- 1) приветствует обучающихся;
- 2) объясняет обучающимся цель предстоящей работы: получение объективной информации о состоянии качества подготовки и освоения

- обучающимися основной профессиональной образовательной программы; доводит правила проведения тестирования;
- 3) устанавливает соответствие представленного профессиональной образовательной организацией списка группы и списка обучающихся, фактически присутствующих;
 - 4) раздает обучающимся бланки заданий и бланки ответов;
 - 5) знакомит со структурой заданий, отмечает особенности, объясняет правила заполнения бланков ответов;
 - 6) обращается к обучающимся: «Есть ли вопросы?» (не имеет права отвечать на вопросы по содержанию заданий);
 - 7) фиксирует время начала и время окончания работы на видном месте (доске);
 - 8) отслеживает полную самостоятельность обучающихся при выполнении работы;
 - 9) предупреждает обучающихся о том, что до конца процедуры осталось 10 мин;
 - 10) по истечении времени выполнения работы собирает материалы работы (заполненные бланки ответов); проверяет соответствие количества работ числу испытуемых обучающихся;
 - 11) благодарит обучающихся за участие в работе, желает успехов.

После завершения задания преподавателям выдаются эталоны ответов для каждого варианта заданий, работы проверяются преподавателями, проводящими проверочную работу согласно системе оценивания заданий и работы в целом. По итогу заполняется протокол.

Действия обучающихся при выполнении тестового задания:

- 1) внимательно читайте все задания работы и указания по его выполнению;
- 2) если не можете выполнить очередное задание, не тратьте время, переходите к следующему;
- 3) только выполнив все задания, вернитесь к тем, которые у вас не получились сразу;
- 4) старайтесь работать быстро и аккуратно;
- 5) все задания выполнять на выданных листах;
- 6) если ошибся, зачеркни ошибку и выбери другой ответ;
- 7) после выполнения всех заданий осуществить проверку.
- 8) сдать заполненные бланки ответов преподавателю.

2. Тестовые задания

2.1. Вариант 1

Задание 1 (ОК 02, ПК 1.5). Установите соответствие между понятиями и их определениями (время: 5 мин):

Инструкция: Соотнесите понятия (А – Г) с их определениями (1 – 5). В правом столбце есть один лишний вариант.

Понятия		Определения	
А.	Угроза ИБ	1.	Свойство информации быть доступной для авторизованных пользователей
Б.	Уязвимость	2.	Потенциальная возможность нарушения безопасности
В.	Риск	3.	Слабость системы, которую можно использовать для атаки
Г.	Конфиденциальность	4.	Ожидаемый ущерб от реализации угрозы
		5.	Свойство информации быть защищенной от несанкционированного доступа

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В	Г

Задание 2 (ОК 03, ПК 3.5). Установите последовательность этапов управления рисками ИБ (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Идентификация активов
2. Оценка рисков
3. Выбор мер защиты
4. Внедрение мер
5. Мониторинг и переоценка

Ответ:

Задание 3 (ОК 01, ПК 2.4). Выберите ОДИН правильный ответ и обоснуйте его (время: 7 мин).

Инструкция: Какая из перечисленных атак относится к типу «Отказ в обслуживании» (DoS)?

1. SQL-инъекция
2. Фишинг
3. SYN-флуд
4. XSS

Ответ:

Обоснование:

Задание 4 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Какие методы защиты относятся к криптографии?

1. Хэширование
2. Межсетевой экран
3. Электронная подпись
4. Антивирус
5. Шифрование

Ответ:

Обоснование:

Задание 5 (ОК 05, ПК 1.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите принципы безопасного хранения паролей в базе данных.

Ответ:

Задание 6 (ОК 09, ПК 3.5). Установите соответствие между стандартами ИБ и их описанием (время: 5 мин):

Инструкция: Соотнесите стандарты ИБ (А – В) с их описаниями (1 – 4). В правом столбце есть один лишний вариант.

Стандарты ИБ		Описание	
А.	ISO 27001	1.	Российский стандарт на СМИБ
Б.	ГОСТ Р ИСО/МЭК 27001	2.	Международный стандарт менеджмента ИБ
В.	PCI DSS	3.	Стандарт безопасности данных индустрии платежных карт
		4.	Стандарт защиты персональных данных

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 7 (ОК 02, ПК 4.4). Установите последовательность реагирования на инцидент ИБ (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Обнаружение
2. Анализ
3. Сдерживание
4. Устранение
5. Восстановление

Ответ:

Задание 8 (ОК 03, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Какой принцип шифрования используется в AES?

1. Асимметричный
2. Симметричный
3. Хэширование
4. Квантовый

Ответ:

Обоснование:

Задание 9 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все уязвимости из OWASP Top 10.

1. SQLi
2. DDoS
3. XSS
4. Физический доступ
5. CSRF

Ответ:

Обоснование:

Задание 10 (ОК 05, ПК 3.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите этапы проведения аудита безопасности веб-приложения.

Ответ:

Задание 11 (ОК 02, ПК 4.4). Установите соответствие между инструментами и их назначением (время: 5 мин):

Инструкция: Соотнесите инструменты (А – В) с их назначением (1 – 4). В правом столбце есть один лишний вариант.

Инструмент		Назначение	
А.	Wireshark	1.	Статический анализ кода
Б.	Burp Suite	2.	Анализ сетевого трафика
В.	SonarQube	3.	Тестирование веб-приложений
		4.	Шифрование данных

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 12 (ОК 09, ПК 1.5). Установите последовательность действий при настройке межсетевого экрана (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Определение политик доступа
2. Анализ сетевой топологии
3. Настройка правил
4. Тестирование правил
5. Мониторинг и обновление

Ответ:

Задание 13 (ОК 01, ПК 3.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «социальная инженерия»?

1. Метод взлома через уязвимости в коде
2. Метод манипуляции людьми для получения информации
3. Метод шифрования данных
4. Метод тестирования сети

Ответ:

Обоснование:

Задание 14 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все меры защиты от XSS.

1. Валидация ввода
2. Использование HTTPS
3. Экранирование вывода
4. Хэширование паролей
5. Content Security Policy (CSP)

Ответ:

Обоснование:

Задание 15 (ОК 02, ПК 2.4). Открытый вопрос (написание кода, время: 12 мин).

Инструкция: Напишите на Python функцию, которая проверяет надежность пароля (минимум 8 символов, заглавные и строчные буквы, цифры).

Ответ:

Задание 16 (ОК 03, ПК 2.4). Установите соответствие между типами тестирования и их описанием (время: 5 мин):

Инструкция: Соотнесите типы тестирования (А – В) с их описаниями (1 – 4). В правом столбце есть один лишний вариант.

Тип тестирования		Описание	
А.	Статическое	1.	Тестирование без запуска программы
Б.	Динамическое	2.	Тестирование с запуском программы
В.	Пентест	3.	Тестирование на проникновение
		4.	Тестирование интерфейса

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 17 (ОК 09, ПК 3.5). Установите последовательность этапов пентеста (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Разведка
2. Сканирование
3. Получение доступа
4. Удержание доступа
5. Анализ следов

Ответ:

Задание 18 (ОК 01, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «электронная подпись»?

1. Шифрование файла
2. Криптографическое средство подтверждения авторства
3. Метод сжатия данных
4. Способ передачи файлов

Ответ:

Обоснование:

Задание 19 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все инструменты для динамического анализа кода.

1. SonarQube
2. Burp Suite
3. OWASP ZAP
4. Checkmarx
5. Wireshark

Ответ:

Обоснование:

Задание 20 (ОК 05, ПК 4.4). Открытый вопрос (анализ кода, время: 12 мин).

Инструкция: Найдите уязвимости в приведенном коде и предложите исправления:

php

```
$user = $_GET['user'];  
$query = "SELECT * FROM users WHERE name = '$user'";  
$result = mysqli_query($conn, $query);
```

Ответ:

2.2.Вариант 2

Задание 1 (ОК 02, ПК 1.5). Установите соответствие между элементами CIA-триады и их описаниями (время: 5 мин):

Инструкция: Соотнесите элементы CIA-триады (А – В) с их описаниями (1 – 5). В правом столбце есть один лишний вариант.

Элементы триады		Описание	
А.	Конфиденциальность	1.	Гарантия того, что информация не была изменена неуполномоченными лицами
Б.	Целостность	2.	Свойство информации быть доступной для авторизованных пользователей
В.	Доступность	3.	Защита от несанкционированного раскрытия
		4.	Способность системы противостоять DDoS-атакам

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 2 (ОК 03, ПК 3.5). Установите последовательность этапов моделирования угроз (Threat Modeling) (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Идентификация активов
2. Определение угроз
3. Оценка уязвимостей
4. Определение контрмер
5. Документирование результатов

Ответ:

Задание 3 (ОК 01, ПК 2.4). Выберите ОДИН правильный ответ и обоснуйте его (время: 7 мин).

Инструкция: Какой метод аутентификации является наиболее стойким на сегодняшний день?

1. Пароль из 6 цифр
2. Одноразовый SMS-код
3. Многофакторная аутентификация (MFA) с биометрией
4. Секретный вопрос

Ответ:

Обоснование:

Задание 4 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Какие из перечисленных мер относятся к защите от CSRF-атак?

1. Использование токенов CSRF
2. Проверка заголовка Origin/Referer
3. Шифрование трафика TLS
4. Валидация ввода на стороне сервера
5. Ограничение сессий по времени

Ответ:

Обоснование:

Задание 5 (ОК 05, ПК 1.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите разницу между симметричным и асимметричным шифрованием. Приведите примеры алгоритмов.

Ответ:

Задание 6 (ОК 09, ПК 3.5). Установите соответствие между видами вредоносного ПО и их описанием (время: 5 мин):

Инструкция: Соотнесите вредоносное ПО (А – В) с их описаниями (1 – 4). В правом столбце есть один лишний вариант.

Вредоносное ПО		Описание	
А.	Троян	1.	Саморазмножающаяся программа
Б.	Черви	2.	Программа, маскирующаяся под легитимную
В.	Кейлоггер	3.	Записывает нажатия клавиш
		4.	Блокирует доступ к системе за выкуп

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 7 (ОК 02, ПК 4.4). Установите последовательность настройки VPN-соединения (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Выбор протокола VPN (например, OpenVPN, IPSec)
2. Настройка сервера VPN
3. Генерация сертификатов/ключей
4. Настройка клиента VPN
5. Тестирование соединения

Ответ:

Задание 8 (ОК 03, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «солевание» (salting) в контексте хэширования паролей?

1. Добавление случайных данных к паролю перед хэшированием
2. Шифрование пароля симметричным алгоритмом
3. Использование нескольких хэш-функций
4. Хранение паролей в открытом виде

Ответ:

Обоснование:

Задание 9 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все инструменты для статического анализа безопасности кода (SAST)

1. SonarQube
2. Burp Suite
3. Checkmarx
4. OWASP ZAP
5. Fortify

Ответ:

Обоснование:

Задание 10 (ОК 05, ПК 3.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите, что такое OWASP Top 10. Перечислите три актуальные уязвимости из этого списка.

Ответ:

Задание 11 (ОК 02, ПК 4.4). Установите соответствие между сетевыми протоколами и уровнями модели OSI (время: 5 мин):

Инструкция: Соотнесите сетевые протоколы (А – В) с их уровнями OSI (1 – 4). В правом столбце есть один лишний вариант.

Протокол		Уровень OSI	
А.	HTTP	1.	Канальный (Data Link)
Б.	TCP	2.	Прикладной (Application)
В.	IP	3.	Транспортный (Transport)
		4.	Сетевой (Network)

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 12 (ОК 09, ПК 1.5). Установите последовательность действий при обнаружении утечки данных (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Изоляция затронутых систем
2. Оценка масштаба инцидента
3. Уведомление ответственных лиц
4. Сбор доказательств
5. Восстановление и отчетность

Ответ:

Задание 13 (ОК 01, ПК 3.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «фишинг»?

1. Вид DDoS-атаки
2. Кража данных через поддельные сайты/письма
3. Взлом через SQL-инъекцию
4. Перехват сетевого трафика

Ответ:

Обоснование:

Задание 14 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все меры защиты от SQL-инъекций.

1. Использование ORM
2. Подготовленные выражения (prepared statements)
3. Валидация ввода на клиенте
4. Хэширование паролей
5. Экранирование специальных символов

Ответ:

Обоснование:

Задание 15 (ОК 02, ПК 2.4). Открытый вопрос (написание кода, время: 12 мин).

Инструкция: Напишите на Python функцию для валидации email-адреса с использованием регулярных выражений

Ответ:

Задание 16 (ОК 03, ПК 2.4). Установите соответствие между типами тестирования безопасности и их целями (время: 5 мин):

Инструкция: Соотнесите типы тестирования безопасности (А – В) с их целями (1 – 4). В правом столбце есть один лишний вариант.

Тип тестирования		Цель	
А.	Пентест	1.	Поиск уязвимостей в коде без его запуска
Б.	SAST	2.	Имитация атаки злоумышленника
В.	DAST	3.	Тестирование работающего приложения
		4.	Анализ сетевого трафика

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 17 (ОК 09, ПК 3.5). Установите последовательность шагов при проведении аудита безопасности (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Планирование и подготовка
2. Сбор информации
3. Анализ уязвимостей
4. Документирование результатов
5. Предоставление рекомендаций

Ответ:

Задание 18 (ОК 01, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «мандатная модель доступа»?

1. Доступ на основе ролей (RBAC)
2. Доскональный контроль доступа субъектов к объектам
3. Доступ на основе списков (ACL)
4. Парольная защита

Ответ:

Обоснование:

Задание 19 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все признаки фишингового письма.

1. Ссылка на поддельный домен
2. Официальный логотип компании
3. Орфографические ошибки
4. Запрос конфиденциальных данных
5. Личное обращение по имени

Ответ:

Обоснование:

Задание 20 (ОК 05, ПК 4.4). Открытый вопрос (анализ кода, время: 12 мин).

Инструкция: Найдите уязвимость в коде и предложите исправление:

javascript

```
let userInput = document.location.hash.substring(1);  
document.getElementById("output").innerHTML = userInput;
```

Ответ:

Вариант 3

Задание 1 (ОК 02, ПК 1.5). Установите соответствие между терминами и их значениями (время: 5 мин):

Инструкция: Соотнесите термины (А – Г) с их значениями (1 – 5). В правом столбце есть один лишний вариант.

Термин		Значение	
А.	Аутентификация	1.	Определение прав доступа
Б.	Авторизация	2.	Шифрование данных
В.	Аудит	3.	Подтверждение личности
Г.	Шифрование	4.	Фиксация событий безопасности
		5.	Резервное копирование

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В	Г

Задание 2 (ОК 03, ПК 3.5). Установите последовательность этапов жизненного цикла разработки безопасного ПО (SDLC) (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Планирование требований
2. Проектирование с учетом безопасности
3. Разработка с безопасным кодом
4. Тестирование на безопасность
5. Внедрение и сопровождение

Ответ:

Задание 3 (ОК 01, ПК 2.4). Выберите ОДИН правильный ответ и обоснуйте его (время: 7 мин).

Инструкция: Какой протокол обеспечивает безопасную передачу данных в интернете?

1. HTTP
2. FTP
3. HTTPS
4. SMTP

Ответ:

Обоснование:

Задание 4 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все компоненты PKI (инфраструктуры открытых ключей)

1. Центр сертификации (СА)
2. Межсетевой экран
3. Репозиторий сертификатов
4. Антивирус
5. Служба отметок времени

Ответ:

Обоснование:

Задание 5 (ОК 05, ПК 1.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите, чем отличается IDS от IPS.

Ответ:

Задание 6 (ОК 09, ПК 3.5). Установите соответствие между типами атак и их описанием (время: 5 мин):

Инструкция: Соотнесите Тип атаки (А – В) с их описаниями (1 – 4). В правом столбце есть один лишний вариант.

Тип атаки		Описание	
А.	MITM	1.	Подмена доверенного ресурса
Б.	Spoofing	2.	Перехват и изменение трафика
В.	Replay	3.	Повторение перехваченных данных
		4.	Заполнение диска данными

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 7 (ОК 02, ПК 4.4). Установите последовательность настройки системы обнаружения вторжений (IDS) (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Определение защищаемых активов
2. Выбор типа IDS (сетевой/хостовой)
3. Настройка правил обнаружения
4. Размещение сенсоров
5. Тестирование и мониторинг

Ответ:

Задание 8 (ОК 03, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «неотказуемость» (non-repudiation) в информационной безопасности?

1. Невозможность отказаться от отправленного сообщения
2. Шифрование данных
3. Резервное копирование
4. Аудит действий

Ответ:

Обоснование:

Задание 9 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все меры защиты от инъекций в командную строку (OS Command Injection)

1. Использование whitelist для аргументов
2. Экранирование спецсимволов
3. Запуск от имени root
4. Использование параметризованных вызовов
5. Валидация ввода на стороне клиента

Ответ:

Обоснование:

Задание 10 (ОК 05, ПК 3.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите, что такое «принцип наименьших привилегий». Приведите пример.

Ответ:

Задание 11 (ОК 02, ПК 4.4). Установите соответствие между технологиями и их назначением в ИБ (время: 5 мин):

Инструкция: Соотнесите технологии (А – В) с их назначением (1 – 4). В правом столбце есть один лишний вариант.

Технология		Назначение	
А.	VPN	1.	Защита беспроводной сети
Б.	WPA3	2.	Создание зашифрованного туннеля
В.	SIEM	3.	Агрегация и анализ логов безопасности
		4.	Шифрование диска

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 12 (ОК 09, ПК 1.5). Установите последовательность обработки инцидента утечки данных (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Классификация инцидента
2. Эскалация ответственной команде
3. Сбор и сохранение доказательств
4. Ликвидация последствий
5. Составление отчета

Ответ:

Задание 13 (ОК 01, ПК 3.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «брутфорс-атака»?

1. Подбор пароля перебором вариантов
2. Фишинг через email
3. SQL-инъекция
4. XSS

Ответ:

Обоснование:

Задание 14 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все меры защиты от DDoS-атак.

1. Использование CDN
2. Настройка файрвола
3. Ограничение запросов с IP
4. Шифрование данных
5. Резервное копирование

Ответ:

Обоснование:

Задание 15 (ОК 02, ПК 2.4). Открытый вопрос (написание кода, время: 12 мин).

Инструкция: Напишите на Python функцию для безопасного сравнения хэшей (защита от timing-атак).

Ответ:

Задание 16 (ОК 03, ПК 2.4). Установите соответствие между стандартами и их областью применения (время: 5 мин):

Инструкция: Соотнесите стандарты (А – В) с их областями применения (1 – 4). В правом столбце есть один лишний вариант.

Стандарт		Область применения	
А.	PCI DSS	1.	Защита персональных данных в РФ
Б.	ФЗ-152	2.	Безопасность платежных карт
В.	HIPAA	3.	Защита медицинских данных (США)
		4.	Управление ИБ в организации

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 17 (ОК 09, ПК 3.5). Установите последовательность шагов при настройке контроля доступа на основе ролей (RBAC) (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Определение ролей в системе
2. Назначение прав ролям
3. Назначение ролей пользователям
4. Тестирование политик доступа
5. Аудит и пересмотр политик

Ответ:

Задание 18 (ОК 01, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «квантовая криптография»?

1. Шифрование с использованием квантовых компьютеров
2. Защита от квантовых атак
3. Использование квантовых явлений для защиты связи
4. Криптография для квантовых алгоритмов

Ответ:

Обоснование:

Задание 19 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все признаки компрометации системы.

1. Необычная сетевая активность
2. Незвестные процессы
3. Обновление антивируса
4. Изменение системных файлов
5. Успешный вход пользователя

Ответ:

Обоснование:

Задание 20 (ОК 05, ПК 4.4). Открытый вопрос (анализ кода, время: 12 мин).

Инструкция: Найдите уязвимость в коде и предложите исправление:

```
python
import os

filename = input("Введите имя файла: ")
os.system("cat " + filename)
```

Ответ:

2.3.Вариант 4

Задание 1 (ОК 02, ПК 1.5). Установите соответствие между типами ключей и их использованием (время: 5 мин):

Инструкция: Соотнесите типы ключей (А – В) с их использованием (1 – 5). В правом столбце есть один лишний вариант.

Тип ключа		Использование	
А.	Публичный	1.	Шифрование данных отправителем
Б.	Приватный	2.	Расшифрование данных получателем
В.	Сессионный	3.	Подписание документов
		4.	Временное шифрование сессии

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 2 (ОК 03, ПК 3.5). Установите последовательность этапов криптоанализа (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Сбор шифротекста
2. Анализ алгоритма шифрования
3. Поиск слабостей
4. Подбор ключа
5. Расшифрование

Ответ:

Задание 3 (ОК 01, ПК 2.4). Выберите ОДИН правильный ответ и обоснуйте его (время: 7 мин).

Инструкция: Какой протокол используется для безопасной передачи файлов?

1. HTTP
2. FTPS
3. Telnet
4. SNMP

Ответ:

Обоснование:

Задание 4 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все меры защиты от перехвата сессии (Session Hijacking)

1. Использование HTTPS
2. Регулярная смена session ID
3. Хранение session ID в cookie
4. Привязка сессии к IP-адресу
5. Использование HTTP-only cookies

Ответ:

Обоснование:

Задание 5 (ОК 05, ПК 1.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите, что такое «сертификат SSL/TLS» и для чего он используется.

Ответ:

Задание 6 (ОК 09, ПК 3.5). Установите соответствие между типами брандмауэров и их описанием (время: 5 мин):

Инструкция: Соотнесите Тип брандмауэра (А – В) с их описаниями (1 – 4). В правом столбце есть один лишний вариант.

Тип брандмауэра		Описание	
А.	Пакетный	1.	Анализ на уровне приложений
Б.	Stateful	2.	Фильтрация по адресам/портам
В.	Прикладной	3.	Отслеживание состояния соединений
		4.	Шифрование трафика

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 7 (ОК 02, ПК 4.4). Установите последовательность развертывания системы шифрования дисков (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Выбор алгоритма шифрования
2. Генерация ключей
3. Шифрование диска
4. Хранение ключей восстановления
5. Тестирование доступа

Ответ:

Задание 8 (ОК 03, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «стеганография»?

1. Шифрование данных
2. Соккрытие данных внутри других данных
3. Сжатие данных
4. Хэширование данных

Ответ:

Обоснование:

Задание 9 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все признаки АРТ-атаки (Advanced Persistent Threat)

1. Длительное присутствие в сети
2. Использование нулевых уязвимостей
3. Массовая рассылка спама
4. Целенаправленность на конкретную организацию
5. Яркие визуальные эффекты

Ответ:

Обоснование:

Задание 10 (ОК 05, ПК 3.5). Открытый вопрос (время: 10 мин).

Инструкция: Опишите, что такое «управление уязвимостями». Какие этапы оно включает?

Ответ:

Задание 11 (ОК 02, ПК 4.4). Установите соответствие между инструментами и типом анализа (время: 5 мин):

Инструкция: Соотнесите Инструмент (А – В) с типом анализа (1 – 5). В правом столбце есть один лишний вариант.

Инструмент		Тип анализа	
А.	Nessus	1.	Статический анализ кода
Б.	Veracode	2.	Сканирование уязвимостей сети
В.	Splunk	3.	Анализ логов безопасности
		4.	Тестирование на проникновение

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 12 (ОК 09, ПК 1.5). Установите последовательность внедрения системы двухфакторной аутентификации (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Выбор методов аутентификации
2. Настройка сервера аутентификации
3. Регистрация пользователей
4. Тестирование системы
5. Обучение пользователей

Ответ:

Задание 13 (ОК 01, ПК 3.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «логирование» в контексте ИБ?

1. Запись событий для последующего анализа
2. Шифрование данных
3. Резервное копирование
4. Аутентификация пользователей

Ответ:

Обоснование:

Задание 14 (ОК 04, ПК 4.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 8 мин).

Инструкция: Выберите все меры защиты от инсайдерских угроз.

1. Мониторинг действий сотрудников
2. Разделение обязанностей
3. Выдача всем полных прав доступа
4. Регулярные проверки сотрудников
5. Отключение логирования

Ответ:

Обоснование:

Задание 15 (ОК 02, ПК 2.4). Открытый вопрос (написание кода, время: 12 мин).

Инструкция: Напишите на Python функцию для безопасной загрузки файлов (проверка расширения, MIME-типа).

Ответ:

Задание 16 (ОК 03, ПК 2.4). Установите соответствие между видами тестирования и их описанием (время: 5 мин):

Инструкция: Соотнесите Вид тестирования (А – В) с их описанием (1 – 4). В правом столбце есть один лишний вариант.

Вид тестирования		Описание	
А.	Фаззинг	1.	Тестирование граничных значений
Б.	Регрессионное	2.	Ввод случайных данных для поиска сбоев
В.	Нагрузочное	3.	Проверка после изменений кода
		4.	Проверка производительности под нагрузкой

Ответ:

Запишите выбранные цифры под соответствующими буквами

А	Б	В

Задание 17 (ОК 09, ПК 3.5). Установите последовательность расследования инцидента ИБ (время: 6 мин):

Инструкция: Запишите последовательность цифр.

1. Идентификация инцидента
2. Сбор и сохранение улик
3. Анализ улик
4. Восстановление системы
5. Составление итогового отчета

Ответ:

Задание 18 (ОК 01, ПК 1.5). Выберите ОДИН правильный ответ и обоснуйте его (время: 4 мин).

Инструкция: Что такое «криптостойкость»?

1. Скорость шифрования
2. Устойчивость алгоритма к взлому
3. Размер ключа
4. Стоимость реализации

Ответ:

Обоснование:

Задание 19 (ОК 04, ПК 2.4). Выберите ВСЕ правильные ответы и обоснуйте их (время: 7 мин).

Инструкция: Выберите все элементы безопасной архитектуры сети.

1. Сегментация сети
2. Единая плоская сеть
3. DMZ (демитаризованная зона)
4. Использование default-паролей
5. Регулярное обновление сетевого ПО

Ответ:

Обоснование:

Задание 20 (ОК 05, ПК 4.4). Открытый вопрос (анализ кода, время: 12 мин).

Инструкция: Найдите уязвимость в коде и предложите исправление:

sql

```
SELECT * FROM users WHERE username = 'admin' AND password = '12345';
```

Ответ:

3. Ключи к оцениванию тестовых заданий

ВАРИАНТ 1

Задание 1.

Ответ:

А	Б	В	Г
2	3	4	5

Задание 2.

Ответ: 1-2-3-4-5

Задание 3.

Ответ: 3 (SYN-флуд).

Обоснование: SYN-флуд перегружает сервер запросами на установление соединения, исчерпывая его ресурсы, что приводит к отказу в обслуживании.

Задание 4.

Ответ: 1, 3, 5.

Обоснование: Хэширование, ЭП и шифрование — криптографические методы. Фаервол и антивирус — средства защиты иного типа.

Задание 5.

Ответ: Хранение хэшей с солью, использование стойких алгоритмов (bcrypt, Argon2), запрет хранения в открытом виде, регулярное обновление.

Задание 6.

Ответ:

А	Б	В
2	1	3

Задание 7.

Ответ: 1-2-3-4-5

Задание 8.

Ответ: 2 (симметричный)

Обоснование: AES — симметричный блочный шифр, использует один ключ для шифрования и расшифрования.

Задание 9.

Ответ: 1, 3, 5.

Обоснование: SQLi, XSS, CSRF входят в OWASP Top 10. DDoS и физический доступ — нет.

Задание 10.

Ответ: Планирование, сканирование, тестирование на проникновение, анализ результатов, отчет.

Задание 11.

Ответ:

А	Б	В
2	3	1

Задание 12.

Ответ: 2-1-3-4-5

Задание 13.

Ответ: 2

Обоснование: Социальная инженерия — это психологическое воздействие на людей с целью получения конфиденциальной информации.

Задание 14.

Ответ: 1, 3, 5.

Обоснование: Валидация, экранирование и CSP — основные меры против XSS. HTTPS и хэширование — другие методы защиты.

Задание 15.

Ответ:

```
import re

def check_password(password):
    if len(password) < 8:
        return False
    if not re.search(r'[A-Z]', password):
        return False
    if not re.search(r'[a-z]', password):
        return False
    if not re.search(r'[0-9]', password):
        return False
    return True
```

Задание 16.

Ответ:

А	Б	В
1	2	3

Задание 17.

Ответ: 1-2-3-4-5

Задание 18.

Ответ: 2.

Обоснование: ЭП обеспечивает целостность и аутентичность документа, подтверждая авторство.

Задание 19.

Ответ: 2, 3, 5.

Обоснование: Burp Suite, ZAP, Wireshark — инструменты динамического анализа. SonarQube и Checkmarx — статического.

Задание 20.

Эталон ответа: Уязвимость — SQL-инъекция.

Исправление: Использовать подготовленные выражения:

```
$stmt = $conn->prepare("SELECT * FROM users WHERE name = ?");  
$stmt->bind_param("s", $user);  
$stmt->execute();
```

ВАРИАНТ 2

Задание 1.

Ответ:

А	Б	В
3	1	2

Задание 2.

Ответ: 1-2-3-4-5

Задание 3.

Ответ: 3 (MFA с биометрией)

Обоснование: MFA с биометрией сочетает несколько факторов (знание, владение, свойство), что значительно усложняет компрометацию.

Задание 4.

Ответ: 1, 2, 5.

Обоснование: Токены CSRF, проверка Origin/Referer и ограничение сессий — прямые меры против CSRF. Шифрование и валидация ввода решают другие задачи.

Задание 5.

Ответ: Симметричное — один ключ для шифрования/расшифрования (AES, DES). Асимметричное — пара ключей (публичный/приватный) (RSA, ECC). Симметричное быстрее, асимметричное безопаснее для обмена ключами.

Задание 6.

Ответ:

А	Б	В
2	1	3

Задание 7.

Ответ: 1-2-3-4-5

Задание 8.

Ответ: 1

Обоснование: Соль — случайная строка, добавляемая к паролю перед хэшированием для защиты от rainbow-таблиц.

Задание 9.

Ответ: 1, 3, 5.

Обоснование: SonarQube, Checkmarx, Fortify — инструменты SAST. Burp Suite и ZAP — инструменты динамического анализа (DAST).

Задание 10.

Ответ: OWASP Top 10 — список наиболее критичных угроз безопасности веб-приложений. Примеры: Инъекции, небезопасная аутентификация, Уязвимые компоненты.

Задание 11.

Ответ:

А	Б	В
2	3	4

Задание 12.

Ответ: 2-1-3-4-5

Задание 13.

Ответ: 2

Обоснование: Фишинг — социальная инженерия, цель — выманивание конфиденциальных данных через поддельные ресурсы.

Задание 14.

Ответ: 1, 2, 5.

Обоснование: ORM, prepared statements, экранирование — прямые меры. Валидация на клиенте ненадежна, хэширование паролей — другая защита.

Задание 15.

Ответ:

```
python
import re

def validate_email(email):
    pattern = r'^[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,}$'
    return bool(re.match(pattern, email))
```

Задание 16.

Ответ:

А	Б	В
2	1	3

Задание 17.

Ответ: 1-2-3-4-5

Задание 18.

Ответ: 2.

Обоснование: Мандатная модель — доступ определяется правилами безопасности (метки конфиденциальности), а не волей пользователя.

Задание 19.

Ответ: 1, 3, 4.

Обоснование: Поддельный домен, ошибки, запрос данных — признаки фишинга. Логотип и личное обращение могут быть и в легитимных письмах.

Задание 20.

Эталон ответа: Уязвимость — XSS через innerHTML.

Исправление: Использовать textContent или санитизацию:

```
javascript
document.getElementById("output").textContent = userInput;
```

ВАРИАНТ 3

Задание 1.

Ответ:

А	Б	В	Г
3	1	4	2

Задание 2.

Ответ: 1-2-3-4-5

Задание 3.

Ответ: 3 (HTTPS).

Обоснование: HTTPS — это HTTP поверх TLS/SSL, обеспечивает шифрование и аутентификацию.

Задание 4.

Ответ: 1, 3, 5.

Обоснование: СА, репозиторий сертификатов, служба отметок времени — части PKI. Фаервол и антивирус — нет.

Задание 5.

Ответ: IDS (система обнаружения вторжений) только обнаруживает атаки и оповещает. IPS (система предотвращения вторжений) также блокирует подозрительную активность.

Задание 6.

Ответ:

А	Б	В
2	1	3

Задание 7.

Ответ: 1-2-3-4-5

Задание 8.

Ответ: 1

Обоснование: Неотказуемость гарантирует, что отправитель не сможет отрицать факт отправки сообщения (обеспечивается ЭЦП).

Задание 9.

Ответ: 1, 2, 4.

Обоснование: Whitelist, экранирование, параметризованные вызовы — меры защиты. Запуск от root опасен, валидация на клиенте ненадежна.

Задание 10.

Ответ: Пользователь/процесс должен иметь минимальные права, необходимые для работы. Пример: веб-сервер не должен работать от имени root.

Задание 11.

Ответ:

А	Б	В
2	1	3

Задание 12.

Ответ: 1-2-3-4-5

Задание 13.

Ответ: 1

Обоснование: Брутфорс — автоматизированный перебор паролей/ключей.

Задание 14.

Ответ: 1, 2, 3.

Обоснование: CDN, фаервол, ограничение запросов — меры против DDoS. Шифрование и бэкапы — другие меры.

Задание 15.

Ответ:

```
python
import hmac

def compare_hashes(hash1, hash2):
    return hmac.compare_digest(hash1, hash2)
```

Задание 16.

Ответ:

А	Б	В
2	1	3

Задание 17.

Ответ: 1-2-3-4-5

Задание 18.

Ответ: 3.

Обоснование: Квантовая криптография использует квантовые эффекты (например, запутанность) для безопасного распределения ключей.

Задание 19.

Ответ: 1, 2, 4.

Обоснование: Необычная активность, неизвестные процессы, изменение файлов — признаки атаки. Обновление антивируса и успешный вход — норма.

Задание 20.

Эталон ответа: Уязвимость — инъекция команд.

Исправление: Использовать subprocess с параметризацией:

```
python
import subprocess
subprocess.run(["cat", filename])
```

ВАРИАНТ 4

Задание 1.

Ответ:

А	Б	В
1	2	4

Задание 2.

Ответ: 1-2-3-4-5

Задание 3.

Ответ: 2 (FTPS)

Обоснование: FTPS — FTP поверх SSL/TLS, обеспечивает шифрование. Остальные небезопасны или для других целей.

Задание 4.

Ответ: 1, 2, 4, 5.

Обоснование: HTTPS, смена ID, привязка к IP, HTTP-only cookies защищают от перехвата. Хранение в cookie — стандартная практика, но не защита.

Задание 5.

Ответ: Сертификат — цифровой документ, подтверждающий принадлежность публичного ключа владельцу. Используется для аутентификации сервера и шифрования связи.

Задание 6.

Ответ:

А	Б	В
2	3	1

Задание 7.

Ответ: 1-2-3-4-5

Задание 8.

Ответ: 2

Обоснование: Стеганография — скрытие факта передачи информации (например, в изображении).

Задание 9.

Ответ: 1, 2, 4.

Обоснование: Длительность, использование 0-day, целенаправленность — признаки АРТ. Спам и визуальные эффекты — нет.

Задание 10.

Ответ: Процесс выявления, оценки, обработки уязвимостей. Этапы: обнаружение, оценка критичности, устранение/снижение риска, переоценка.

Задание 11.

Ответ:

А	Б	В
2	1	3

Задание 12.

Ответ: 1-2-3-4-5

Задание 13.

Ответ: 1

Обоснование: Логирование — фиксация событий для аудита, расследования инцидентов.

Задание 14.

Ответ: 1, 2, 4.

Обоснование: Мониторинг, разделение обязанностей, проверки — меры против инсайдеров. Полные права и отключение логирования увеличивают риски.

Задание 15.

Ответ:

```
python
import mimetypes
import os

ALLOWED_EXTENSIONS = {'.txt', '.pdf', '.png'}
ALLOWED_MIMES = {'text/plain', 'application/pdf', 'image/png'}

def safe_upload(filename, file_content):
    ext = os.path.splitext(filename)[1].lower()
    if ext not in ALLOWED_EXTENSIONS:
        return False
    mime = mimetypes.guess_type(filename)[0]
    if mime not in ALLOWED_MIMES:
        return False
    # Дальнейшая обработка
    return True
```

Задание 16.

Ответ:

А	Б	В
2	3	4

Задание 17.

Ответ: 1-2-3-4-5

Задание 18.

Ответ: 2.

Обоснование: Криптостойкость — способность противостоять криптоанализу.

Задание 19.

Ответ: 1, 3, 5

Обоснование: Сегментация, DMZ, обновления — элементы безопасной архитектуры. Плоская сеть и default-пароли — уязвимости.

Задание 20.

Эталон ответа: Уязвимость — хранение пароля в открытом виде, отсутствие хэширования.

Исправление: Хранить хэш пароля с солью, проверять хэш:

sql

```
SELECT * FROM users WHERE username = 'admin' AND password_hash = ?;
```