Оценочные материалы для промежуточной аттестации по дисциплине

Методы защиты, 7 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые задания для контрольной работы:

Примерные вопросы для контрольной работы:

1. Дайте определение понятию «информационная безопасность». Назовите три базовых свойства информации, обеспечиваемых защитой.
2. В чём различие между угрозами, уязвимостями и атаками в контексте ИБ? Приведите примеры.
3. Классифицируйте угрозы информационной безопасности по источнику возникновения и способу реализации.
4. Что понимается под «несанкционированным доступом» (НСД)? Перечислите основные каналы утечки информации.
5. Охарактеризуйте модель нарушителя безопасности информационной системы. Какие категории нарушителей вы знаете?
6. Назовите основные нормативно-правовые акты РФ, регулирующие вопросы защиты информации.
7. В чём суть политики безопасности организации? Какие уровни детализации она включает?
8. Какие организационные меры применяются для защиты информации от внутренних угроз?
9. Опишите порядок разграничения прав доступа к информационным ресурсам в организации.
10. Какие требования предъявляются к обработке персональных данных в соответствии с 152-ФЗ?
11. В чём принципиальное различие между симметричными и асимметричными криптосистемами? Приведите примеры алгоритмов.
12. Опишите принцип работы электронной цифровой подписи (ЭЦП). Какие задачи она решает?
13. Что такое хеш-функция? Назовите требования к криптографически стойким хеш-функциям.
14. Объясните суть протокола обмена ключами Диффи-Хеллмана. В чём его уязвимость?

15. Какие режимы использования блочных шифров вы знаете? В чём преимущества и недостатки режима CBC?
16. Какие функции выполняет межсетевой экран (firewall)? Опишите различия между пакетными фильтрами и stateful-инспекцией.
17. Что такое система обнаружения вторжений (IDS)? В чём разница между сигнатурным и аномальным детектированием?
18. Опишите механизмы аутентификации пользователей: парольные, одноразовые коды, биометрические методы.
19. Какие меры защиты применяются против вредоносного ПО (вирусов, троянов, шпионских программ)?
20. Что такое виртуальная частная сеть (VPN)? Какие протоколы туннелирования вы знаете?
21. Какие уязвимости характерны для веб-приложений? Опишите методы защиты от SQL-инъекций и XSS-атак.
22. Что такое модель безопасности Белла-ЛаПадулы? В каких системах она применяется?
23. Опишите принципы построения защищённой архитектуры корпоративной сети (DMZ, сегментация, Zero Trust).
24. Какие методы резервного копирования и восстановления данных вы знаете? В чём разница между полным, инкрементальным и дифференциальным бэкапом?
25. Как обеспечивается безопасность при удалённом доступе к корпоративным ресурсам?

***Типовые вопросы к зачету*:**

1. Раскройте сущность триады информационной безопасности (конфиденциальность, целостность, доступность). Приведите примеры нарушений каждого из свойств в реальных информационных системах.
2. Дайте классификацию угроз информационной безопасности по различным основаниям: источник, способ реализации, объект воздействия.
3. Опишите жизненный цикл управления информационной безопасностью (ISO/IEC 27001). Какова роль каждого этапа в обеспечении защиты?
4. Что такое модель угроз и модель нарушителя? В какой последовательности они разрабатываются и как используются при проектировании системы защиты?
5. Раскройте понятие «риск информационной безопасности». Опишите качественные и количественные методы оценки рисков.
6. Охарактеризуйте систему нормативно-правового обеспечения информационной безопасности в РФ. Какова иерархия документов и сфера применения каждого уровня?
7. В чём особенности регулирования защиты персональных данных (152-ФЗ)? Опишите обязанности оператора ПДн и права субъекта ПДн.
8. Раскройте требования к защите информации в государственных информационных системах (ГИС). Что такое уровни защищённости и как они определяются?
9. Каковы основные положения Доктрины информационной безопасности РФ? Как они влияют на практику защиты информации в организациях?
10. Опишите порядок проведения аттестации объектов информатизации. Какие документы оформляются по результатам?
11. Сравните симметричные и асимметричные криптосистемы по критериям: скорость, управление ключами, стойкость, области применения.

12. Опишите архитектуру инфраструктуры открытых ключей (PKI). Каковы функции центра сертификации, регистрационного центра и хранилища сертификатов?
13. Раскройте механизм формирования и проверки электронной подписи. В чём разница между простой, неквалифицированной и квалифицированной ЭП?
14. Опишите принципы построения и применения протоколов аутентификации: Kerberos, OAuth 2.0, OpenID Connect.
15. Какие криптографические методы обеспечивают целостность данных? Сравните коды аутентичности сообщений (MAC) и хеш-функции.
16. Опишите архитектуру и принципы работы межсетевых экранов нового поколения (NGFW). Какие дополнительные функции они предоставляют по сравнению с традиционными firewall?
17. Сравните системы обнаружения (IDS) и предотвращения (IPS) вторжений. В каких сценариях целесообразно применение каждого типа систем?
18. Раскройте механизмы защиты от вредоносного программного обеспечения: сигнатурный анализ, эвристическое детектирование, песочницы, поведенческий анализ.
19. Опишите методы защиты от утечек информации (DLP-системы). Какие каналы утечек они контролируют и какие технологии анализа контента используют?
20. Каковы особенности защиты виртуализированных сред и облачных инфраструктур? Какие модели ответственности за безопасность существуют в облачных сервисах (IaaS, PaaS, SaaS)?
21. Опишите основные уязвимости веб-приложений согласно классификации OWASP Top 10. Предложите методы защиты для каждой из топ-5 уязвимостей.
22. Раскройте принципы безопасной разработки программного обеспечения (Secure SDLC). На каких этапах жизненного цикла ПО внедряются меры безопасности?
23. Опишите механизмы защиты беспроводных сетей: WPA2/WPA3, аутентификация через RADIUS, изоляция клиентов.
24. Какие методы применяются для защиты от сетевых атак: DoS/DDoS, ARP-spoofing, DNS-spoofing, MITM?
25. Раскройте принципы построения защищённой сетевой архитектуры: сегментация, демилитаризованная зона (DMZ), микросегментация, Zero Trust.
26. Опишите жизненный цикл управления инцидентами информационной безопасности (NIST SP 800-61). Какова роль SOC и CSIRT в этом процессе?
27. Раскройте понятие «план обеспечения непрерывности бизнеса» (BCP) и «план аварийного восстановления» (DRP). В чём их различия и взаимосвязь?
28. Какие методы резервного копирования обеспечивают защиту от программ-вымогателей? Опишите стратегию «3-2-1» и её модификации.
29. Опишите порядок проведения учений по реагированию на инциденты (tabletop exercises, red team/blue team). Каковы критерии эффективности таких учений?
30. Как осуществляется мониторинг и аудит событий безопасности? Опишите роль SIEM-систем и требования к хранению логов.