ПРИМЕРНАЯ ТЕМАТИКА
ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль «Организация и технология защиты информации»
на 2023/24 учебный год
(Утверждено на заседании Совета института 31.08.2023, протокол № 1)

1. Разработка организационно-технических рекомендаций по повышению эффективности защиты конфиденциальной информации предприятия (на конкретном примере).

2. Разработка организационно-технических мер по защите информации, составляющей служебную тайну предприятия (на конкретном примере).

3. Разработка предложений по созданию системы защиты информации предприятия централизованной структуры.

4. Разработка предложений по созданию защищенной информационной системы предприятия децентрализованной структуры.

5. Обоснование решений по определению способов оценки угроз информационной безопасности предприятия (на конкретном примере).

6. Разработка организационно-технических мер защиты выделенного помещения предприятия (на конкретном примере).

7. Разработка рекомендаций руководителю предприятия по оборудованию помещения для проведения служебных совещаний (на конкретном примере).

8. Разработка рекомендаций руководителю предприятия по оборудованию помещения для обработки персональных данных (на конкретном примере).

9. Системный анализ информационной инфраструктуры и разработка защищенной корпоративной информационной системы предприятия (на конкретном примере).

10. Разработка модели комплексной системы защиты информации предприятия (на конкретном примере).

11. Оценка рисков и управление информационной безопасностью предприятия в условиях новых реалий (на конкретном примере).

12. Разработка автоматизированной системы оценки информационных рисков предприятия (на конкретном примере).

13. Организация комплексной системы защиты конфиденциальной информации предприятия (на конкретном примере).

14. Разработка политики информационной безопасности на основе анализа информационных рисков предприятия (на конкретном примере).

15. Совершенствование нормативно-методической базы защиты конфиденциальной информации предприятия (на конкретном примере).

16. Разработка организационно-технических мер противодействия утечке информации по техническим каналам предприятия (на конкретном примере).

17. Разработка рекомендаций по совершенствованию защиты коммерческой тайны предприятия (на конкретном примере).

18. Разработка рекомендаций по совершенствованию защиты ресурсов автоматизированной системы предприятия (на конкретном примере).

19. Оценка эффективности системы защиты информации предприятия (на конкретном примере).

20. Разработка рекомендаций по проведению аудита информационной безопасности предприятия (на конкретном примере).

21. Разработка рекомендаций по использованию зарубежного опыта (на примере конкретной страны или ряда стран) при организации защиты конфиденциальной информации.

22. Организация информационно-аналитической деятельности по обеспечению информационной безопасности предприятия (на конкретном примере).

23. Формирование информационно-аналитического обеспечения для работы руководителя подразделения защиты информации предприятия (на конкретном примере).

24. Разработка направлений совершенствования и регламентации доступа персонала к конфиденциальной информации, документам и продукции предприятия (на конкретном примере).

25. Разработка нормативно-методических документов по регламентации организационной защиты информации, обрабатываемой средствами вычислительной и организационной техники предприятия (на конкретном примере).

26. Разработка направлений и способов контроля надежности и эффективности организационной зашиты информации предприятия (на конкретном примере).

27. Разработка направлений, методов и нормативно-методических документов по защите информации в рекламной, выставочной и издательской деятельности предприятия (на конкретном примере).

28. Разработка направлений, методов и нормативно-методических документов по организационной защите продукции при ее производстве, транспортировки и хранении предприятия (на конкретном примере).

29. Разработка направлений, методов и нормативно-методических документов по организационной защите персональных данных предприятия (на конкретном примере).

30. Разработка предложений по реализации на предприятии комплекса мер противодействия утечки информации по скрытым информационным каналам.

32. Разработка направлений, методов и нормативно-методического обеспечения работы с персоналом, обладающих конфиденциальной информацией.

33. Разработка и регламентация технологии хранения и использования конфиденциальных документов в архивах (на конкретном примере).

34. Разработка и регламентация организационной защиты информации при проведении научно-исследовательских и опытно-конструкторских работ (на конкретном примере).

35. Организация защиты конфиденциальной информации при разработке инновационных проектов (на конкретном примере).

36. Организация защиты конфиденциальной информации корпоративными пользователями систем интернет-банкинга (на конкретном примере).

37. Организация защиты конфиденциальной информации корпоративными пользователями систем удаленного доступа (на конкретном примере).

38. Разработка системы защиты персональных данных предприятия (на конкретном примере).

39. Организация системы защиты электронного документооборота предприятия (на конкретном примере).

40. Организация защищенного документооборота предприятия (на конкретном примере).

41. «Разработка рекомендаций по совершенствованию организации и управления службой защиты информации предприятия (на конкретном примере)».

41. Разработка организационно-технических рекомендаций по совершенствованию защиты конфиденциальной информации предприятия (на конкретном примере).

42. Разработка предложений по совершенствованию управления системой защиты информации предприятия (на конкретном примере).

45. Разработка защиты персональных данных в автоматизированных системах

46. Обеспечение информационной безопасности в кредитно-финансовой сфере в условиях новых реалий

47. Организация защищенности персональных данных на основании изменений Федерального закона №152-ФЗ «О персональных данных» (на конкретном примере)

48. Реализация организационно-технических мер по повышению защищенности объектов информационной инфраструктуры (на конкретном примере).

49. Организация мониторинга инцидентов информационной безопасности, реагирования на них и ликвидации их последствия (ГосСОПКА)

50. Порядок категорирования объектов КИИ: порядок пересмотра категории значимости (на конкретном примере).

51. Проектирование подсистемы безопасности АСУ ТП - значимого объекта КИИ

52. Построение безопасности критической информационной инфраструктуры

53. Организация защиты от внутренних угроз как обязательный элемент защиты КИИ

54. Методы построения коммерческого SOC.