Вопросы к государственному экзамену (обновлено 2026 г.)

Магистерская программа «Кибербезопасность»

1. Хеш-функции. Формальное определение хеш-функции. Понятие Хеш-функции стойкой к поиску коллизий. Другие подходы к определению стойкости. Доказательство, что стойкость к поиску коллизий является более сильной, чем другие подходы. Преобразование Меркля-Дамгарда и его стойкость.

2. Аутентифицированное шифрование. Неподделываемое шифрование. Конструкция Enc-than-Mac. Теорема о стойкости этой конструкции.

3. CPA-стойкость криптосистемы с открытым ключом. Ограничение CPA-стойкости. CPA-стойкость криптосистемы Эль-Гамаля в предположениях сложности распознавательной задачи Диффи–Хеллмана.

4. Схемы электронной цифровой подписи. Формальное определение. Схема подписи для сообщений фиксированной длины. Эксперимент подделки подписи. Понятие схемы подписи стойкой к экзистенциальной подделке. Подход к построению схем подписи Hash-and-Sign. Обоснование его стойкости.

5. Цифровая подпись RSA. Формальное определение. Проблема RSA. Проблема RSA: формализация вычислительной трудности. Стойкость схемы подписи RSA.

6. Принципы безопасности операционной системы: Зальтцер и Шредер, ГОСТ Р ИСО/МЭК 15408-1-2008. Модели безопасности операционной системы: модель Белла-Лападулы, модель Биба. Политика безопасности: дискреционная, мандатная, ролевая, изолированной программной среды, безопасности информационных потоков.

7. Безопасность операционной системы Linux. Модель пользователя. Модели доступа: дискреционная, списки контроля доступа, расширенные атрибуты безопасности. Мандатное управление доступом Astra Linux, SELinux, Apparmor. Примеры атак на системы Linux.

8. Безопасность операционной системы Windows. Модель управления доступом: маркеры доступа, дескрипторы безопасности, списки управления доступом. Модель пользователя: ролевая модель, объекты, привилегии. Active Directory: служба каталогов, защита на уровне службы каталогов, доменные объекты групповая политика. Примеры атак на системы Windows.

9. Интернет вещей. Архитектура IoT. Международные и отечественные стандарты IoT. Основные понятия: M2M, IIoT, CPS. Присоединенные системы. Протоколы прикладного уровня в системах Интернета вещей MQTT, AMQP и CoAP

10. Кибербезопасность Интернета вещей. Угрозы и атаки для систем IoT, NIST Cybersecurity framework, Zero Trust модель, модель безопасности ETSI EN 303 645, ioXt альянс. Киберфизические системы.

11. Архитектура Blockchain. Схема хранения, P2P обмен данными. Децентрализованный реестр. Механизмы консенсуса. Согласование данных и хешфункции. и атаки на блокчейн. Риски безопасности в блокчейн. Аутентификация и авторизация в блокчейн. Безопасность алгоритмов консенсуса блокчейна. Атаки на блокчейн. Атаки на смарт-контракты. Аудит, OWASP

12. Принципы работы протокола Wi-Fi. Атаки на протокол W-Fi и механизмы безопасности Wi-Fi.

13. Назначение и принципы работы протоколов ARP, DHCP, NDP, DHCPv6. Атаки на эти протоколы и методы защиты от этих атак.

14. Основные типы межсетевых экранов: пакетные фильтры, межсетевые экраны прикладного уровня, межсетевые экраны следующего поколения (NGFW), прокси-шлюзы прикладного уровня, унифицированное управление угрозами (UTM), трансляция сетевых адресов (NAT). Топологии сети при использовании межсетевых экранов.

15. Инфраструктура открытого ключа (PKI). Уязвимости открытых ключей. Сертификаты X.509 v3. Основные компоненты PKI. Репозиторий сертификатов. Способы отмены сертификатов.

16. Основные уязвимости в веб-приложениях. Уязвимость SQL-внедрений и способы ее предотвращения. Уязвимость межсайтового выполнения сценариев (Cross-site Scripting – XSS) и способы ее предотвращения. Уязвимость межсайтовой подделки запросов (Cross Site Request Forgery – CSRF) и способы ее предотвращения.

17. Сегментация компьютерных сетей: назначение и основные подходы. Корпоративные сети: требования и основные механизмы безопасности. Сети ЦОД: архитектурные решения, требования и механизмы безопасности. Программно-определяемые сети в ЦОД.

18. Защита передаваемой информации на транспортном уровне. Протокол TLS: внутренняя архитектура, основные принципы работы, сценарии установления защищенного соединения. Использование криптографических алгоритмов и сертификатов открытых ключей в TLS. Режим шифрования AEAD и его варианты. Использование элементов протокола TLS в протоколах 802.1X и MACSec, NTP/NTS, QUIC.

19. Атаки и механизмы безопасности канального уровня. Атаки MAC-spoofing, MAC-flooding. Механизмы Port Security, ACL, 802.1X, MACSec, Storm Control. Назначение протокола STP. Атаки на STP и защита STP. Назначение VLAN. Типы VLAN. Атаки на VLAN и способы противодействия им.

20. Атаки DoS и DDoS. Понятия и примеры. Подходы к защите от атак DDoS. Варианты развертывания защиты от атак DDoS.

21. Система электронной почты и ее безопасность. Назначение основных протоколов электронной почты (SMTP, POP3, IMAP4). Защита трафика почтовых протоколов. Защита сообщений электронной почты end-to-end, системы S/MIME и PGP (OpenPGP). Защита от вредоносных и нежелательных почтовых сообщений: обзор подходов; механизмы greylist, DNSBL, SPF, DKIM, DMARC.

22. Понятие атаки на модель машинного обучения. Классификация атак. Атлас MITRE. Способы защиты от атак на модели машинного обучения.

23. Атаки отравления данных и атаки отравления моделей. Способы защиты от отравления данных и атак отравления моделей на модели.

24. Классификация уязвимостей типа Cross-site Scripting. Предотвращение уязвимостей типа Cross-site Scripting.

25. Уязвимость межсайтовой подделки запросов (Cross Site Request Forgery – CSRF) и способы ее предотвращения.

26. SQL Injection: Последовательность действий при выполнении, способы предотвращения и способы обхода проверок наличия SQL Injection.

27. Технологии хранения больших данных. Сетевые файловые системы. Распределенные файловые системы. Распределенная файловая система HDFS.

28. Распределенные базы данных. Распределенные реляционные базы данных. Базы данных ключ-значение, графовые, документоориентированные, основанные на семействах столбцов.

29. Вычислительные модели для больших данных. Парадигма распределенных вычислений MapReduce. Технология Spark.

30. Информационная безопасность больших данных. Модель нарушителя, модель рисков и угроз. Протокол сетевой аутентификации Kerberos. Информационная безопасность в Hadoop.

31. Исследовательский анализ данных. Очистка данных. Интеграция данных из разных источников. Трансформация данных.

32. Этапы процесса обучения моделей. Переобучение и недообучение. Обучение с учителем и без учителя: основные особенности, примеры.

33. Классификация: определение и применения. Выбор признаков для классификации. Логистическая регрессия. Деревья решений.

34. Кластеризация: определение и применения. Выбор признаков для кластеризации. Алгоритм кластеризации k-Means. Алгоритм иерархической кластеризации.

35. Искусственные нейронные сети. Многослойный перцептрон. Рекуррентные нейронные сети. Трансформеры.

36. Модели жизненного цикла программного обеспечения, их классификация и особенности применения. Модель жизненного цикла на основе инкрементальной сборки (Incrementalbuild). Прототипирование в разработке программного обеспечения (ПО). Спиральные модели жизненного цикла ПО, спиральная модель Барри Боэма, ее достоинства и недостатки. Модель спирали возрастающих обязательств.

37. Гибкие технологии (Agile) разработки ПО. Agile-манифест разработки ПО. Agile-практики и принципы. Участники Agile проектов и их функции, групповая поведенческая динамика. Эволюционный последовательный процесс Скрам (Scrum). Архитектурные

гибкие методы (Architected Agile Methods). Принципы бережливого производства и разработки ПО.

38. Стандартные процессы жизненного цикла систем (стандарт ISO/IEC/IEEE 15288), цель стандарта, основные концепции, процессный подход, эталонная модель процесса, классификация процессов жизненного цикла и их назначение. Состав процессов высокого уровня и их назначение. Процессы соглашения и их функции, реализация взаимодействий организаций с помощью процессов соглашения. Процессы организационного обеспечения проекта и их функции. Процессы технического управления и их функции. Технические процессы и их функции.

39. Основные понятия и процесс менеджмента риска информационной безопасности. (ISO/IEC 27005). Критерии оценки рисков, критерии принятия рисков. Методы качественной оценки вероятности и воздействия рисков: SWOT-анализ, экспертные опросы, мозговые штурмы. Методы количественной оценки рисков: ALE (Annual Loss Expectancy), SLE (Single Loss Expectancy), ROI (Return on Investment).

40. Методики проведения аудита кибербезопасности и инструменты выявления и анализа уязвимостей в рамках аудита.