Перечень вопросов для подготовки к экзамену по учебной дисциплине:

«СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. Часть 2»

1. Асимметричные криптосистемы: особенности построения и информационная безопасность.
2. Однонаправленные функции шифрования на основе дискретного логарифмирования и факторизации больших чисел. Необратимые функции с «потайным ходом». Однонаправленные хэш-функции на основе симметричных алгоритмов шифрования блочного типа.
3. Схемы применения однонаправленных функций шифрования для контроля целостности данных.
4. Алгоритм RSA: структурная схема криптосистемы, этапы реализации, быстродействие и уровень информационной безопасности.
5. Атаки на криптосистемы RSA.
6. Алгоритм Рабина: структурная схема криптосистемы, этапы реализации, быстродействие и уровень информационной безопасности.
7. Алгоритм Полига-Хеллмана: структурная схема криптосистемы, этапы реализации, быстродействие и уровень информационной безопасности.
8. Алгоритм Эль-Гамаля: структурная схема криптосистемы, этапы реализации, быстродействие и уровень информационной безопасности.
9. Сопоставительный анализ асимметричных и симметричных криптосистем.
10. Оценка информационной безопасности алгоритмов RSA, Рабина, Полига-Хеллмана и Эль-Гамаля.
11. Типовые схемы идентификации и аутентификации пользователей. Применение пароля для аутентификации пользователей. Схема простой аутентификации. Схема аутентификации с использованием идентификационной таблицы.
12. Аутентификация автора документа и самого документа с помощью электронной цифровой подписи.
13. Формирование электронной цифровой подписи.
14. Обеспечение конфиденциальности документа с электронной цифровой подписью.
15. Алгоритм электронной цифровой подписи RSA.
16. Алгоритм электронной цифровой подписи Эль-Гамаля.
17. Алгоритм электронной цифровой подписи DSA.
18. Взаимная проверка подлинности пользователей. Схема процедуры рукопожатия.
19. Взаимная проверка подлинности пользователей. Схема непрерывной проверки подлинности отправителя.
20. Упрощенный протокол идентификации с нулевой передачей знаний Фейге-Фиата-Шамира.
21. Протокол параллельной идентификации с нулевой передачей знаний.
22. Модифицированный протокол параллельной идентификации с нулевой передачей знаний.
23. Протокол идентификации с нулевой передачей знаний Гиллоу-Куискуотера.
24. Аутентификация пользователей с использованием многоразового пароля в протоколе CHAP.
25. Генерация ключей.
26. Хранение ключей.
27. Концепция иерархии ключей.
28. Расчет основных параметров алгоритмов RSA, Рабина, Полига-Хеллмана и Эль-Гамаля при зашифровании данных и расшифровании шифртекстов: вычисление ключей, шифртекстов и сообщений.
29. Расчет основных параметров алгоритмов электронных цифровых подписей RSA, Эль-Гамаля и DSA: вычисление ключей, цифровых подписей и уравнений верификации.
30. Расчет основных параметров протоколов идентификации с нулевой передачей знаний Фейге-Фиата-Шамира, параллельной идентификации и Гиллоу-Куискуотера: вычисление секретных ключей.