**На 3:**

"1) Концепция информационной безопасности.

2) Виды и формы представления информации. Информация как объект защиты.

3) Определение и цели, механизмы, инструментарий, концепция информационной

безопасности.

4) Угрозы информационной безопасности автоматизированных систем. Классификация

угроз ИБ.

5) Программные закладки и компьютерные вирусы. Методы и средства борьбы с

компьютерными вирусами.

6) Средства защиты информации. Технические средства защиты информационных

ресурсов.

7) Организационное обеспечение системы защиты информации.

8) Технологические основы обработки конфиденциальных документов.

9) Нормативно-правовое обеспечение информационной безопасности.

10) Угрозы информационной безопасности и их место в национальной безопасности

страны.

11) Основные нормативные руководящие документы, касающиеся государственной тайны,

нормативно-справочные документы.

12) Международные и отечественные стандарты информационной безопасности.

13) Модели безопасности: типовые модели нападения.

14) Классификация атак. Атаки на поток данных.

15) Модели безопасности и их применение. Модель безопасности информационных

потоков и матрицы доступа.

16) Управление рисками. Методики оценки рисков.

17) Политика информационной безопасности. Автоматизированные средства управления

политикой безопасности.

18) Многоуровневая защита данных персонального компьютера.

19) Концепция построения систем контроля и разграничения доступа.

20) Криптографические средства защиты информации. Общие сведения о криптографии.

21) Поточное шифрование: основные понятия. Классификация шифров.

22) Особенности построения симметричных поточных шифров.

23) Блочное симметричное шифрование: основные способы формирования и примитивы

симметричных блочных шифров.

24) Симметричное шифрование на основе сетей Файштеля.

25) Асимметричное шифрование и электронная цифровая подпись:.

26) Практическая стойкость шифров.

27) Протоколы и алгоритмы. Хэш-функции.

28) Электронная цифровая подпись. Отечественные и зарубежные стандарты.

Перспективы криптографии.

29) Защита информации в Internet. Методы и средства обеспечения безопасности

информационных обменов в глобальной сети.

30) Основные этапы, методологию, технологию и средства проектирования средств

защиты информационных систем.

**На 4:**

1) Методологию построения защищенных автоматизированных информационных систем.

2) Схему и алгоритм шифрования RSA.

3) Схему и алгоритм шифрования Рабина.

4) Схему и алгоритм шифрования Эль Гамаль.

5) Средства и способы реализации шифров Цезаря.

6) Средства и способы реализации шифров Полибия.

7) Средства и способы реализации шифров Кардано.

8) Средства и способы реализации шифров Виженера.

9) Аппаратное шифрование в стандарте DES.

10) Аппаратное шифрование в стандарте ГОСТ.

11) Схему и алгоритм электронной цифровой подписи RSA.

12) Схему и алгоритм электронной цифровой подписи Рабина.

13) Схему и алгоритм электронной цифровой подписи Эль Гамаль.

14) Защиту информации в Internet. Протоколы сетевой безопасности.

15) Защиту информации в Internet. Электронная почта и ее защита.

16) Защиту информации в Internet. Безопасность электронных платежей.

17) Концепцию информационной безопасности АСУ ЖТ.

18) Вирусы, программные закладки и механизмы борьбы с ними.

19) Организационно-технологические и технические средства защиты ИБ.

20) Блочное шифрование как следствие развития вычислительной техники.

21) Способы оценки стойкости шифров.

22) Основные нормативно-правовые документы, обеспечивающие стандарты

информационной безопасности.

23) ЭЦП как средство обеспечения достоверности результатов информационного обмена

в сетях.

24) Математические методы при решении профессиональных задач повышенной

сложности.

25) Методы настройки конкретных конфигураций систем и отдельных средств защиты

информации.

**На 5:**

1) Методами и средствами разработки и оформления технической документации на

системы защиты информации объектов транспорта.

2) Техническими и программными средствами защиты информации при работе с

компьютерными системами, включая приемы антивирусной защиты.

3) Методами и средствами исследований свойств защищенности информационных

ресурсов АСУ ЖТ.

4) Методами и средствами исследований угроз информационной безопасности и

управление рисками в АСУ ЖТ.

5) Методами и средствами исследований нормативно-правового обеспечения

информационной безопасности объектов АСУ ЖТ.

6) Методами и средствами исследований алгоритмов поточного шифрования.

7) Методами и средствами исследований алгоритмов блочного симметричного

шифрования.

8) Методами и средствами исследований алгоритмов асимметричного шифрования.

9) Методами и средствами исследований хэш-функций.

10) Методами и средствами исследований алгоритмов электронной цифровой подписи.

11) Приемами обнаружения и нейтрализации программных закладок.

12) Приемами обнаружения и нейтрализации компьютерных вирусов.

13) Техническими средствами защиты информационных ресурсов.

14) Знаниями основных нормативных документов, касающиеся государственной тайны.

15) Знаниями основных нормативно-справочных документов.

16) Международными и отечественными стандартами информационной безопасности.

17) Моделями типовых атак.

18) Моделями безопасности информационных потоков и матрицы доступа.

19) Методиками оценки рисков.

20) Методологией построения защищенных автоматизированных информационных

систем.

21) Автоматизированными средствами управления политикой безопасности.

22) Приемами построения систем контроля и разграничения доступа.

23) Приемами криптоанализа.

24) Приемами оценки стойкости шифров.

25) Протоколами и алгоритмами Хэш-функций.