Оценочные материалы для промежуточной аттестации по дисциплине

Название дисциплины “ Разработка и эксплуатация защищенных информационных систем ”, 7 семестр

Код, направление подготовки	09.03.02 «Информационные системы и технологии»
Направленность (профиль)	Безопасность информационных систем и технологий
Форма обучения	Очная
Кафедра-разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые задания для контрольной работы (7 семестр):

Задание 1. Теоретический вопрос
Раскройте сущность модели угроз для информационной системы. Укажите:

- цели и задачи разработки модели угроз;
- основные этапы построения модели по методике ФСТЭК;
- примеры контрмер для нейтрализации 3–5 типовых угроз.
-

Задание 2. Практическое задание: криптографическое проектирование
Ситуация: Необходимо организовать защищённый обмен документами между двумя филиалами организации.
Задание: Разработайте схему криптографической защиты, включающую:

1. Выбор алгоритмов шифрования и ЭП (с обоснованием выбора ГОСТ/международные стандарты);
2. Архитектуру управления ключами (генерация, хранение, распределение, ротация);
3. Протокол аутентификации сторон и обмена ключами;
4. Меры защиты от компрометации ключей и атак типа MitM.

Задание 3. Аналитическая задача: оценка рисков
Исходные данные:

Актив	Стоимость (у.е.)	Частота угрозы (раз/год)	Коэффициент уязвимости
Сервер БД	400 000	0.4	0.35
Веб-шлюз	150 000	1.5	0.5
Канал связи	80 000	0.8	0.45

Задание:

1. Рассчитайте годовой уровень риска (ALE) для каждого актива: ALE = Стоимость × Частота × Коэффициент уязвимости;
2. Предложите по 1–2 меры снижения риска для каждого актива;
3. Оцените экономическую целесообразность предложенных мер.

Задание 4. Теоретический вопрос (20 баллов)
Опишите принципы безопасной разработки ПО (Secure SDLC). Раскройте:

- отличия от традиционного жизненного цикла разработки;
- инструменты и практики для каждого этапа (требования, дизайн, кодирование, тестирование);
- роль автоматизированных проверок безопасности в CI/CD-конвейере.

Задание 5. Практическое задание: архитектура безопасности (40 баллов)

Ситуация: Организация разрабатывает веб-приложение для обработки персональных данных пользователей.
Задание: Разработайте фрагмент архитектуры безопасности, включающий:
1. Схему сетевой сегментации (DMZ, внутренний контур, зона БД);
2. Механизмы аутентификации и разграничения прав доступа (роли, политики);
3. Меры защиты данных «на отдыхе» (шифрование БД) и «в движении» (TLS);
4. Компоненты логирования и мониторинга событий безопасности.

Задание 6. Кейс-стади: реагирование на инцидент (40 баллов)
Сценарий: В логах веб-приложения зафиксированы множественные попытки подбора учётных данных с последующей аномальной активностью (массовая выгрузка данных).
Задание:
1. Составьте алгоритм первичного реагирования (первые 2 часа);
2. Определите необходимые источники данных для расследования (логи, артефакты, метаданные);
3. Предложите меры по локализации инцидента и предотвращению повторения;
4. Сформулируйте требования к отчётности для руководства.

Задание 7. Теоретический вопрос (20 баллов)
Раскройте особенности обеспечения безопасности в облачных средах (IaaS/PaaS/SaaS).
Укажите:
- модель разделения ответственности между провайдером и клиентом;
- типовые угрозы для каждого типа сервиса;
- методы защиты конфигураций, данных и управления доступом в облаке.

Задание 8. Практическое задание: политики безопасности (40 баллов)
Ситуация: В организации внедряется система электронного документооборота (СЭД) с обработкой персональных данных.
Задание: Разработайте фрагмент политики безопасности, регламентирующий:
1. Требования к аутентификации и разграничению прав (роли: администратор, оператор, аудитор, пользователь);
2. Правила обработки, хранения и передачи ПДн;
3. Процедуры резервного копирования и восстановления;
4. Требования к логированию и аудиту действий пользователей.

Задание 9. Аналитическая задача: сравнительный анализ (40 баллов)
Задание: Сравните модели разграничения доступа: дискреционную (DAC), мандатную (MAC), ролевую (RBAC) и атрибутивную (ABAC).
Критерии сравнения:
- гибкость настройки политик;
- масштабируемость;
- сложность администрирования;
- применимость в государственных/коммерческих ИС.

Типовые вопросы к зачету (7-ой семестр)

1. Дайте определение «безопасность информации». Какие три базовых свойства она обеспечивает?
2. В чём разница между симметричным и асимметричным шифрованием? Приведите примеры алгоритмов.
3. Что такое хеш-функция? Назовите требования к криптографически стойким хеш-функциям.
4. Дайте определение понятию «аутентификация». Чем она отличается от авторизации?
5. Что такое электронная цифровая подпись (ЭЦП)? Какие задачи она решает?
6. Что понимается под «стеганографией»? В чём её отличие от криптографии?
7. Назовите основные этапы жизненного цикла криптографического ключа.
8. Что такое модель угроз и модель нарушителя? Для чего они используются?
9. Перечислите основные категории угроз информационной безопасности по источнику

возникновения.

10. Что такое криптоанализ? В чём его отличие от криптографии?
11. Что является основой большинства современных блочных симметричных алгоритмов шифрования?
12. Укажите размер блока шифрования в алгоритме «Магма» (ГОСТ 34.12-2018).
13. Назовите асимметричный алгоритм шифрования из списка: AES, RSA, DES, Blowfish.
14. Какие способы распределения ключей в вычислительной сети вы знаете?
15. Что такое протокол Диффи-Хеллмана? Для чего он применяется?
16. Какие виды вредоносного программного обеспечения вы знаете? Дайте определение «вирусу» и «червю».
17. Что такое межсетевой экран (firewall)? Какие функции он выполняет?
18. В чём разница между системами IDS и IPS?
19. Что такое PKI (инфраструктура открытых ключей)? Какие компоненты в неё входят?
20. Какие основные угрозы нарушают доступность информации? Приведите примеры.
21. Почему сотрудники считаются наиболее рискованной категорией с точки зрения внутренней угрозы?
22. Что такое политика безопасности организации? Какие уровни детализации она включает?
23. Какие меры защиты применяются против атак типа «человек посередине» (MitM)?
24. Что такое резервное копирование? Опишите стратегию «3-2-1».
25. Какие нормативные документы РФ регулируют вопросы защиты персональных данных?