7. Учебно-методическое обеспечение самостоятельной работы обучающихся

Рекомендации студентам

Для лучшего усвоения положений дисциплины студенты должны:

- постоянно и систематически, с использованием рекомендованной литературы и электронных источников информации, закреплять знания, полученные на лекциях;
- находить решения проблемных вопросов, поставленных преподавателем в ходе лекций и практических заданий;
- регулярно и своевременно изучать материал, выданный преподавателем на самостоятельную проработку;
- с использованием средств информационных систем, комплексов и технологий, электронных учебников и практикумов, справочных правовых и тренинго-тестирующих систем, информационных ресурсов сети Интернет выполнить на компьютере тематические практические задания, предназначенные для самостоятельной работы;
- находить, используя разные источники информации, ответы на теоретические и практические контрольные вопросы по темам дисциплины;
- использовать информацию, найденную на сайтах фирм-разработчиков информационных систем и технологий, применяемых в экономике;
- при подготовке к экзамену учитывать общие требования и рекомендации.

При освоении данного курса бакалаврам может быть предложено выполнение инициативной научно-исследовательской работы.

Методические указания по выполнению научно-исследовательской работы

Целью выполнения работы является:

– закрепление знаний, полученных студентами в процессе теоретического обучения;

– проведение исследования проблемы;

– активное использование пакетов прикладных программ; анализ библиографических материалов.

– отработка приемов и способов аналитических расчетов на практическом материале.

Выбор темы производится студентом и утверждается преподавателем. Рекомендуемый объем работы 10-15 страниц машинописного текста.

В каждой работе, кроме основных разделов, независимо от темы, предусматривается «Введение», «Заключение», «Список используемой литературы», «Приложения».

Список литературы должен быть составлен в соответствии с библиографическими требованиями.

Выполнять научно-исследовательскую работу необходимо с использованием текстового редактора MS Word, электронных таблиц Excel, а также можно использовать пакеты прикладных программ (ППП).

К оформлению научно-исследовательской работы предъявляются общие типовые требования.

Рекомендуемые направления научно-исследовательских работ

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

6 Информационная безопасность (по материалам зарубежных источников и литературы).

7 Правовые основы защиты конфиденциальной информации.

8 Экономические основы защиты конфиденциальной информации.

9 Организационные основы защиты конфиденциальной информации.

10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

11 Составление инструкции по обработке и хранению конфиденциальных документов.

12 Направления и методы защиты документов на бумажных носителях.

13 Направления и методы защиты машиночитаемых документов.

14 Архивное хранение конфиденциальных документов.

15 Направления и методы защиты аудио- и визуальных документов.

16 Порядок подбора персонала для работы с конфиденциальной информацией.

17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

18 Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

19 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

20 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

21 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

22 Порядок защиты информации в рекламной и выставочной деятельности.

23 Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

24 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

25. ИТ в цифровой экономике и их инф безопасность

25 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

26 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

27 Назначение, виды, структура и технология функционирования системы защиты информации.

28 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

29 Аналитическая работа по выявлению каналов утечки информации фирмы.

30 Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

31 Направления и методы защиты профессиональной тайны.

32 Направления и методы защиты служебной тайны.

33 Направления и методы защиты персональных данных о гражданах.

34 Методы защиты личной и семейной тайны.

35 Построение и функционирование защищенного документооборота.

36 Защита секретов в дореволюционной России.

37 Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Перечень вопросов к экзамену

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.

22. Деятельность ~~международных~~ Российских организаций в сфере информационной безопасности. (Инфофорум-2020)

23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.

24. Доктрина информационной безопасности России.

25. Уголовно-правовой контроль над компьютерной преступностью в России.

26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.

28. Фрагментарный и системный подход к защите информации.

29. Методы и средства защиты информации.

30. Организационное обеспечение ИБ.

31. Организация конфиденциального делопроизводства.

32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.

33. Инженерно-техническое обеспечение компьютерной безопасности.

34. Организационно-правовой статус службы безопасности.

35. Защита информации в Интернете.

36. Электронная почта и ее защита.

37. Защита от компьютерных вирусов.

38. «Больные» мобильники и их «лечение».

39. Популярные антивирусные программы и их классификация.

40. Организация системы защиты информации экономических объектов.

41. Криптографические методы защиты информации.

42. Этапы построения системы защиты информации.

43. Оценка эффективности инвестиций в информационную безопасность.

44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.

45. Управление информационной безопасности на государственном уровне.

46. Аудит ИБ автоматизированных банковских систем.

47. Электронная коммерция и ее защита.

48. Менеджмент и аудит информационной безопасности на уровне предприятия.

49. Информационная безопасность предпринимательской деятельности.

50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.