МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационных систем и технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«____» _____ 2020

ДОКЛАДЫ ПО ТЕМАМ РАЗДЕЛА: "БАЗОВЫЕ ТЕХНИЧЕСКИЕ ВОПРОСЫ ОРГАНИЗАЦИИ БЕЗОПАСНОСТИ ДАННЫХ И ИНФОРМАЦИОННОЙ ЗАЩИТЫ"

методические указания по выполнению практической работы №2
по дисциплине «Информационные технологии»
для направления подготовки 10.05.02 Информационная
безопасность телекоммуникационных систем

Курск -2020

УДК 004

Составитель: Л.В. Стародубцева

Рецензент
Кандидат технических наук, доцент *Ю.А. Халин*

Доклады по темам раздела: "Базовые технические вопросы организации безопасности данных и информационной защиты": методические указания по выполнению практической работы №2 / Юго-Зап. гос. ун-т; сост.: Л.В. Стародубцева. - Курск, 2020. 12 с.

Содержит теоретические сведения по дисциплине «Информационные технологии».

Методические указания по структуре, содержанию и стилю изложения материала соответствуют методическим и научным требованиям, предъявляемым к учебным и методическим пособиям.

Предназначены для студентов направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ.л. . Уч.-изд. л. . Тираж экз. Заказ.
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическая работа №2

Доклады по темам раздела: "Базовые технические вопросы организации безопасности данных и информационной защиты"

Теоретические сведения

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т. д.) на носителях различных типов. Она может представлять ценность для отдельных лиц или организаций.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

В последнее время все большие объемы информации, в том числе и критически важной для отдельных людей, организаций или государств, хранятся, обрабатываются и передаются с использованием автоматизированных систем (АС) обработки информации.

Система обработки информации — совокупность технических средств и программного обеспечения, а также методов

обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации

Объект информатизации— совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

В зависимости от конкретных условий может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов — информационных, программных и т. д.

Информационные ресурсы (активы) — отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Рассматривая вопросы безопасности АС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание. Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить, соответственно, удаление пользователем файла с важной информацией и пожар в здании. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) — свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям, как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подойти к определению трех основных угроз безопасности.

Угроза конфиденциальности (угроза раскрытия) — это угроза, в результате реализации которой конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась. Здесь надо пояснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию, относящуюся к разряду государственной тайны, а «конфиденциальной» — персональные данные, коммерческую тайну и т. п.

Угроза целостности — угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности.

Политика безопасности — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) — угроза, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Ряд авторов дополняют приведенную классификацию, вводя *угрозу раскрытия параметров* АС, включающей в себя подсистему защиты. Угроза считается реализованной, если

злоумышленником в ходе нелегального исследования системы определены все ее уязвимости. Данную угрозу относят к разряду опосредованных: последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность для реализации первичных (непосредственных) угроз.

Таким образом, *безопасность информации* — это состояние защищенности информации, при котором обеспечены се конфиденциальность, доступность и целостность.

Защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Выделяются следующие направления защиты информации:

- *правовая защита информации* — защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- *техническая защита информации* — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- *криптографическая защита информации* — защита информации с помощью ее криптографического преобразования;
- *физическая защита информации* — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

- средства контроля эффективности защиты информации;
- средства физической защиты информации;
- криптографические средства защиты информации.

Варианты тем доклада

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.

6. Классификация источников и носителей информации.

7. мероприятия по управлению доступом к информации.

8. Функциональные источники сигналов. Опасный сигнал.

9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.

10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

12. Виды угроз безопасности информации.

13. Основные принципы добывания информации.

14. Процедура идентификации, как основа процесса обнаружения объекта.

15. Методы синтеза информации.

16. Методы несанкционированного доступа к информации.

17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

18. Способы наблюдения с использованием технических средств.

19. Каналы утечки информации. Технические каналы утечки

20. Классификация технических каналов утечки по физической природе носителя.

21. Классификация технических каналов утечки по информативности.

22. Классификация технических каналов утечки по времени функционирования.

23. Классификация технических каналов утечки по структуре.

24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

25. Перехват электромагнитных излучений.

26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.

27. Понятия скрытия информации, виды скрытий. Информационный портрет.

28. Противодействие наблюдению. Способы маскировки.

29. Способы и средства противодействия подслушиванию.

30. Нейтрализация закладных устройств.

31. Состав инженерной защиты и технической охраны объектов.

32. Инженерные конструкции и сооружения для защиты информации. Их классификация.

33. Средства идентификации личности.

34. Классификация датчиков охранной сигнализации.

35. Классификация извещателей.

36. Телевизионные системы наблюдения.

37. Основные средства системы видеоконтроля.

38. Защита личности как носителя информации.

39. Системный подход к защите информации.

40. Параметры системы защиты информации.

41. Этапы проектирования системы защиты информации.

42. Потенциальные каналы утечки информации.

43. Этапы разработки мер по предотвращению угроз утечки информации.

44. Угрозы сохранности данных в компьютере случайного характера.

45. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.

46. Дефекты магнитных дисков.

47. Простые приемы, используемые для защиты компьютера от умышленных действий.

48. Классификация вирусов.

49. Классификация антивирусных программ.

50. Компьютерная преступность. Виды преступной деятельности.

51. Преступления, связанные с нарушением частной тайны.

52. Информационные процессы.

53. Информационные технологии и их основные свойства.

54. Понятия сигнала, сообщения и данных.

55. Методы защиты информации от преднамеренного доступа.

56. Методы обеспечения безопасности каналов передачи данных.

57. Методы обеспечения достоверности передачи информации (методов защиты от ошибок).

58. Механизмы обеспечения безопасности радиолиний.

59. Криптографическая защита информации (основные понятия).

60. Методы шифрования данных.