**[1 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ](" \l "aaa)**

Основы защиты информации в условиях перехода к информационному обществу для каждого гражданина являются актуальными и связаны со свободами слова, перемещения, тайны переписки и другими свободами, нарушение которых в условиях электронных технологий могут быть без особых усилий использованы и против самого человека.

Контрольная работа включает теоретические и практические вопросы по различным разделам курса, на которые необходимо дать ответы, выполнить практическое задание и привести выводы.

Каждый студент выполняет свой вариант задания, определяемый по порядковому номеру в списке группы.

Контрольная работа включает:

*Введение,* где определяется актуальность проблем информационной безопасности предприятий всех форм собственности, организационно-правовых форм и сфер деятельности общества.

*Теоретический вопрос,* включающий подразделы и отражающий современное состояние отдельных проблем в области информационной безопасности согласно заданию и варианту.

*Практические вопросы*.

*Заключение,* содержащее краткие выводы по выполненной работе.

*Литература* – использованные источники при выполнении работы.

**[2 ТЕОРЕТИЧЕСКИЕ ВОПРОСЫ](" \l "aaa)**

Тема определяется по порядковому номеру в списке группы. Студент вправе исследовать по согласованию с преподавателем другую тему.

Примерный перечень тем:

1. Защита информации в кредитных организациях: направления и проблемы.
2. Информационные ресурсы общества и методы их защиты.
3. Аудит информационной безопасности предприятия.
4. Государственные и международные стандарты в области информационной безопасности защиты данных: классификация и обзор.
5. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях: опыт и рекомендации.
6. Основы криптографии: история, методы и алгоритмы.
7. Защита информации в государственных организациях: нормирование и контроль.
8. Программно-аппаратные технологии обеспечения защиты информации в сети Интернет.
9. Сложность алгоритмов криптографии: криптоанализ и направления исследований.
10. Политика информационной безопасности предприятия.
11. Классификация информации по степени защиты и нормативные акты.
12. Системы криптографической защиты информации в России: законодательство, организации инфраструктуры, использование в электронном обмене информацией.
13. Практические модели обеспечения защиты информации корпоративных систем.
14. Интеграция предприятий в Интернет и информационная безопасность: модели и способы защиты.
15. Комплексные системы защиты информации предприятия: компоненты и задачи.
16. Защита информации в Интернет: направления и проблемы.
17. Защита информации в вычислительных сетях.
18. Электронная цифровая подпись, законодательство, инфраструктура.
19. Экономические аспекты защиты информации предприятия.
20. Векторы атак на информационные системы и способы защиты.
21. Понятие национальной безопасности. ИБ в системе национальной безопасности РФ. Информационный аспект в других составляющих национальной безопасности.
22. Основные источники угроз и угрозы ИБ РФ. Основные задачи по обеспечению ИБ РФ. Региональные проблемы информационной безопасности.
23. Общеметодологические принципы теории ИБ. Стандарты и руководящие документы. Структура службы безопасности организации.
24. Принцип целенаправленности и целесообразности в анализе безопасности объектов и синтеза систем защиты.
25. Модели и методы риск-анализа, основные представления, элементы и структура, факторы риска.
26. Методики расчета рисков.
27. Оценка эффективности применения средств защиты. Соотношение надёжности и безопасности, допустимый ущерб.
28. Мониторинг и аудит безопасности, экспертные системы.
29. Физическая безопасность, методы и технические средства ее обеспечения. Основные составляющие ИТСО.
30. Современные компьютерные методы обеспечения физической безопасности.
31. Технические каналы утечки информации.
32. Пассивные методы технической защиты информации.
33. Активные методы технической защиты информации.
34. Закладные устройства.
35. НСД к информации, его место в проблеме информационной безопасности.
36. История международной нормативной базы в области ИБ.
37. РД ФСТЭК «Концепция защиты от НСД».
38. РД ФСТЭК «СВТ защита от НСД…»
39. РД ФСТЭК « АС защита от НСД…»
40. РД ФСТЭК «Защита от НСД. Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей»
41. ГОСТ Р 15408 и его применение.
42. ГОСТы РФ в области ИБ. С требованиями стандартов можно ознакомиться на открытом web-ресурсе: <http://docs.cntd.ru/document/1200075565>
43. Формальные модели информационной безопасности
44. Субъекты и объекты доступа к ресурсам, модели доступа. Правила разграничения доступа.
45. Понятие об идентификации и аутентификации субъектов доступа.
46. Классификация защищенности СВТ и АС от НСД к информации.
47. Основные технические методы и средства получения НСД к информации.
48. Средства защиты информации от несанкционированного доступа (СЗИ от НСД).
49. Отечественные компьютеры на основе российской аппаратной платформы. Понятие защищенного компьютера.
50. Реализация общероссийских защищенных компьютерных сетей.
51. Перспективы развития отечественных защищенных АС.
52. Оптические компьютеры и их применение.
53. Квантовые компьютерные технологии и их применение.
54. Информационная безопасность и перспективные технологии.
55. Механизмы защиты ОС. Отечественные защищенные ОС.
56. Механизмы защиты СУБД. Отечественные защищенные СУБД.
57. Защита программ от копирования.
58. Защита программ от исследования.
59. Защита программ и данных от модификации.
60. Организация контроля целостности.
61. Обеспечение непрерывности функционирования информационных систем предприятия. Международный подход.
62. План восстановления после бедствий.
63. Компьютерные технологии обеспечивающие надежное восстановление. Классы восстановления.
64. Методика разработки планов восстановления после бедствий.
65. Гибридное противоборство, возможности и перспективы обеспечения ИБ на международном уровне.

**2. ПРАКТИЧЕСКИЙ ВОПРОС**

* 1. Представить классификацию и обзор законодательных актов в области информационной безопасности и защиты данных.

(Доктрина информационной безопасности РФ и последующие стратегические документы. Законодательные акты в сфере информационной безопасности (ФЗ №149 от 27.07.2006, ФЗ №152 от 27.07.2006, Указ Президента №334 от 03.04.1995, Указ Президента РФ №351 от 17.03.2008, Постановление Правительства РФ №608 от 26.06.1995, №504 от 15.08.2006, №532 от 31.08.2006 и др.) и руководящие документы ФСБ РФ, ФСТЭК РФ, Роскомнадзора РФ.)

Рекомендуемое содержание модели угроз:

1.Описание информационной системы и особенностей ее функционирования.

1.1 Цель и задачи, решаемые информационной системой.

1.2 Описание структурно-функциональных характеристик информационной системы.

1.3 Описание технологии обработки информации.

2. Возможности нарушителей (модель нарушителя).

2.1 Типы и виды нарушителей.

2.2 Возможные цели и потенциал нарушителей.

2.3 Возможные способы реализации угроз безопасности информации.

3. Актуальные угрозы безопасности информации. Информация об угрозах безопасности:

- идентификатор угрозы безопасности информации;

- описание угрозы безопасности информации;

- источник угрозы безопасности информации;

- объект, на который может быть направлена угроза безопасности информации;

- возможные последствия от реализации угрозы безопасности информации.

Используя банк данных угроз безопасности информации, который представляет собой единую систему учета, хранения, предоставления информации об уязвимостях и угрозах безопасности информации (www.bdu.fstec.ru), представить описание угроз для информационной системы.

Рекомендации по формированию: существуют угрозы, связанные с потенциальным наличием нарушителя с определенным потенциалом, связанные с отсутствием реализованных мер защиты информации, связанные с новыми/выявленными уязвимостями в ТС, ПО, СЗИ. В Модели необходимо указать, что для конкретной ИС конкретного уровня/класса защищенности либо нет "лишних" угроз, расширяющих требования НМД, либо есть такие угрозы, которые необходимо нейтрализовать за счет дополнительных орг.-тех. мероприятий в области ЗИ. Для обоснования и стоит пользоваться банком данных ФСТЭК России (наряду с международными банками данных).

К примеру (очень условно и коротко), сама по себе угроза пассивного сбора информации о сетевой структуре высокой опасности не несет – в ряде случаев ею можно пренебречь. В особенности, если результирующий потенциал нарушителя в такой ситуации по Модели вытекает, например, "низким" (хакер-любитель). В конце концов, любой грамотный желающий может использовать тот же NMAP для скана ИС, имеющей выход в Интернет. Но, в купе с, предположим, недавно обнаруженной уязвимостью сервера Apache (ссылка на bdu.fstec.ru), который крутится на web-сервере ИС и доступен через Интернет, такая угроза повышает свой статус до актуальной. Ибо позволяет проанализировать демаскирующие признаки, позволяет сформировать допустимый вектор атаки.

1. <http://pdsec.ru/uroven_zaschischennosti/> сайт где калькулятор защищенности
2. <http://weta.ru/services-protection-classification-personal-data.php> такой же сайт

Перечень возможных информационных систем для проведения анализа:

1. Финансово-экономическая информационная система – информационная система, предназначенная для выполнения функций управления на предприятии.
2. Медицинская информационная система – информационная система, предназначенная для использования в лечебном или лечебно-профилактическом учреждении.
3. Географическая информационная система – информационная система, обеспечивающая сбор, хранение, обработку, доступ, отображение и распространение пространственно-координированных данных (пространственных данных).
4. Производственные системы
5. Административные системы.
6. Системы маркетинга.
7. Системы научных исследований.
8. Системы поддержки принятия решения (руководителя, должностного лица и т.д.)
9. Информационно-вычислительные: автоматизации проектирования, проблемно-ориентированные, моделирующие.
10. Справочные системы: системы делопроизводства, автоматизированные архивы.
11. Системы обучения: системы управления образованием и образовательными организациями, системы деловых игр, системы программного обучения.
12. Мобильные системы.

Литература

1. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - М.: Гор. линия-Телеком, 2011. - 288 с.: ил. <http://ibooks.ru/reading.php?productid=334002>
2. Пособие, электронный ресурс: <http://www.volpi.ru/umkd/zki/index.php?man=1&page=1>
3. Методы и средства защиты компьютерной информации : учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, <http://www.tstu.ru/book/elib/pdf/2006/shamkin2.pdf>
4. Мартемьянов, Юрий Федорович. Операционные системы. Концепции построения и обеспечения безопасности [Текст] : учебное пособие / Ю. Ф. Мартемьянов, А. В. Яковлев, А. В. Яковлев. - Москва : Горячая линия -Телеком, 2010. - 332 с. <http://ibooks.ru/reading.php?productid=334008>