МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Кафедра «Вычислительной и прикладной математики»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки
09.03.01 «Информатика и вычислительная техника»

Направленность (профиль) подготовки
Системный анализ и инжиниринг информационных процессов
Системы автоматизированного проектирования вычислительных средств
Вычислительные машины, комплексы, системы и сети

Уровень подготовки
Бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная, заочная

Рязань

1. Темы практических занятий

Тема 1. Освоение приемов восстановления файлов, инфицированных вирусом, при отсутствии антивирусного программного обеспечения.

Изучение законодательных актов РФ в области защиты информации и информационных систем от разрушающих программных средств. Изучение различных видов разрушающих программных средств. Понятие компьютерного вируса. Классификация вирусов по различным признакам. Изучение алгоритмов работы резидентных вирусов, вирусов, использующих стелс-алгоритмы, полиморфичность. Анализ деструктивных, разрушительных возможностей разрушающих программных средств. Основной механизм заражения вирусом, макровирусом. Методы обнаружения макровируса. Методы обезвреживания макровируса.

Цель занятия. Освоить методы и приемы обнаружения различных видов разрушающих программных средств, изучить алгоритмы работы резидентных, стелс, полиморфных вирусов. Изучить механизмы заражения вирусом, макровирусом, методы обнаружения макровируса, методы обезвреживания макровируса.

Задачи закрепления теоретических знаний и практических умений и навыков: студент должен знать основные законодательные акты РФ в области защиты информации и информационных систем от разрушающих программных средств. Знать алгоритмы работы и механизм заражения вирусов и макровирусов, уметь применять методы обезвреживания вирусов и макровирусов.

Форма проведения: обсуждение и теоретический опрос по теме занятия, самостоятельное решение студентами задачи обнаружения инфицированного объекта и применение метода обезвреживания макровируса в аудитории, выполнение домашнего задания по изучаемой теме.

Тема 2. Основные принципы работы с электронной цифровой подписью.

Основные понятия и определения электронной цифровой подписи. Основные алгоритмы электронной цифровой подписи. Виды атак на алгоритмы электронной цифровой подписи. Математическая и программная реализация алгоритмов электронной цифровой подписи.

Цель занятия. Освоить базовые математические методы и способы практической реализации наиболее известных алгоритмов электронной цифровой подписи.

Задачи закрепления теоретических знаний и практических умений и навыков: студент должен знать основные понятия и базовые математические зависимости для практической реализации алгоритмов электронной цифровой подписи.

Форма проведения: анализ базовых математических приемов рассматриваемых алгоритмов на аудиторных занятиях, самостоятельная реализация студентами изучаемых задач в аудитории, выполнение домашнего задания по изучаемой теме.

Тема 3. Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус»

Основные компоненты отечественного алгоритма электронной цифровой подписи «Нотариус». Состав библиотеки программ и основных включенных алгоритмов в рамках данного механизма цифровой подписи.

Цель занятия. Освоить основные методы и способы практической реализации отечественного алгоритма электронной цифровой подписи «Нотариус».

Задачи закрепления теоретических знаний и практических умений и навыков: студент должен знать основные понятия и практические приемы для создания отечественного алгоритма электронной цифровой подписи «Нотариус».

Форма проведения: изучение основных компонентов рассматриваемого алгоритма на аудиторных занятиях, самостоятельная реализация студентами изучаемых задач в аудитории, выполнение домашнего задания по изучаемой теме.

Тема 4. Изучение стеганографического метода защиты информации от несанкционированного доступа

Основные понятия и определения стеганографии, понятие стеганографическая система или стегосистема. Практическое применение методов стеганографии. Алгоритмы стеганографии. Методы стеганографии. Виды атак на стегосистемы.

Цель занятия. Освоить методы и приемы стеганографической защиты информации от несанкционированного доступа, требования к стегосистеме, основные этапы компьютерной стеганографии. Приобрести навыки стеганографического сокрытия текстовой информации. Программная реализация метода сокрытия текстовой информации на базе алгоритма LSB. Получить навыки стеганографического сокрытия информации с использованием битов цветовой палитры изображений.

Задачи закрепления теоретических знаний и практических умений и навыков: студент должен знать основные методы и приемы стеганографической защиты информации от несанкционированного доступа, требования к стегосистеме, основные этапы компьютерной стеганографии, уметь применять их для целей программной реализации сокрытия текстовой информации на базе стеганографических алгоритма.

Форма проведения: анализ проблем защиты информации методами стеганографии, анализ существующих алгоритмов программной реализации данных методов на аудиторных занятиях, самостоятельная программная реализация домашнего задания по изучаемой теме.

2. Контрольные вопросы текущего контроля на практических занятиях и при защите лабораторных работ

1. Базовые понятия дисциплины «Информационная безопасность»
2. Дайте определение понятия «Информационная безопасность».
3. Дайте определение понятия «Защита информации».
4. Дайте определение понятия «Информация» с точки зрения информационной безопасности.
5. Назовите свойства информации, наиболее значимые с точки зрения информационной безопасности.
6. Чем определяется уровень (степень) секретности информации или документа?
7. Что такое количественная характеристика информации, какие методы определения данной характеристики существуют?
8. Чем характеризуются прагматические свойства информации?
9. Дайте определение понятия «Информационная система».
10. Что понимают под информационным процессом?
11. Чем характеризуются информационные системы?
12. Что такое обработка информации в информационных системах?
13. Что такое физическая структура информационной системы?
14. Что такое логическая структура информационной системы?
15. Что такое топологическая структура информационной системы?
16. Что такое конфигурация информационной системы?
17. Что такое архитектура информационной системы?
18. Что такое информационный узел?
19. Что такое ресурсы информационной системы?
20. Кто считается пользователем информационной системы?
21. Какими критериями можно оценить качество информационной системы?
22. Что относится к средствам обеспечения информационных систем и их технологий?

23. Дайте характеристику распределённых информационных систем.
24. Какой структурный компонент системы понимается под объектом защиты?
25. Какой структурный компонент системы является элементом защиты?
26. Перечислите характеристики, влияющие на безопасность информации в информационной системе?
27. Дайте определение понятия «Угроза безопасности».
28. Дайте определение понятия «Уязвимость информации».
29. Что такое атака на информационную систему?
30. Что такое утечка информации?
31. Что такое разглашение информации?
32. Что такое несанкционированный доступ?
33. Дайте определение понятия «Политика безопасности»?
34. Какую угрозу информации представляют собой хакеры.
35. Что такое бесконтрольный уход информации?
36. Что такое канал утечки?
37. Назовите виды каналов утечки?
38. Назовите классификационные признаки угроз безопасности.
39. Какие виды угроз считаются умышленными, а какие непреднамеренными?
40. Что такое активные и пассивные угрозы?
41. Перечислите пути несанкционированного доступа к информации.
42. В чем особенности угроз и уязвимостей корпоративных сетей?
43. Перечислите виды атак в IP-сетях.
44. Перечислите наиболее общие проблемы безопасности информационных систем.
45. Перечислите основные группы методов и средств защиты информации.
46. Что входит в понятие комплексной защиты информации?
47. На какие виды подразделяются средства защиты информации?
48. Перечислите основные средства защиты информации.
49. Перечислите основные методы защиты информации.
50. Перечислите основные механизмы защиты информации.
51. Поясните содержание подходов к обеспечению безопасности информации и ин формационных систем, изложенные в межгосударственных стандартах информационной безопасности.

3. Типовые контрольные задания итогового контроля при поведении лабораторных работ

Задание 1.

Изучение методов криптографической защиты информации с использованием шифров перестановки.

1. ***Шифр маршрутной перестановки***
2. ***Шифр перестановки «Сцитала»***
3. ***Шифр «Поворотная решетка»***
4. ***Шифр вертикальной перестановки***
5. ***Шифр на основе магических квадратов***

Варианты заданий

Для нечетных вариантов (1,3,…,25) предлагается реализовать процедуру шифрования, для четных (2,4,…,26) – дешифрования с использованием указанных методов. Ключ, используемый при шифровании, определите самостоятельно.

1-2. Исходную последовательность разбейте на группы по 4 символа. В каждой группе символы переставьте с использованием подстановки, выбираемой самостоятельно.

3-4. Исходную последовательность разбейте на группы по 4 символа. Реализуйте двойную перестановку каждой последовательности символов.

5-6. Исходную последовательность разбейте на группы по 8 символов. Реализуйте шифрование методом перестановки по заданному ключу, при этом четные группы символов шифровать в исходном направлении, нечетные – в обратном.

7-8. Исходную последовательность разбейте на группы по 8 символов. В каждой группе символы переставьте с использованием подстановки, выбираемой самостоятельно.

9-10. Исходную последовательность разбейте на группы по 8 символов. Реализуйте двойную перестановку каждой группы символов, начиная с последнего.

11-12. Исходную последовательность разбейте на группы по 8 символов. Реализуйте шифрование методом перестановки по заданному ключу, при этом нечетные группы шифровать в исходном направлении, четные – в обратном.

13-14. Реализуйте маршрутную перестановку с использованием шифрующей таблицы 6x4. Маршрут: по горизонтали, начиная с левого верхнего угла, поочередно слева направо и справа налево.

15-16. Реализуйте маршрутную перестановку с использованием шифрующей таблицы 6x4. Маршрут: по вертикали, начиная с левого верхнего угла, поочередно сверху вниз и снизу-вверх.

17-18. Зашифруйте исходное сообщение поворотной решеткой размером 6x5. Выполните поворот по часовой стрелке. Решетку выберите самостоятельно.

19-20. Реализуйте процедуру, моделирующую использование «Сцитала». Число столбцов шифрующей таблицы выберите самостоятельно.

21-22. Зашифруйте исходное сообщение поворотной решеткой размером 5x8. Выполните поворот против часовой стрелки. Решетку выберите самостоятельно.

23-24. Реализуйте шифрование вертикальной перестановкой. Основа ключа – ваше собственное имя.

25-26. Смоделируйте использование магических квадратов. Размерность квадратов больше 3.

Задание 2.

Изучение методов криптографической защиты информации с использованием шифров замены.

1. ***Шифр простой замены***
2. ***Шифр Цезаря***
3. ***Шифр «Аффинная система подстановок Цезаря»***
4. ***Шифр лозунговый***
5. ***Шифр «Полибианский квадрат»***
6. ***Шифрующая таблица Трисемуса***
7. ***Шифр биграммный Плейфера***
8. ***Шифрующая система омофонов***

Задание 3.

Изучение методов криптографической защиты информации с использованием шифров сложной замены.

1. Шифр Гронсфельда

2. Система шифрования Вижинера

3. Шифр Вижинера с автоключом

4. Шифр Вижинера с перемешанным алфавитом

5. Двойной квадрат Уитстона

Варианты заданий

Для нечетных вариантов (1,3,…, 25) предлагается реализовать процедуру шифрования файлов, для четных (2,4,…, 26) – дешифрования с использованием указанных методов. Если ключ, используемый при шифровании, не указан, задайте его самостоятельно.

1-2. Зашифровать исходное сообщение с использованием системы шифрования Цезаря.

3-4. Зашифровать исходное сообщение, используя аффинную систему подстановок Цезаря при A=12, B=7.

5-6. Зашифровать исходное сообщение с использованием Полибианского квадрата. Заполнение таблицы размером 8x4 буквами алфавита реализовать в следующем порядке: сначала нечетные столбцы, затем – четные.

7-8. Зашифровать исходное сообщение с использованием лозунгового шифра. В качестве ключа использовать свое имя или фамилию.

9-10. Зашифровать исходное сообщение с использованием Полибианского квадрата. Заполнение таблицы размером 8x4 буквами алфавита реализовать в следующем порядке: по вертикали, начиная с левого верхнего угла сверху вниз и снизу-вверх.

11-12. Зашифровать исходное сообщение с использованием шифра Гронсфельда. В качестве ключа использовать группу из 5 цифр.

13-14. Зашифровать исходное сообщение используя аффинную систему подстановок Цезаря при A=13, B=5.

15-16. Зашифровать исходное сообщение с использованием шифрующей таблицы Трисемуса.

17-18. Зашифровать исходное сообщение с использованием биграммного шифра Плейфера.

19-20. Зашифровать исходное сообщение с использованием системы омофонов.

21-22. Зашифровать исходное сообщение с использованием системы шифрования «Двойной квадрат Уитстона».

23-24. Зашифровать исходное сообщение с использованием системы шифрования Вижинера.

25-26. Зашифровать исходное сообщение с использованием системы шифрования Вижинера с автоключом.

Задание 4.

Изучение методов криптографической защиты информации путем проверки правильности ключа

,,

Выполнить любую из лабораторных работ по криптографии, добавив проверку правильности ключа одним из предлагаемых методов.

1-2. Для проверки добавлять пароль в начало зашифрованного файла.

3-4. Выполнить шифрование пароля с использованием того же алгоритма, что и для основного файла. В качестве ключа взять константу.

5-6. Выполнить шифрование пароля самого на себя.

7-8. Выполнить шифрование константной строки.

9-10. Для проверки добавлять пароль в конец зашифрованного файла.

11-12. Выполнить шифрование пароля с использованием того же алгоритма, что и для основного файла. В качестве ключа взять цифры своего года рождения.

13-14. Выполнить шифрование константной строки «Москва столица нашей Родины».

15-16. Для проверки добавлять пароль в конец первой строки зашифрованного файла.

17-18. Выполнить шифрование пароля самого на себя. Поместить его в конец зашифрованного файла.

19-20. Выполнить шифрование константной строки. Поместить константную строку в конец зашифрованного файла.

21-22. Выполнить шифрование пароля с использованием того же алгоритма, что и основной файл. В качестве ключа взять свой номер телефона.

23-24. Выполнить шифрование константной строки, содержащей ваши фамилию, имя и отчество.

25-26. Для проверки добавлять пароль в конец второй строки зашифрованного файла.

4. Типовые задания для самостоятельной работы. Темы рефератов для подготовки выступлений и коллективной дискуссии

1. Проблемы защиты информационной системы. Защита для открытых информационных систем.
2. Характеристики, влияющие на безопасность информации.
3. Возможности сети Интернет и проблемы безопасности.
4. Угрозы и уязвимости корпоративных сетей и систем.
5. Задачи обеспечения информационной безопасности сетей.
6. Политика безопасности в сетях.
7. Технологии безопасности данных.
8. Использование комбинированной криптосистемы.
9. Строгая аутентификация.
10. Протокол Kerberos.
11. Биометрическая аутентификация.
12. Типовые решения по применению межсетевых экранов для защиты информационных ресурсов.
13. Классификация сетей VPN.
14. Управление сетевой безопасностью.
15. Глобальная и локальная политики безопасности.
16. Законодательный уровень информационной безопасности.
17. Анализ текущего состояния российского законодательства в области информационной безопасности.
18. Методы управления средствами сетевой безопасностью.
19. Задачи управления системой информационной безопасности предприятия.
20. Концепция глобального управления безопасностью.
21. Освоение приемов противодействия разрушающим программным средствам.
22. Основные принципы работы с электронной цифровой подписью.
23. Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус».
24. Изучение стеганографического метода защиты информации от несанкционированного доступа.

5. Темы для самостоятельной работы

Тема 1. Проблемы защиты информационной системы. Защита для открытых информационных систем.
Тема 2. Характеристики, влияющие на безопасность информации.
Тема 3. Возможности сети Интернет и проблемы безопасности.
Тема 4. Угрозы и уязвимости корпоративных сетей и систем.
Тема 5. Задачи обеспечения информационной безопасности сетей.
Тема 6. Политика безопасности в сетях.
Тема 7. Технологии безопасности данных.
Тема 8. Использование комбинированной криптосистемы.
Тема 9. Строгая аутентификация.
Тема 10. Протокол Kerberos. (
Тема 11. Биометрическая аутентификация.
Тема 12. Типовые решения по применению межсетевых экранов для защиты информационных ресурсов.
Тема 13. Классификация сетей VPN.
Тема 14. Управление сетевой безопасностью.
Тема 15. Законодательный уровень информационной безопасности
Тема 16. Анализ текущего состояния российского законодательства в области информационной безопасности.
Тема 17. Методы управления средствами сетевой безопасностью
Тема 19. Задачи управления системой информационной безопасности предприятия
Тема 21. Освоение приемов противодействия разрушающим программным средствам.
Тема 22. Основные принципы работы с электронной цифровой подписью.
Тема 23. Основные принципы работы алгоритма отечественной цифровой подписи «Нотариус»

6. Вопросы итогового контроля (к зачету) по дисциплине

1. Введение. Сценарий безопасной работы информационной системы.
2. Все определения понятия «Информационная безопасность».
3. Составляющие информационной безопасности (ИБ).
4. Понятие предмета защиты.
5. Понятие объекта защиты.
6. Понятие комплексной системы защиты.
7. Системно-концептуальный подход к построению систем защиты.
8. Методы и средства построения ИБ. Их структура.
9. Виды собственного ПО системы ИБ.
10. Методы и средства обеспечения ИБ.
11. Основные средства защиты.
12. Методы, составляющие основу механизмов защиты.
13. Основные механизмы защиты.
14. Основные средства защиты от НСД.
15. Инженерно-технические средства защиты.
16. Методы и средства защиты от утечки по каналам ПЭМИН.
17. Методы и средства организационной защиты.

18. Основные понятия теории информационной безопасности.
19. Понятие информации как предмета защиты
20. Понятие информационного сервиса безопасности.
21. Свойства информации.
22. Законодательная база в сфере ИБ.
23. Статьи УК РФ в области ИБ.
24. Нормативно-правовые основы ИБ РФ.
25. Понятие тайны, виды тайн.
26. Понятие и свойства защищенной системы.
27. Информационные системы как объект защиты
28. Характеристики, влияющие на безопасность информации в информационной системе
29. Структура и состав основных компонентов информационных систем
30. Общие подходы к защите информации и информационных систем
31. Роль стандартов ИБ.
32. Международные стандарты ИБ.
33. Отечественные стандарты ИБ.
34. Особенности угроз в IP-сетях.
35. Основные виды угроз информационной безопасности.
36. Классификация угроз информационной безопасности.
37. Атаки на сеть. Сценарий проведения атак.
38. Виды атак, в IP-сетях
39. Понятие несанкционированного доступа к информации (НСД).
40. Виды НСД.
41. Основные виды разрушающих программных средств.
42. Каналы утечки информации. Технические каналы утечки информации.
43. Механизмов аутентификации и идентификации.
44. Функции и назначение межсетевых экранов.
45. Требования к межсетевым экранам.
46. Классификация межсетевых экранов.
47. Механизмы построения виртуальных защищенных сетей (VPN-технологии).
48. Защита интернет – подключений.
49. Защита системы электронной почты.
50. Разрушающие программные средства.
51. Вирусы. Основные понятия.
52. Классификация вирусов.
53. Криптография. Основные понятия.
54. Современные алгоритмы криптографии.
55. Понятие абсолютно стойкого шифра.
56. Классификация криптографических алгоритмов.
57. Понятие криптографии с открытым ключом.
58. Понятие электронной цифровой подписи (ЭЦП)
59. Понятие хэш-функции.
60. Основные алгоритмы ЭЦП, их различия.

7. Список литературы приведён в тексте рабочей программы по дисциплине «Защита информации»