ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ
на 2020/21 учебный год
(направление подготовки 10.03.01 «Информационная безопасность»
по профилю подготовки «Организация и технология защиты информации»)
(Утверждено на заседании кафедры 31.08.2020, протокол № 1)

1. Порядок разработки политики информационной безопасности предприятия.

2. Порядок реализации политики информационной безопасности с учетом применения комплексного подхода к обеспечению информационной безопасности объекта защиты.

3. Организация процедуры аттестации объекта информатизации по требованиям безопасности информации.

4. Порядок сопровождения аттестации объекта информатизации по требованиям безопасности информации.

5. Организация контрольных проверок работоспособности и эффективности применяемых средств защиты информации на объекте защиты.

6. Нормативно-методическое обеспечение комплексной системы защиты информации на объекте защиты.

7. Разработка мероприятий по обеспечению безопасности на предприятии.

8. Порядок проведения анализа для проектирования подсистем и средств обеспечения информационной безопасности на предприятии.

9. Организация проведения технико-экономического обоснования проектных решений для проектирования подсистем и средств обеспечения информационной безопасности на предприятии.

10. Порядок разработки и оформления рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности.

11. Порядок составления обзора актуальной научно-технической литературы по вопросам обеспечения информационной безопасности по профилю «Организация и технология защиты информации»

12. Требования, предъявляемые к объектам и системам информатизации на соответствие требованиям стандартов в области информационной безопасности.

13. Порядок организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы

безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

14. Повышение информационной безопасности электронного документооборота.

15. Разработка алгоритма аудита информационной безопасности системы.

16. Исследование методов оценки рисков информационной безопасности на объекте защиты.

17. Разработка плана мероприятий по внедрение eToken на объекте защиты.

18. Защита информации при подключении информационных систем общего пользования к международной сети «Интернет».

19. Использование электронной подписи для обеспечения защиты информации при использовании системы электронного документооборота.

20. Требования к автоматизированному рабочему месту для разработки конфиденциальных документов.

21. Требования, предъявляемые к автоматизированному рабочему месту специалиста по информационной безопасности.

22. Разработка и внедрение системы гарантированного уничтожения носителей конфиденциальной информации.

23. Особенности разработки и коммерциализации решений в области информационной безопасности.

24. Разработка методики расследования действий, связанных с использованием АРМ и информационных ресурсов организации.

25. Моделирование политики безопасности, достоинства и недостатки моделей.

26. Особенности организации и обеспечения защиты персональных данных в РФ на современном этапе.

27. Разработка статистического классификатора системы обнаружения атак.

28. Порядок учета персонала, получившего доступ к конфиденциальной документированной информации.

29. Место и роль системы внутреннего контроля в обеспечении информационной безопасности объекта защиты.

30. Защита информации с помощью интегрированных систем охраны.

31. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности.

32. Разработка модели угроз ИБ и модели нарушителей ИБ выбранного объекта.