Оценочные материалы для промежуточной аттестации по дисциплине

Название дисциплины «Информационная безопасность»

Код, направление подготовки	38.05.01 Экономическая безопасность
Направленность (профиль)	Экономико-правовое обеспечение экономической безопасности
Форма обучения	Очная, Заочная
Кафедра-разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Экономических и учетных дисциплин

Примерные вопросы для контрольной работы:

1. Актуальность проблемы защиты информации.
2. Основные факторы повышения уязвимости информации.
3. Перечислить риски в промышленности, связанные с ИТ.
4. Актуальность защиты информации, связанной с составом и функциональными возможностями современных ИТ.
5. Основные понятия информационной безопасности.
6. Информационные ресурсы сбора информации об уязвимостях и рисках информационных и вычислительных систем.
7. Перечислите основные законы РФ, связанные с информационной безопасностью.
8. Основные положения Федерального закона №149.
9. Основные положения Федерального закона №152.
10. Способы и подходы к поиску основных законодательных актов РФ в области защиты информации.
11. Проблемы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла.
12. Организация секретного делопроизводства и мероприятий по защите информации.

Типовые вопросы к зачёту:

1. Основные понятия информационной безопасности.
2. Информационные технологии и необходимость ИБ.
3. Система защиты информации и ее структуры.
4. Экономическая информация как товар и объект безопасности.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.

17. Субъекты и причины совершения компьютерных преступлений.
18. Вредоносные программы, их виды.
19. История компьютерных вирусов и современность.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Государственное регулирование информационной безопасности в РФ.
22. Задачи ИБ в программе «цифровая экономика».
23. Доктрина информационной безопасности России.
24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.
25. Уголовно-правовой контроль над компьютерной преступностью в РФ.
26. Политика безопасности и ее принципы.
27. Фрагментарный и системный подход к защите информации.
28. Методы и средства защиты информации.
29. Организационное обеспечение ИБ.
30. Организация конфиденциального делопроизводства.
31. Организационно-экономическое обеспечение ИБ.
32. Инженерно-техническое обеспечение компьютерной безопасности.
33. Организационно-правовой статус службы безопасности.
34. Защита информации в Интернете.
35. Электронная почта и ее защита.
36. Защита от компьютерных вирусов.
37. «Больные» мобильники и их «лечение».
38. Популярные антивирусные программы и их классификация.
39. Этапы и освоение защиты информации экономических объектов.
40. Криптографические методы защиты информации.
41. Оценка эффективности инвестиций в информационную безопасность.
42. Российские компании в сфере ИБ.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47.Информационная безопасность предпринимательской деятельности.