ПЕРЕЧЕНЬ ЭКЗАМЕННАЦИОНЫХ ВОПРОСОВ

по магистерским программам

10.04.01 «Аудит информационной безопасности», «Информационно-аналитическое обеспечение процессов принятия решений», «Математическое моделирование и прогнозирование информационных угроз»

1. Лицензирование, аттестация и сертификация в области информационной безопасности.
2. Понятие информационной безопасности. Система информационной безопасности. Основные положения Доктрины информационной безопасности Российской Федерации.
3. Контроль наличия и порядка обращения конфиденциальных документов.
4. Способы и средства обеспечения целостности информации.
5. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений.
6. Классификация информации по ее роли в правовой системе, по степени доступа к ней, классификация информационных ресурсов.
7. Типы атак на компьютерные системы и средства противодействия.
8. Сущность и классификация разрушающих программных воздействий.
9. Принципы и методы планирования функционирования комплексной системы защиты информации. Сущность и содержание контроля.
10. Модели управления доступом.
11. Инсайдерские атаки. Методы защиты от инсайдеров.
12. Направления, силы, средства и методы, используемые для организационного обеспечения информационной безопасности.
13. Опасные и вредные факторы системы «человек – среда обитания», методы анализа антропогенных опасностей, организационные основы защиты окружающей среды.
14. Структура систем документационного обеспечения.
15. Принципы организации информационных систем в соответствии с требованиями по защите информации.
16. Организация допуска персонала к информации ограниченного доступа (к государственной тайне, к коммерческой тайне).
17. Антивирусная защита. Основные подходы к обнаружению вредоносных программ.
18. Классификация и общая характеристика программно-аппаратных средств защиты информации.
19. Анализ и оценка угроз информационной безопасности.
20. Анализ подходов к проектированию стека сетевых протоколов на примере модели OSI и стека протоколов TCP/IP.
21. Методы, принципы и технологии добывания информации
22. Организация защиты информации при проведении совещаний, в ходе рекламной и издательской деятельности.
23. Сетевые экраны: основные функции и подходы к реализации.
24. Комплексное планирование мероприятий по обеспечению информационной безопасности.
25. Организация ИТЗИ, типовые меры, контроль эффективности.
26. Правовая защита информации ограниченного доступа (уголовно-правовая, административно-правовая, гражданско-правовая, дисциплинарная и материальная ответственность).
27. Алгоритмы блочного шифрования.
28. Понятие, виды защищенного документооборота. Особенности конфиденциального делопроизводства.
29. Правовые нормы и стандарты по лицензированию в области обеспечения сертификации средств защиты информации.
30. Методы и средства выявления угроз информационной безопасности.
31. Стандарт шифрования ГОСТ 28147-89.

32. Учет конфиденциальных документов (входящих, исходящих, внутренних, выделенного хранения).
33. Средства инженерной защиты и технической охраны объектов.
34. Моделирование системы ИТЗИ.
35. Идентификация, аутентификация, авторизация.