Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ И АЛГОРИТМЫ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»

Для студентов специалитета по специальности 10.05.03
очной формы обучения

Ульяновск, 2021

Методические указания для самостоятельной работы студентов по дисциплине «Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2021. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса, вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к зачёту и экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/21 от 16 марта 2021 г.).

Оглавление

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ 4
СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 5
МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ 7
Лабораторная работа 1. Простые числа 7
Лабораторная работа 2. Факторизация целых чисел 7
Лабораторная работа 3. Анализ рисков информационной безопасности 7
Лабораторная работа 4. Построение концепции информационной безопасности предприятия 9
Лабораторная работа 5. Процедура аутентификации пользователя на основе пароля 11
Лабораторная работа 6. Программная реализация криптографических алгоритмов 16
Лабораторная работа 7. Механизмы контроля целостности данных 22
Лабораторная работа 8. Алгоритмы поведения вирусных и других вредоносных программ 25
Лабораторная работа 9. Алгоритмы предупреждения и обнаружения вирусных угроз 31
Лабораторная работа 10. Пакеты антивирусных программ 37
Лабораторная работа 11. Построение VPN на базе программного обеспечения 38
МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ 40

СПИСОК РЕКОМЕНДОВАННОЙ ЛИТЕРАТУРЫ

1. Щеглов, А. Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / А. Ю. Щеглов, К. А. Щеглов. — Санкт-Петербург : Университет ИТМО, 2015. — 93 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/67260.html — Режим доступа: для авторизир. пользователей
2. Дискретная математика: прикладные задачи и сложность алгоритмов : учебник и практикум для вузов / А. Е. Андреев, А. А. Болотов, К. В. Коляда, А. Б. Фролов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 317 с. — (Высшее образование). — ISBN 978-5-534-04246-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/468282
3. Крупский, В. Н. Теория алгоритмов. Введение в сложность вычислений : учебное пособие для вузов / В. Н. Крупский. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 117 с. — (Высшее образование). — ISBN 978-5-534-04817-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/473006
4. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / Щеглов А.Ю., Щеглов К.А.. — Санкт-Петербург : Университет ИТМО, 2015. — 93 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/67260.html — Режим доступа: для авторизир. пользователей
5. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов [и др.].. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 с. — ISBN 978-5-8265-1737-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85968.html — Режим доступа: для авторизир. пользователей
6. Пушкарев В.П. Защита информационных процессов в компьютерных системах : учебное пособие / Пушкарев В.П., Пушкарев В.В.. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/13929.html — Режим доступа: для авторизир. пользователей.
7. Журавлев, Ю. И. Дискретный анализ. Формальные системы и алгоритмы : учебное пособие для вузов / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 318 с. — (Высшее образование). — ISBN 978-5-534-06279-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470982
8. Пашинцев, В. П. Нестандартные методы защиты информации : лабораторный практикум / В. П. Пашинцев, А. В. Ляхов. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 196 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/63217.html — Режим доступа: для авторизир. пользователей.
9. Котова, Л. В. Сборник задач по дисциплине «Методы и средства защиты информации» : учебное пособие / Л. В. Котова. — Москва : Московский педагогический государственный университет, 2015. — 44 с. — ISBN 978-5-4263-0221-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/70020.html — Режим доступа: для

авторизир. Пользователей
10. Бондаренко, И. С. Методы и средства защиты информации : лабораторный практикум / И. С. Бондаренко, Ю. В. Демчишин. — Москва : Издательский Дом МИСиС, 2018. — 32 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/84413.html — Режим доступа: для авторизир. пользователей
11. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети / составители Д. В. Костин. — Москва: Московский технический университет связи и информатики, 2016. — 42 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/61546.html — Режим доступа: для авторизир. пользователей
12. http://www.securitylab.ru – российский портал по компьютерной безопасности.
13. http://www.pgpru.com – русскоязычный сайт, посвященный криптографическому стандарту PGP.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Теоретико-числовые алгоритмы в криптологии

Тема 1. Теория алгоритмов. Частично рекурсивные функции и их вычислимость

Типы алгоритмических моделей. Машина произвольного доступа и вычислимые функции. Тезис Черча для машины произвольного доступа.

Рекурсия как метод определения арифметических функций. Класс частично рекурсивных функций. Базисные функции. Операции над функциями.

Общерекурсивные и примитивно-рекурсивные функции. Тезис Черча для частично-рекурсивных функций. Способы доказательства вычислимости функций.

Теорема о вычислимости суперпозиции. Теорема о вычислимости рекурсии. Теорема о вычислимости минимизации. Теорема о частичной рекурсивности функций, вычислимых на машине произвольного доступа. Алгоритмически неразрешимые проблемы.

Тема 2. Сложность вычислений

Характеристики сложности вычислений: временная и емкостная сложность.

Классы сложности P и NP и их взаимосвязь. Понятие недетерминированной машины Тьюринга. Полиномиальная сводимость задач. NP-полные и NP-трудные задачи. Формулировка теоремы Кука.

Тема 3. Тестирование чисел на простоту и построение больших простых чисел

Простое число. Каноническое разложение натурального числа. Методы проверки простоты чисел. Метод пробных делений. Решето Эратосфена. Тест на основе малой теоремы Ферма. Тесты на простоту для чисел специального вида. Числа Мерсенна. ($N\pm1$)-методы проверки простоты чисел и построения больших простых чисел. Алгоритм Конягина – Померанса. Вероятностные тесты на простоту. Тест Соловея – Штрассена. Тест Рабина – Миллера. Современные методы проверки простоты чисел.

Тема 4. Факторизация целых чисел с экспоненциальной сложностью

Понятие факторизации целых чисел. Алгоритм Ферма. (P-1)-метод Полларда и оценка его сложности. ρ-метод Полларда. Метод Шермана – Лемана. Алгоритм Ленстры. Алгоритм Полларда – Штрассена.

Тема 5. Факторизация целых чисел с субэкспоненциальной сложностью

Алгоритм Диксона. Стратегия LP и использование больших простых чисел. Стратегия PS и алгоритм Полларда – Штрассена. Стратегия EAS – стратегия раннего обрыва.

Квадратичное решето. Субэкспоненциальные вероятностныеалгоритмы. Методы Шнорра – Ленстры и Ленстры – Померанса. Алгоритмы решета числового поля.

Тема 6. Алгоритмы дискретного логарифмирования

Задача дискретного логарифмирования. Алгоритм согласования. Алгоритм Полига – Хеллмана. ρ-метод Полларда для дискретного логарифмирования.

Дискретное логарифмирование в простых полях. Дискретное логарифмирование в полях Галуа. Дискретное логарифмирование и решето числового поля.

Раздел 2. Угрозы информации

Тема 7. Информационная безопасность сетей.

Информационная безопасность вусловиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.

Тема 8. Способы совершения компьютерных преступлений

Тема 9. Уязвимость сети Интернет

Пользователи и злоумышленники в сети Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

Раздел 3. Виды возможных нарушений безопасности информационной системы

Тема 10. Компьютерные преступления

Классификация компьютерных преступлений. Виды противников или «нарушителей».

Тема 11. Вредоносные программы

Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

Раздел 4. Информационная безопасность информационных систем

Тема 12. Модели информационной безопасности информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 13. 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.

Тема 14. Организация информационной безопасности компании

Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

Тема 15. Обеспечение информационной безопасности

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контрольдоступа к аппаратуре.

Раздел 5. Методы и средства защитыкомпьютерной информации

Тема 16. Контроль доступа к информации

Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

Тема 17. 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.

Тема 18. Антивирусное ПО

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

Цель. Лабораторный практикум по дисциплине направлен на изучение студентами современных подходов для обеспечения информационной безопасности всех видов современных информационных систем.

Методология основывается на самостоятельном обучении студентов решению стандартных задач на основе технической документации, теоретического материала. Поиск технической информации, а также подбор необходимого решения производится самостоятельно студентами в открытых источниках и контролируется в ходе лабораторных занятий и в процессе демонстрации полученного решения.

В методических указаниях не определен язык, а также среда программирования, в которой студенты должны выполнять работу. Выбор остается за студентом.

Лабораторная работа 1. Простые числа

Реализация алгоритма построения таблицы простых чисел.
Реализация теста Соловея–Штрассена).
Реализация теста Миллера–Рабина).
Реализация алгоритма Люка для доказательства простоты.
Реализация алгоритма вычисления последовательностей Люка.
Реализация алгоритма построения простого числа.
Реализация алгоритма построения сильно простого числа.

Лабораторная работа 2. Факторизация целых чисел

Реализация алгоритма факторизации Ферма.
Реализация алгоритма вычисления целозначного квадратного корня.
Реализация алгоритма Лемана.
Реализация метода Полларда-Флойда.
Реализация алгоритма Брента.
Реализация p–1 алгоритма факторизации Вильямса.
Реализация p+1 алгоритма факторизации Вильямса.

Лабораторные работы 1 и 2 выполняются самостоятельно

Лабораторная работа 3. Анализ рисков информационной безопасности

1. Цель работы

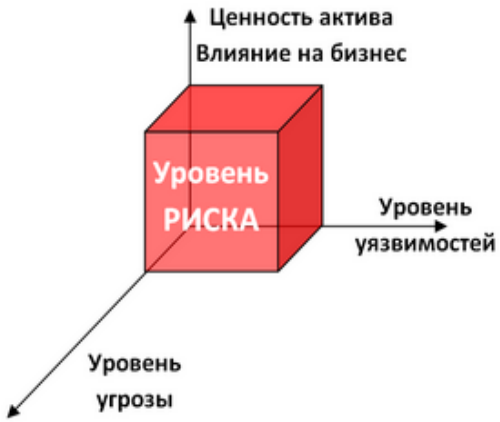
Ознакомиться с алгоритмами оценки риска информационной безопасности.

2. Краткие теоретические сведения

Риск ИБ – потенциальная возможность использования определенной ***угрозой уязвимостей актива*** или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза ИБ - совокупность условий и факторов, которые могут стать причиной нарушений



целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

3. Задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь **Приложением C** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении E** ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ
8. Оценка рисков
9. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	Организация	Метод оценки риска (см. Приложение E ГОСТа)
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3

12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Лабораторная работа 4. Построение концепции информационной безопасности предприятия

1. Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

2. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – **Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты

(приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

4.5. Программа создания системы информационной безопасности Предприятия

5. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

6. Варианты

Вариант – номер по списку в журнале.

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Лабораторная работа 5. Процедура аутентификации пользователя на основе пароля

1. Цель работы

Изучение технологии аутентификации пользователя на основе пароля.

2. Краткие теоретические сведения

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности

проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

3. Задание

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:

1. В качестве информационного ресурса использовать любой файл или приложение.

Для справки: работа с текстовым файлом в среде Delphi:

```
var
  myFile : TextFile;
  text   : string;

begin
  // Попытка открыть файл Test.txt для записи
  AssignFile(myFile, 'Test.txt');
  ReWrite(myFile);

  // Запись нескольких известных слов в этот файл
  WriteLn(myFile, 'Hello');
  WriteLn(myFile, 'World');

  // Закрытие файла
  CloseFile(myFile);

  // Открытие файла в режиме только для чтения
  FileMode := fmOpenRead;
  Reset(myFile);

  // Показ содержимого файла
  while not Eof(myFile) do
  begin
    ReadLn(myFile, text);
    ShowMessage(text);
  end;

  // Закрытие файла в последний раз
  CloseFile(myFile);
end;
```

2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.

Для справки: Пример поиска элемента в массиве (Delphi):

```
// ввод массива for i:=l to SIZE do
a[i] := StrToInt(StringGridl.Cells[i - 1, 0]);
// ввод образца для поиска
obr := StrToInt(edit2.text);
// поиск
found := FALSE; // пусть нужного элемента в массиве нет
i := 1;
repeat
  if a[i] = obr then
    found := TRUE
  else
    i := i + 1;
until (i > SIZE) or (found = TRUE);
```

3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.

4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Текст программы
5. Пример работы программы
6. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	Длина пароля (количество символов)	Используемые символы	Дополнительные средства защиты
1	6	Латиница (строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.
2	7	Кириллица (строчные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
3	8	Цифры	Применение метода аутентификации на основе одноразовых паролей: каждый следующий пароль=предыдущий пароль+5
4	5	Цифры+ знаки арифметических операций	При смене пароля: проверка на отсутствие повторяющихся символов.
5	8	Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя

			(храниться в системе) в формате дд.мм.гг или дд/мм/гг
6	10	Латиница (прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: при каждой следующей попытке входа в систему последняя буква пароля меняется на следующую по алфавиту.
7	11	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с фамилией пользователя (если используется идентификационный номер, то в системе должны храниться имена каждого пользователя)
8	10	Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с датой рождения пользователя (храниться в системе) в формате дд.мм.гггг или дд/мм/гггг
9	7	Цифры	Применение метода аутентификации на основе одноразовых паролей: к первой цифре каждого следующего пароля прибавляется 1.
10	8	Кириллица (прописные и строчные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.
11	5	Латиница (строчные и прописные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля к нему добавляется «случайная» величина, такая же величина добавляется к паролю, который хранится в системе, после чего производится сравнение.(в качестве «случайной» величины использовать «Abc»)
12	9	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с отчеством пользователя.
13	10	Цифры	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: xxxxxxxxxx.
14	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий месяцев).
15	6	Латиница (строчные и прописные буквы)	При смене пароля: проверка на отсутствие повторяющихся символов.
16	7	Кириллица (строчные буквы)	Применение метода аутентификации на основе одноразовых паролей: после ввода пользователем пароля в его начало добавляется «случайная» величина, такая

			же величина добавляется к паролю, который хранится в системе, после чего производится сравнение (в качестве «случайной» величины использовать «АБВ»)
17	4	Цифры	При смене пароля: проверка на совпадение пароля с годом рождения пользователя
18	5	Цифры	Применение односторонней (хэш) функции: сложение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей.
19	9	Кириллица (строчные буквы)	Шифрование пароля (В качестве алгоритма шифрования применить метод перестановки: поменять местами первую и последнюю букву пароля) Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей.
20	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с местом рождения пользователя.
21	13	Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с номером телефона пользователя в формате: ххх-ххх-хх-хх
22	6	Латиница (строчные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив названий дней недели).
23	7	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля с именем пользователя, записанным в обратном порядке.
24	8	Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гг или дд/мм/гг
25	5	Цифры	Применение односторонней (хэш) функции: перемножение всех цифр пароля. Такая же функция должна быть применена к паролю, который хранится в системе. Затем проводится сравнение паролей.
26	6	Цифры	Шифрование пароля (В качестве алгоритма шифрования применить метод замены:к каждой цифре пароля прибавить по цифре из даты рождения пользователя соответственно) Тот же алгоритм должен быть применен к паролю, который хранится в системе. Затем проводится сравнение паролей.

27	10	Кириллица (прописные буквы)	При смене пароля: проверка на совпадение пароля со словами в словаре (в качестве словаря использовать массив из любых 10 слов, длиной в 10 символов).
28	4	Кириллица (строчные и прописные буквы)	При смене пароля: проверка на совпадение пароля с месяцем рождения пользователя
29	10	Цифры+ знаки препинания	При смене пароля: проверка на совпадение пароля с текущей датой в формате дд.мм.гггг или дд/мм/гггг
30	9	Цифры	При смене пароля: проверка на отсутствие повторяющихся символов.

Лабораторная работа 6. Программная реализация криптографических алгоритмов

1. Цель работы

Знакомство с основными методами криптографической зашиты информации.

2. Краткие теоретические сведения

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой

криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-

250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i=Г(ш)_i+Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y= G^x \bmod P$.
4. Получатель выбирает целое число K, 1< K< P-1.
5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.
2. Получатель выбирает целое число e ($1<e< \varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

3. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1 (\bmod \varphi(n))$.

Пара чисел **(d,n)** является **секретным ключом**.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod (n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod (n)}$.

3. Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).
2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Применение алгоритма симметричного шифрования
5. Применение алгоритма асимметричного шифрования

4.1. Программа шифрования и дешифрования сообщения при помощи алгоритма RSA

4.2. Результаты шифрования и дешифрования заданных сообщений

5. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	**Исходные данные**							
	Часть 1	**Часть 2**						
	Алгоритм шифрования	**p**	**q**	**e**	**d**	**m_1**	**m_2**	**m_3**
1	Простая перестановка	3	11	7	3	9	12	23
3	Одиночная перестановка	17	11	7	23	8	15	45
3	Двойная перестановка	13	7	5	29	3	16	55
4	Магический квадрат	101	113	3533	6597	6	19	23
5	Шифр Цезаря	7	11	37	13	8	18	51
6	Полибианский квадрат	7	17	5	77	9	11	86
7	Шифр Гронсфельда	3	11	7	3	8	13	25
8	Многоалфавитная замена	17	11	7	23	7	14	47
9	Простая перестановка	13	7	5	29	2	17	55
10	Одиночная перестановка	17	11	7	23	3	20	51
11	Двойная перестановка	13	7	5	29	2	12	15
12	Магический квадрат	101	113	3533	6597	3	15	86
13	Шифр Цезаря	7	11	37	13	3	16	54
14	Полибианский квадрат	7	17	5	77	3	19	36
15	Шифр Гронсфельда	3	11	7	3	4	18	25
16	Многоалфавитная замена	17	11	7	23	5	11	64
17	Простая перестановка	101	113	3533	6597	4	13	91

18	Одиночная перестановка	7	11	37	13	7	14	34
19	Двойная перестановка	7	17	5	77	7	17	73
20	Магический квадрат	3	11	7	3	5	20	23
21	Шифр Цезаря	17	11	7	23	2	11	85
22	Полибианский квадрат	13	7	5	29	3	13	57
23	Шифр Гронсфельда	17	11	7	23	2	14	59
24	Многоалфавитная замена	13	7	5	29	5	17	56
25	Простая перестановка	101	113	3533	6597	6	20	92
26	Одиночная перестановка	7	11	37	13	5	14	76
27	Двойная перестановка	7	17	5	77	4	17	64
28	Магический квадрат	3	11	7	3	8	20	32
29	Одиночная перестановка	7	17	5	77	4	13	91
30	Шифр Гронсфельда	13	7	5	29	9	11	58

Лабораторная работа 7. Механизмы контроля целостности данных

1. Цель работы

Изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

2. Теоретические сведения

В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумышленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭЦП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭЦП использует секретный ключ отправителя сообщения, а процедура проверки ЭЦП – открытый ключ отправителя сообщения (рис. 1). Здесь

M – электронный документ, E – электронно-цифровая подпись.

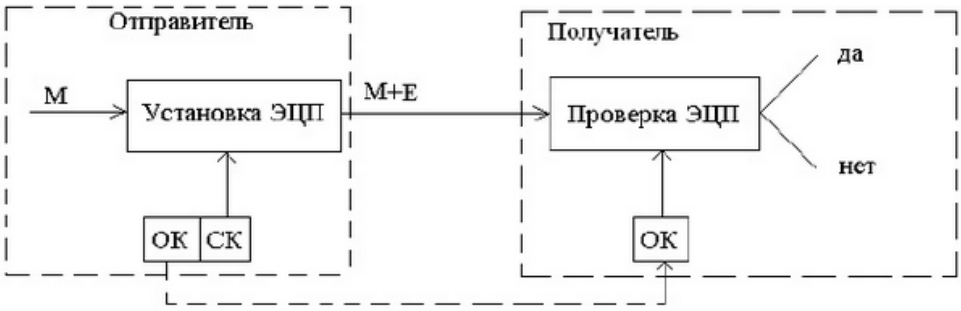


Рис. 1 – Схема использования ЭЦП

В технологии ЭЦП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

Схема установки ЭЦП (рис. 2):

1. Для документа M формируется дайджест H с помощью заданного алгоритма хэширования.

2. Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭЦП.

3. Сообщение M и его ЭЦП передаются получателю сообщения.

Рис. 2 – Схема установки ЭЦП.

Схема проверки ЭЦП (рис. 3):

1. Получатель для проверки ЭЦП должен иметь доступ к самому сообщению M и его ЭЦП.

2. Зная алгоритм хэширования, который был использован при установке ЭЦП, получатель получает дайджест H1 присланного сообщения M.

3. Зная открытый ключ отправителя, получатель дешифрует ЭЦП, в результате чего получает дайджест H2, сформированный на этапе установки ЭЦП.

4. Критерием целостности присланного сообщения M и подтверждения его автора является совпадение дайджестов H1 и H2. Если это равенство не выполнено, то принимается решение о некорректности ЭЦП.

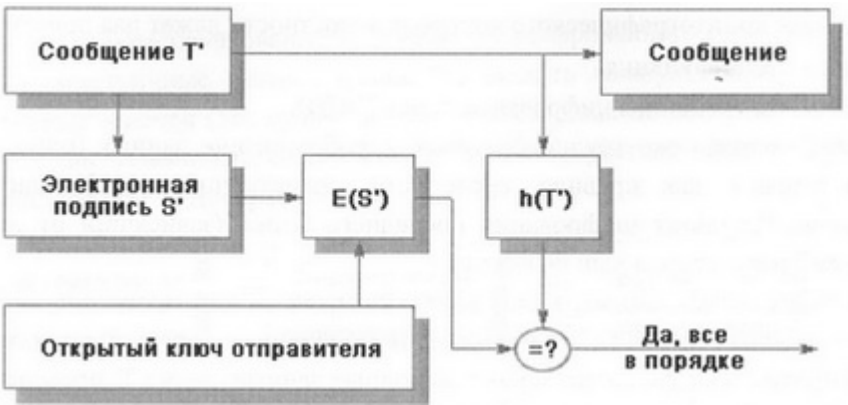


Рис. 3 – Схема проверки ЭЦП.

3. Задание

Сформировать ЭЦП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.

Порядок выполнения работы:

1. Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.
2. На стороне отправителя выполнить следующие действия:

2.1. Записать сообщение M (см. вариант).

2.2. Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.

2.3. Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).

3. На стороне получателя выполнить следующие действия:

3.1. Записать сообщение M (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).

3.2. Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).

3.3. Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (e, n) см. в таблице с вариантами задания).

3.4 Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Лист расчета и проверки ЭЦП
5. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	p	q	e	d	M
1	3	11	7	3	5523
3	17	11	7	23	8866
3	13	7	5	29	3565
4	101	113	3533	6597	6546
5	3	11	7	3	8562
6	17	11	7	23	9795
7	13	7	5	29	8462
8	17	11	7	23	7785
9	13	7	5	29	2123
10	101	113	3533	6597	3145
11	7	11	37	13	2566
12	101	113	3533	6597	3782

13	3	11	7	3	3465
14	17	11	7	23	3895
15	13	7	5	29	4132
16	17	11	7	23	5123
17	13	7	5	29	4416
18	101	113	3533	6597	7895
19	3	11	7	3	7459
20	17	11	7	23	5654
21	13	7	5	29	2456
22	17	11	7	23	3585
23	13	7	5	29	2652
24	101	113	3533	6597	5656
25	3	11	7	3	6685
26	17	11	7	23	5566
27	13	7	5	29	4652
28	17	11	7	23	8666
29	13	7	5	29	4556
30	101	113	3533	6597	9266

Лабораторная работа 8. Алгоритмы поведения вирусных и других вредоносных программ

1. Цель работы

Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.

2. Краткие теоретические сведения

Исторически первое определение компьютерного вируса было дано в 1984 г. Фредом Коэном: «Компьютерный вирус — это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в этом определении являются *способность вируса к саморазмножению* и *способность к модификации вычислительного процесса*.

В настоящее время под компьютерным вирусом принято понимать программный код, обладающий следующими свойствами:
• способностью к созданию собственных копий, не обязательно совпадающих с оригиналом, но обладающих свойствами оригинала (самовоспроизведение);
• наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Указанные свойства следует дополнить свойствами деструктивности и скрытности действий данной вредоносной программы в вычислительной среде.

Основной и наиболее распространенной классификацией компьютерных вирусов является классификация по *среде обитания*, или по *типам объектов* компьютерной системы, в которые внедряются вирусы. В соответствии с этой классификацией вирусы делятся на файловые, загрузочные, сетевые (черви) и макровирусы.

Существует также много комбинированных типов компьютерных вирусов.

Кроме вирусов принято выделять еще несколько видов вредоносных программ. Это троянские программы, логические бомбы, хакерские утилиты скрытого администрирования удаленных компьютеров, программы, ворующие пароли доступа к

ресурсам Интернет и прочую конфиденциальную информацию. Четкого разделения между ними не существует: троянские программы могут содержать вирусы, в вирусы могут быть встроены логические бомбы и т. д.

3. Задание

Разработать программу имитирующую некоторые (см. вариант) действия вируса или другой вредоносной программы и подготовить отчет о проделанной работе.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Алгоритм работы программы
5. Листинг программы
6. Пример работы программы
7. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Вариант	Действие вирусной или другой вредоносной программы	Задание	Входные данные процедуры	Выходные данные процедуры	Примечание
1	**"Поиск жертвы"**	Разработать и отладить процедуру поиска файлов по заданной маске в текущей папке	Маска файла	Массив имен найденных файлов и их количество	Маска файлов: *.exe
2	**"Подмена файла"**	Разработать и отладить процедуру замены указанного файла на другой указанный файл	Имена двух файлов	Признак успешности замены	Подмена путем удаления файла и использования его имени для изменения имени "вирусного" файла
3	**"Модификация файла"**	Разработать и отладить процедуру записи информации из одного указанного файла в конец другого указанного файла	Имена двух файлов	Преобразованный файл	
4	**"Принцип действия программы-шпиона"**	Разработать процедуру копирования содержимого всех файлов, к которым обращается пользователь в заданный файл	Имя файла	Преобразованный файл	В программе создать форму обращения к нескольким файлам (своеобразный каталог)
5	**"Создание звуковых эффектов"**	Разработать процедуру запуска звукового файла при наступлении какого-либо события (попытка доступа к файлу, каталогу, наступление определенного времени и т. п.)	Имя файла, каталога, заданное время или др.	Запуск звукового файла	Содержимое звукового файла: творческая работа
6	**"Проверка файла на зараженность"**	Разработать и отладить процедуру поиска заданной строки в файле	Имя файла, строка текста	Логическая переменная	

	(вирус не должен заражать уже зараженные файлы)				
7	**"Маскировка "**	Разработать и отладить процедуру запуска указанной программы на выполнение	Имя файла с программой	Логическая переменная	Принцип маскировки: после выполнения заданного алгоритма вирус запускает на выполнение сам файл, чтобы скрыть от пользователя факт заражения
8	**"Маскировка "**	Разработать и отладить процедуру изменения даты и времени создания указанного файла на заданные значения	Имя файла, значения даты, времени	Логическая переменная	
9	**"Маскировка "**	Разработать и отладить процедуру изменения атрибутов и размера указанного файла на заданные значения	Имя файла, значения атрибутов и размера	Логическая переменная	
10	**"Принцип работы логической бомбы"**	Разработать и отладить процедуру удаления содержимого всех файлов в заданном каталоге при наступлении какого-либо времени	Заданное значение времени, имя каталога	Логическая переменная	
11	**"Имитация сбоев ОС и аппаратуры"**	Разработать и отладить процедуру появления сообщений о сбое ОС и/или аппаратуры при попытке доступа к какому-либо файлу (файлам)	Имя файла (файлов)	Появление сообщений о сбое	
12	**"Маскировка "**	Разработать и отладить процедуры шифрования и дешифрования указанного файла	Имя файла	Логическая переменная	
13	**"Принцип работы логической**	Разработать и отладить процедуру запуска некоторой программы при	Заданное значение	Запуск некоторой программы	

	бомбы"	наступлении какого-либо часа или минуты	времени, имя файла		
14	**"Принцип работы баннера"**	Разработать и отладить процедуру запуска баннера при попытке перехода по какой-либо ссылке	Ссылка, баннер	Запуск баннера	Содержание баннера: творческая работа
15	**"Принцип работы логической бомбы"**	Разработать и отладить процедуру удаления всех файлов в заданном каталоге при наступлении какого-либо времени	Заданное значение времени, имя каталога	Логическая переменная	
16	**"Модификация файла"**	Разработать и отладить процедуру записи информации из одного указанного файла в середину другого файла	Имена двух файлов	Преобразованный файл	Место в середине файла должно выбираться случайным образом
17	**"Принцип работы логической бомбы"**	Разработать и отладить процедуру запуска некоторой программы при наступлении какой-либо даты	Дата, имя запускаемого файла	Запуск некоторой программы	
18	**"Жадная программа"**	Разработать и отладить процедуру создания копий заданного файла (файлов) и размещения их в заданном каталоге (каталогах)	Имя файла, количество копий, заданный каталог	Созданные копии	
19	**"Принцип действия клавиатурного шпиона"**	Разработать процедуру записи в заданный файл информации, вводимой пользователем в поля "логин" и "пароль"	Имя файла	Преобразованный файл	За основу взять программу, разработанную при выполнении практической работы № 4
20	**"Принцип работы логической бомбы"**	Разработать и отладить процедуру запуска некоторой программы при наступлении какого-либо дня недели	День недели, имя запускаемого файла	Запуск некоторой программы	
21	**"Поиск жертвы"**	Разработать и отладить процедуру поиска файлов по заданной маске в	Маска файла	Массив имен найденных	Маска файлов: *.bat

		текущей папке.		файлов и их количество	
22	**"Модификация файла"**	Разработать и отладить процедуру перемешивания символов (строк) в файле	Имя файла	Преобразованный файл	
23	**"Маскировка"**	Разработать процедуру подмены зараженного файла незараженным при обращении к нему пользователя	Имя файла	Открытый файл	Для проверки работоспособности программы создать 2 файла: "зараженный" и "незараженный"
24	**"Подмена файла"**	Разработать и отладить процедуру замены указанного файла на другой указанный файл.	Имена двух файлов	Признак успешности замены	Подмена путем замены содержимого файла на содержимое "вирусного" файла
25	**"Жадная программа"**	Разработать и отладить процедуру создания копий заданного каталога (каталогов)	Заданный каталог, количество копий	Созданные копии	
26	**"Проверка файла на зараженность" (вирус не должен заражать уже зараженные файлы)**	Разработать и отладить процедуру проверки следующего факта: является ли содержимое двух файлов одинаковым	Имена двух имеющихся файлов	Логическая переменная	
27	**"Проверка файла на зараженность" (вирус не может заражать сам себя)**	Разработать и отладить процедуру проверки следующего факта: не является ли некоторый файл, заданный своим именем, той программой, которая эту проверку производит (т.е. самой запущенной программой)	Проверяемое имя файла	Логическая переменная	

Лабораторная работа 9. Алгоритмы предупреждения и обнаружения вирусных угроз

1. Цель работы

Знакомство с некоторыми алгоритмами предупреждения и обнаружения вирусных угроз.

2. Краткие теоретические сведения

Для зашиты от компьютерных вирусов и других вредоносных программ могут использоваться:

• общие методы и средства защиты информации;

• специализированные программы для защиты от вирусов;

• профилактические меры, позволяющие уменьшить вероятность заражения вирусами.

Существуют две основные разновидности общих методов и средств защиты информации, также эффективных при борьбе вирусными угрозами:

•средства копирования информации;

• средства разграничения доступа.

При заражении компьютера вирусом важно его обнаружить. К внешним признакам проявления деятельности вирусов можно отнести следующие:

• вывод на экран непредусмотренных сообщений или изображений;

• подача непредусмотренных звуковых сигналов;

• изменение даты и времени модификации файлов;

• исчезновение файлов и каталогов или искажение их содержимого;

• частые зависания и сбои в работе компьютера;

• медленная работа компьютера;

• невозможность загрузки ОС;

• существенное уменьшение размера свободной оперативной памяти;

• прекращение работы или неправильная работа ранее успешно функционировавших программ;

• изменение размеров файлов;

• неожиданное значительное увеличение количества файлов на диске.

Но мало заметить, что компьютерная система подверглась воздействию вредоносного ПО, необходимо обнаружить источник угрозы. К основным методам обнаружения компьютерных вирусов можно отнести следующие:

• метод сравнения с эталоном;

• эвристический анализ;

• антивирусный мониторинг;

• метод обнаружения изменений;

• встраивание антивирусов и др.

Различают следующие виды антивирусных программ:

• программы-фаги (сканеры);

• программы-ревизоры (CRC-сканеры);

• программы-блокировщики;

• программы-иммунизаторы.

Однако, абсолютно надежных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с компьютерными вирусами является своевременная профилактика. Чтобы существенно уменьшить вероятность заражения вирусом и обеспечить надежное хранение информации на дисках, необходимо выполнять следующие меры профилактики:

• применять только лицензионное ПО;

• оснастить компьютер современными антивирусными программами и постоянно возобновлять их версии;

• всегда проверять съемные носители информации на наличие вирусов (запуская

антивирусные программы своего компьютера) перед считыванием с них информации, записанной на других компьютерах;

• при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

• периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков;

• всегда защищать съемные носители информации от записи при работе на других компьютерах, если на них не будет производиться запись информации;

• обязательно делать на съемных дисках архивные копии ценной для пользователя информации;

• использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

3. Задание

Разработать программу имитирующую некоторые (см. вариант) действия по предупреждению вирусных угроз, обнаружению и удалению вирусных и других вредоносных программ и подготовить отчет о проделанной работе.

4. Содержание отчета

8. Титульный лист
9. Содержание
10. Задание
11. Алгоритм работы программы
12. Листинг программы
13. Пример работы программы
14. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Вариант		Задание	Входные данные процедуры	Выходные данные процедуры	Дополнительные условия
1	**Алгоритм работы антивирусной программы-ревизора**	Ревизоры запоминают исходное состояние файлов/каталогов, тогда, когда компьютер еще не заражен вирусом, а затем периодически сравнивают текущее состояние файла/каталога с исходным. Если обнаружены изменения, то на экран дисплея выводятся сообщения. Разработать процедуру поиска заданных (см. доп. усл.) изменений в файле/каталоге.	Имя файла (файлов)/ Имя каталога (каталогов)	Сообщение о наличии/ отсутствии изменений	Поиск изменений в дате и времени создания файла
2					Поиск изменений в атрибутах и размере файла
3					Поиск изменений в содержании файла
4					Поиск изменений в содержании каталога
5	**Обнаружение файлов-компаньонов**	Программа должна осуществлять поиск файлов-компаньонов (исполняемые файлы с тем же названием, что и исходный файл, но другим расширением) и по решению пользователя осуществлять следующие действия: (см. доп усл.)	Имя файла	Список обнаруженных файлов-компаньонов	Удаление файлов-компаньонов
6					Перемещение файлов-компаньонов в другой каталог (на карантин)
7	**Обнаружение признаков заражения вирусом**	Разработать процедуру обнаружения копий файлов в заданном каталоге. Осуществлять поиск по имени файла и по содержимому. Информировать пользователя. Предлагать на выбор следующие действия: (см. доп. усл.)	Имя файла, каталога	Список обнаруженных копий	Удаление обнаруженных копий
8					Перемещение обнаруженных копий в другой каталог (на карантин)

9	**Профилактика заражения вирусом (Резервное копирование)**	Разработать процедуру создания резервных копий. Предусмотреть возможность выбора пользователем периодичности создания резервных копий (см. доп. усл.). При этом должны делаться копии только тех файлов, которые были созданы или изменены в период после предыдущей процедуры копирования.	Имя каталога	Логическая переменная	Периодичность копирования: раз в неделю (предоставить возможность выбора дня недели)
10					Периодичность копирования: через день (предоставить возможность выбора четных или нечетных чисел)
11					Периодичность копирования: раз в несколько часов (предоставить возможность выбора интервала времени, проходящего между процедурами копирования)
12	**Обнаружение вирусного кода в теле файла**	Разработать и отладить процедуру поиска заданной строки целиком или частично в заданных файлах(см. доп. усл.). В случае обнаружения вирусного кода в теле файла реализовать следующий алгоритм «лечения»: (см. доп. усл.)	Строка, имя файла (файлов, каталога)	Логическая переменная	Поиск заданной строки и ее фрагментов (слов) в указанном файле. Алгоритм "лечения": удаление строки или ее фрагментов
13					Поиск заданной строки и ее фрагментов (слов) в указанном файле. Алгоритм "лечения": перемещение зараженного файла в другой каталог (на карантин)
14					Поиск заданной строки и ее фрагментов (слов) в указанном файле. Алгоритм "лечения": удаление зараженного файла
15					Поиск заданной строки во всех текстовых файлах заданного каталога. Алгоритм "лечения": удаление строки из всех файлов
16					Поиск заданной строки во всех текстовых файлах заданного каталога. Алгоритм "лечения": перемещение зараженных файлов в другой каталог (на карантин)
17					Поиск заданной строки во всех текстовых файлах заданного каталога. Алгоритм "лечения": удаление всех зараженных файлов

18	**Защита от клавиатурных шпионов**	Разработать генератор одноразового пароля на основе псевдослучайного выбора символов из данных, введенных пользователем. Применить следующий алгоритм ГПСЧ: (см. доп. усл.)	Массив с набором данных пользователя (для упрощения задачи: каждый элемент массива - цифра из данных пользователя: номера паспорта, даты рождения и т.п.)	Одноразовый пароль длинной N символов	X_i=round(10* sin(i* sin(i/У $_i$)) +10), где X_i -выбираемый номер элемента в массиве i - счетчик [1;N]; У- элемент в массиве данных пользователя, N=10. Минимальное количество элементов массива: 20
19					Линейный конгруэнтный метод (функция Random), N=12
20					Метод Фибоначчи с запаздываниями*: $X_i = \begin{cases} Y_{i-a} - Y_{i-b}, & если\ Y_{i-a} \geq Y_{i-b} \\ -(Y_{i-a} - Y_{i-b}), & если\ Y_{i-a} < Y_{i-b} \end{cases}$ где X_i -выбираемый номер элемента в массиве i - счетчик [max(a,b)+1; N+ max(a,b)+1]; У- элемент в массиве данных пользователя, a,b - целые положительные числа, называемые лагами, рекомендуемые значения (a,b)=(17,5), N=7. Минимальное количество элементов массива: max(a,b)
21	**Защита от массовой рассылки спама методом CAPTCHA**	Разработать программу регистрации пользователя с проверкой методом CAPTCHA. Для завершения регистрации пользователю должна быть предложена такая задача, которую с лёгкостью может решить человек, но которую несоизмеримо сложнее решить компьютеру (см. доп. усл.).	Данные пользователя	Логическая переменная	В качестве задачи предложить пользователю ввести число (слово) с картинки (одной или нескольких)
22					В качестве задачи предложить пользователю произвести показанную на картинке простую арифметическую операцию
23					В качестве задачи предложить пользователю выбрать из нескольких картинок одну, соответствующую определенному условию
24	**Защита от**	Разработать “умную” программу	Пароль	Логическая	Разработать программу, запрашивающую только

	программ открытия пароля	запроса паролей (smart password asker). Этот метод предполагает использование специальной программы запроса паролей, которая работает не по стандартному алгоритму, а по алгоритму с псевдослучайным исходом (см. доп. усл.). Реализовать 7-10 запросов пароля	(см. доп. усл.)	переменная	часть пароля: первые три символа
25					Разработать программу запрашивающую не сам пароль, а сумму цифр, входящих в пароль
26					Разработать программу запрашивающую не сам пароль, а сумму части пароля и числа месяца текущей даты
27					Разработать программу, запрашивающую только часть пароля: первый, третий и последний символ

* В данной практической работе представлен один из широко распространённых фибоначчиевых датчиков с некоторыми изменениями, т. к. датчик рассчитан на генерацию случайных вещественных чисел из диапазона $[0, 1)$, а для выполнения задания требуется сгенерировать целое число

Лабораторная работа 10. Пакеты антивирусных программ

1. Цель работы

Ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

2. Краткие теоретические сведения

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;
- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

3. Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.
   Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.
2. Заполнить таблицу " Пакеты антивирусных программ " на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Таблица "Пакеты антивирусных программ"
5. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Пакет антивирусного ПО	Основные функции	Достоинства	Недостатки
Антивирус Касперского	1	2	3
Антивирус Dr.Web для Windows	4	5	6
Panda Antivirus	7	8	9
ESET NOD32 Антивирус	10	11	12
avast! Free Antivirus	13	14	15
Avira AntiVir Personal	16	17	18
Norton AntiVirus	19	20	21
Trend Micro Internet Security	22	23	24
Microsoft Security Essentials	25	26	27
McAfee VirusScan	28	29	30

Лабораторная работа 11. Построение VPN на базе программного обеспечения

1. Цель работы

Ознакомиться с принципами построения VPN на базе программного обеспечения.

2. Краткие теоретические сведения

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернет).

Виртуальная частная сеть базируется на трех методах реализации:

Туннелирование;

Шифрование;

Аутентификация.

Hamachi— это программа, позволяющая создать виртуальную частную сеть (VPN) через Интернет и объединить в ней несколько компьютеров. После создания такой сети пользователи могут устанавливать VPN-сессии между собой и работать в этой сети точно так же, как в обычной локальной (LAN) сети с возможностью обмена файлами, удаленного администрирования компьютеров и т.д. Преимущество VPN-сети заключается в том, что она полностью защищена от несанкционированного вмешательства и невидима из Интернета, хотя и существует в нем.

Программа Hamachi должна быть установлена на всех компьютерах, которые предполагается объединить в виртуальную частную сеть.

Виртуальная сеть создается с помощью специализированного сервера Hamachi в Интернете.

После того как с помощью сервера Hamachi создается виртуальная сеть между выбранными компьютерами, обмен информацией между клиентами VPN-сети происходит уже напрямую, то есть без участия сервера Hamachi. Для обмена данными между клиентами VPN-сети используется протокол UDP.

3. Задание

Задание рассчитано на работу в паре.

Порядок выполнения задания:

1. Загрузить программу "LogMeIn Hamachi" с сайта http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.
2. Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html
3. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).
4. Подготовить отчет.

4. Содержание отчета

1. Титульный лист
2. Содержание отчета
3. Задание
4. Имена созданной сети и пользователей. Основные настройки сети (скриншоты). **Отобразить в отчете настройки аутентификации и шифрования.**
5. Пример совместной работы пользователей в сети (скриншоты).
6. Выводы

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Приступая к изучению дисциплины, необходимо в первую очередь ознакомиться с содержанием рабочей программы дисциплины.

Лекции имеют целью дать систематизированные основы научных знаний о методах и средствах защиты информации. При изучении и проработке теоретического материала необходимо:

- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в рабочей программе литературные источники;

Практические занятия проводятся с целью углубления и закрепления знаний, полученных на лекциях и в процессе самостоятельной работы над нормативными документами, учебной и научной литературой. При подготовке к практическому занятию необходимо:

- изучить, повторить теоретический материал по заданной теме;
- повторить типовые задания, выполняемые в аудитории.

Рекомендации по работе с научной и учебной литературой

Работа с учебной и научной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на практических занятиях, лабораторным работам, зачету и экзамену. Она включает проработку лекционного материала и изучение рекомендованных источников и литературы по тематике лекций.

Конспект лекций должен содержать реферативную запись основных вопросов лекции, предложенных преподавателем схем (при их демонстрации), основных источников литературы по темам, выводы по каждому вопросу. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным.

В процессе работы с учебной и научной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать переченьосновных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест источника, краткое изложение основных мыслей автора);
- создавать конспекты.

Технология самостоятельной работы должна обеспечивать овладение знаниями, закрепление и систематизацию знаний, формирование умений и навыков. Апробированная технология характеризуется алгоритмом, который включает следующие логически связанные действия:

- чтение текста (учебника, пособия, конспекта лекций);
- конспектирование текста;
- решение задач и упражнений;
- подготовка к практическим занятиям;
- подготовка к выполнению лабораторных работ;