Контрольная работа по дисциплине «Информационная безопасность»

Контрольная работа состоит из двух частей: 1) Ответы на теоретические вопросы; 2) Подготовка доклада по выбранной теме.

1. Теоретические вопросы:
2. *Назовите основные виды угроз безопасности предприятия.*
3. *Перечислите цель и задачи системы безопасности* *предприятия.*
4. *Какие средства используются для обеспечения безопасности* *предприятия?*
5. *Что понимается под информационной безопасностью предприятия? Компоненты ИБ.*
6. *Дайте определение трем видам овладения* *конфиденциальной информацией.*
7. *Определите в процентах степень опасности внутренних и* *внешних угроз неправомерному овладению информацией.*
8. *Какие компоненты входят в состав концептуальной модели безопасности информации?*
9. *Какими инструкциями руководствуются при организации работы службы безопасности предприятия?*
10. *Назвать основные виды безопасности на предприятии.*
11. *Что необходимо включать в коллективный договор для правового обеспечения защиты информации?*
12. *Перечислить основные нормативные документы, регламентирующие деятельность в области защиты информации.*
13. *В чем состоит суть лицензирования деятельности предприятий в области защиты информации?*
14. *Какие виды деятельности предприятия в области защиты информации необходимо лицензировать?*
15. *Назвать разделы устава службы безопасности предприятии и дать им характеристику.*
16. *Назовите основные задачи подразделения и охраны.*
17. *Какие требования предусматривает внутриобъектовый режим?*
18. *Какие требования предусматривает пропускной режим на предприятии?*
19. *Какие функции возлагаются на специальный отдел?*
20. *Что является источниками конфиденциальной информации на предприятии?*
21. *Назовите виды конфиденциальной информации, используемой на предприятии.*
22. *С какой целью на предприятии создается подразделение информационно аналитической деятельности?*
23. *Какие мероприятия по защите информации выполняет подразделение инженерно-технической защиты?*
24. *Дайте характеристику мероприятий по блокированию несанкционированного получения конфиденциальной информации.*
25. *Зачем на предприятии создаются подразделения разведки?*
26. *Что является объектом анализа подразделения контрразведки на предприятии?*
27. *Перечислите виды деятельности, выполняемые службой информационной безопасности (СЗИ).*
28. *Кто должен входить в состав СЗИ?*
29. *Назовите перечень основных организационных технических мероприятий, выполняемых сотрудниками СЗИ.*
30. Темы докладов
31. Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.
32. Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Способы совершения компьютерных преступлений.
33. Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.
34. Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам.
35. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.
36. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.
37. Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
38. Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.
39. Организация защиты служебной информации и персональных данных на примере организации.
40. Актуальные проблемы информационной безопасности компьютерных систем в банковской и торгово-экономической деятельности.

**Требования к оформлению**

1. Контрольная работа сдается в электронном виде (высылается на адрес: andr-ilim@mail.ru). К сообщению 'электронной почты прикрепляется текстовый файл в формате \*.docx или \*.doc, размер листа - A4, поля: верхнее и нижнее – 2 см., правое – 1,5, левое – 3 см., Шрифт: Times New Roman, 14 пунктов, полуторный междустрочный интервал. Нумерация со второй страницы, номер расположен в нижнем правом углу. На титульном листе указывается «Контрольная работа».
2. В контрольной работе должны присутствовать следующие структурные компоненты: титульный лист, оглавление, две части, список использованной литературы (и/или Интернет-источников с указанием адреса web-страницы).

3. Файл, созданный в ходе выполнения контрольной работы, именуется по образцу:

"ИБк.р.\_группа ФИО", например: "ИБ к.р. ПИЭз Новикова И.А."

- и высылается по электронной почте. В электронном письме обязательно заполняется поле **тема.**  Контрольная работа должна быть отправлена *за две недели* до начала сессии.