

РАСМОТРЕНО

Цикловой комиссией специальности
230105

Председатель



Афиногенова О.А.

«05» 05 2014 г..

СОГЛАСОВАННО

Зам директора по УР



Т.В.Трусова

«06» 05 2014г.

Вопросы к экзамену по дисциплине «Основы информационной безопасности»:

1. Информационная безопасность человека и общества. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
2. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
3. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
4. Основные каналы утечки информации. Защита от утечки информации по техническим каналам.
5. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
6. Реализация методов и средств защиты информации.
7. Средства опознавания и разграничения доступа к информации.
8. Криптография. Симметричные криптосистемы.
9. Криптография. Асимметричные криптосистемы.
10. Обзор и классификация методов шифрования информации.
11. Электронно-цифровая подпись.
12. Основные алгоритмы шифрования данных: RSA.
13. Основные алгоритмы шифрования данных: DES.
14. Основные алгоритмы шифрования данных: ГОСТ.
15. Правовые средства защиты информации. Защита программных продуктов. Авторское право.
16. Защита данных в автономном компьютере.
17. Защита данных в вычислительных сетях. Разработка сетевых аспектов политики безопасности.
18. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
19. Показатели оценки достоверности (безошибочности) передачи данных в сетях.
20. Методы взлома компьютерных систем: атаки на уровне операционных систем, атаки на уровне программного обеспечения, атаки на уровне систем управления базами данных.
21. Парольная защита операционных систем. Парольные взломщики.
22. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
23. Структуризация методов обеспечения информационной безопасности. Основные методы реализации угроз информационной безопасности.
24. Основные принципы обеспечения информационной безопасности в автоматизированной системе.
25. Причины, виды и каналы утечки информации.
26. Методы построения защищенных автоматизированных систем.
27. Политика безопасности. Основные типы политики безопасности.
28. Политика безопасности. Модели безопасности.
29. Стандарты информационной безопасности.
30. Правовое обеспечение защиты информации. Нормативные документы.
31. Разрушающие программные воздействия: вирусы и закладки. Антивирусные средства.
32. Психологические аспекты информационной безопасности организации.