МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по проведению практических занятий по дисциплине
«Защита программ и данных» для студентов
направления подготовки
10.04.01 «Информационная безопасность»
(профиль“Математическое и программное
обеспечение защиты информации”)

(Электронный документ)

Ставрополь
2025

СОДЕРЖАНИЕ

Методические указания к практическим занятиям
Практическое занятие №1 Защита файлов от несанкционированного доступа с помощью архиваторов и средств Microsoft office
Практическое занятие №2 Криптография и стеганография
Практическое занятие №3 Защита данных с помощью программы PGP
Практическое занятие №4 Защита жестких дисков с помощью программы BESTCRYPT
Практическое занятие №5 Восстановление удаленных файлов и необратимое удаление информации

Методические указания к практическим занятиям
Практическое занятие №1
Защита файлов от несанкционированного доступа с помощью архиваторов и средств Microsoft office

Цель работы: знакомство с защитой файлов от несанкционированного доступа с помощью архиваторов и средств microsoft office

Теоретическая часть

В Word, Excel, Power Point и других программах MS Office есть возможность защиты файлов от несанкционированных изменений. Например, в Word существуют следующие возможности ограничения доступа к документу для защиты его от несанкционированных изменений:

- Назначение пароля для открытия документа. Чтобы предотвратить любое открытие документа посторонними пользователями, можно назначить пароль.
- Назначение пароля разрешения записи. Чтобы разрешить открытие документа всем пользователям, а изменение — лишь некоторым, можно назначить пароль разрешения записи. Если какой-либо пользователь изменит документ без разрешения записи, он сможет сохранить этот документ только под другим именем.

Рекомендация доступа только для чтения. Можно предлагать (но не требовать) другим пользователям открыть документ только для чтения. Если пользователь откроет документ только для чтения и изменит его, он сможет сохранить этот документ только под другим именем.

В других программах MS Office также есть встроенные в эти программы средства защиты файлов от несанкционированных изменений, мы не будем их перечислять (более подробно познакомиться с ними можно с помощью справочной системы программ).

Однако следует помнить, что защита файлов встроенными средствами программ MS Office , позволяет защитить данные лишь от любопытства непрофессионалов. Об этом говорит существование программ подбора паролей к программам MS Office на тот случай, если пользователь забыл пароль. Ниже вы убедитесь в том, что «закрытый» паролем документ «открывается» одной из программ Passware Kit.

Защита файлов в MS Office

Программы MS Office (Word, Excel, Access и др.) имеют встроенные средства защиты создаваемых файлов, которые позволяют при сохранении файлов указать пароль для открытия файла и пароль разрешения записи.

Запустите Word (Пуск - WinWord). Введите свою фамилию и сохраните документ следующим образом:

- выберите команду Сохранить как... из меню Файл;
- в поле Папка выберите Рабочий стол;
- в поле Имя файла введите имя файла, например, Doc1;
- в правом верхнем углу окна нажмите кнопку Сервис и далее выберите строку Параметры безопасности;
- в окне Безопасность введите пароль в поле Пароль для открытия файла.

Примечание

- На учебном занятии не рекомендуется вводить пароль длиной более пяти символов, так как при последующем подборе пароля будет потрачено достаточно много времени. В практической же деятельности наоборот рекомендуется выбирать пароль длиной более шести символов.
- На учебном занятии не рекомендуется вводить пароль русскими буквами. На практике можно и нужно использовать любые символы.
- нажмите кнопку ОК.
- в окне Подтверждение пароля введите пароль еще раз и нажмите кнопку ОК;

- нажмите кнопку Сохранить;
- закройте Word.

Защита файлов с помощью архиватора WinRAR

Программы - архиваторы (WinZIP, WinRar) позволяют использовать криптографическую защиту, т.е. выполнять операции архивирования и разархивирования файлов с паролем. Использование операции архивирования файла с паролем несколько надежнее, чем защита файлов встроенными средствами MS Office.

1. Запустите WinRAR (Пуск - WinRAR).
2. Выберите в главном окне программы диск D:\ и далее папку Договор.
3. В папке выделите первые три файла.
4. Нажмите кнопку Добавить.
5. В поле Архив введите имя архива - Proba
6. Нажмите кнопку Обзор и в поле Папка выберите место сохранения архива - Рабочий стол
7. Нажмите кнопку «Открыть».
8. Выберите вкладку Дополнительно и нажмите кнопку Установить пароль
9. Введите пароль длиной 4-5 символов в верхнем поле и повторите ввод пароля в нижнем поле.
10. Нажмите кнопку ОК.

Подбор пароля для файла Word

Подбор пароля к файлу Word выполним с помощью программы Office Key. Эта программа предназначена для подбора паролей в следующих программах:

- Access, Excel, Outlook, Word, Visual Basic for Applications и др.
- Запустите программу Office Key (Пуск - Программы - Тема Защита и преодоление - Преодоление защиты - Office Key).

На экране появится главное окно Office Key

Перед запуском программы для поиска паролей необходимо настроить программу. Для этого нажмите кнопку Settings (Настройки).

На экране появится окно Settings (Настройки).

По умолчанию открывается вкладка General (Общие), состоящая из двух групп. В левой части вкладки находится группа Process Priority (Приоритет процесса). Здесь можно установить один из трех приоритетов работы программы: Low (Низкий), Normal (Нормальный), High (Высокий). По умолчанию установлен нормальный приоритет.

Примечание. Под приоритетом процесса следует понимать загруженность процессора при работе программы подбора паролей. Если планируется работа Office Key на фоне работы других программ, то рекомендуется установить низкий приоритет.

В правой части вкладки находится группа Attack types (Тип атаки). Office Key позволяет выбрать три метода подбора паролей к файлам: Dictionary

(Словарь), Brute-force with xieve optimization и Brute-force.

Dictionary (Словарь) - словарный метод атаки. Подбор пароля к файлу выполняется методом перебора слов, хранящимся в словаре dict.txt. Программа позволяет подключить и другой словарь.

Brute-force with xieve optimization - подбор паролей методом Brute-force со встроенным алгоритмом, повышающим скорость подбора паролей. При использовании этого метода пропускаются пароли из бессмысленных комбинаций символов. Вероятность восстановления паролей из английских символов составляет 85% при скорости свыше 75,000,000 паролей в минуту.

Brute-force - подбор пароля прямым перебором всех комбинаций символов выбранных на вкладке Symbol set.

Выбор приоритета работы программы и типа атаки выполняется щелчком мыши на выбранной опции.

Метод Brute-force является самым медленным методом и может протестировать все

пароли длиной до 7 символов.

Метод Brute-force with xieve optimization - значительно быстрее и способен восстановить пароли длиной до 9 символов.

Словарная атака является самым быстрым методом - ограничения по длине пароля нет.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и

программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практической работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал - полуторный, поля левое - 3 см., правое - 1,5 см., верхнее и нижнее - 2 см. Абзацный отступ - 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 - Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Как осуществляется защита файлов с помощью программ MS Office?
2. Какие в Word существуют возможности ограничения доступа к документу для защиты его от несанкционированных изменений?
3. От какой группы людей осуществляется защита файлов встроенными средствами программ MS Office? Почему?
4. Как осуществляется защита файлов с помощью программы WinRAR?
5. Как подбирается пароль с помощью утилиты Office Key из пакета Passware Kit?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс. - 1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-Ы7.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- прсс.-1991.-N10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности

компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №2
Криптография и стеганография

Цель работы: ознакомиться с криптографической защитой и стеганографической защитой файлов

Теоретическая часть

Криптография. Программы шифрования файлов

Самой надежной защитой от несанкционированного доступа к информации и программным продуктам компьютера является применение различных методов шифрования (криптографических методов защиты информации).

Криптографические методы защиты информации представляют собой шифрование данных с целью скрыть их смысл. До тех пор, пока пользователь не идентифицирован по ключу, смысл данных ему недоступен. Криптография предполагает наличие трех компонентов: данных, ключа и криптографического преобразования. При шифровании исходными данными будет сообщение, а результирующими - шифровка. При расшифровании они меняются местами. Считается, что криптографическое преобразование известно всем, но, не зная ключа, с помощью которого пользователь закрыл смысл сообщения, требуется потратить много усилий на восстановление текста сообщения. Такое требование удовлетворяется рядом современных криптографических систем, например, созданных по «Стандарту шифрования данных Национального бюро стандартов США» DES и ГОСТ 28147-89. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ, расширяющих стандартные возможности операционной системы.

Далее будет рассмотрена программа шифрования файлов FileCrypt32.

Шифрование файлов с помощью программы FileCrypt32

Программа FileCrypt32 (далее FileCrypt32) предназначена для шифрования файлов и каталогов с применением различных модификаций алгоритмов ГОСТ 28147-89, DES, BlowFish и алгоритма блочного гаммирования (более подробная информация по алгоритмам шифрования находится в справке программы). Длина ключа варьируется от 56 до 512 бит. Шифрование может осуществляться на всех логических дисках компьютера (в том числе на сетевых дисках и дискетах). FileCrypt 32 поддерживает: технологию Drag & Drop («перетаскивание» файлов), быстрый запуск для расшифрования зашифрованных документов, отправку документов по электронной почте.

Запуск программы FileCrypt32

Выполните подготовительную работу:

1. Создайте на рабочем столе текстовый файл (правая кнопка мыши на рабочем столе - Создать - текстовый документ) с именем TEXT.TXT.
2. Откройте созданный файл, введите свою фамилию, сохраните и закройте файл.

Запустите программу FileCrypt32 (Пуск - Программы - Тема Защита и преодоление - Защита информации - FileCrypt32). Откроется окно программы.

Работать с программой FileCrypt32 можно одним из трех способов: через меню программы, используя панель инструментов и совместно с программой Проводник. Все эти способы приводят к равнозначному результату и какой из них выбрать зависит лишь от Вас.

Шифрование файлов

Для шифрования файла выполните следующее:

1. Выберите команду Файлы - Зашифровать или нажмите кнопку Зашифровать;
2. В окне Открыть выберите файл TEXT.TXT на Рабочем столе и нажмите кнопку Открыть;
3. В окне Шифрование в поле введите пароль наберите любой пароль и нажмите кнопку ввести;
4. В окне Шифрование в поле Повторите пароль введите пароль еще раз и нажмите кнопку ввести;
5. После окончания шифрования Вы увидите окно с сообщением об успешном окончании шифрования. Нажмите кнопку ОК.

В результате шифрования на рабочем столе появится зашифрованный файл TEXT.TXT.FCRPT.

Также можно использовать технологией Drag&Drop:

1. Создайте на рабочем столе текстовый файл TEXT2.TXT, введите свою фамилию, сохраните и закройте файл.
2. Перетащите файл TEXT2.TXT в окно программы FileCrypt32.
3. В появившемся окне выберите «Зашифровать» и нажмите кнопку «Начать»
1. Выполните пункты 3-5 указанные выше.

Обратите внимание!

2. Появление на диске файла с расширением .FCRPT говорит о том, что файл зашифрован программой FileCrypt32.
3. Для скрытия этого факта можно убрать флажок (галочку) Изменять тип файла в окне Установки параметров (меню программы FileCrypt32

Настройки - Настройки" или щелчок мыши на кнопке Настройки). Флажок находиться в правом нижнем углу окна. После этих действий расширение файла изменяться не будет.

Шифрование папок с файлами

Выполните подготовительную работу. На рабочем столе создайте папку. Скопируйте в нее из папки Договор на диске D:\ три первых файла.

Для шифрования папки с файлами воспользуемся технологией Drag&Drop, использование которой совместно с программой Проводник значительно облегчает выбор файлов и папок для шифрования (расшифрования).

1. Выделите на Рабочем столе созданную Вами папку и перетащите ее в окно File Crypt 32.
2. В появившемся окне Drag&Drop нажмите кнопку Начать.
3. В окне Шифрование дважды введите пароль.
4. По окончании шифрования нажмите кнопку ОК.
5. Откройте зашифрованную папку и вы увидите в ней три зашифрованных файла. Дешифрование файлов

Для дешифрования файла выполните следующее:

1. Выберите команду Файлы - Расшифровать или нажмите кнопку Расшифровать;
2. В окне Открыть выберите на рабочем столе файл TEXT2.TXT и нажмите кнопку Открыть;
3. В окне Дешифрование в поле Введите пароль наберите пароль и нажмите кнопку ввести;
4. По окончании дешифрования нажмите кнопку ОК.

Можно использовать более простой способ:

1. Откройте на рабочем столе файл TEXT.TXT.FCRPT
2. Выполните пункты 3-4 указанные выше.

Обратите внимание!

Так как в настройках программы установлена опция «Не изменять тип файла », после

дешифрования файл останется с расширением FCRPT и для того чтобы прочитать его содержимое необходимо переименовать файл в TEXT.TXT

Также можно использовать технологией Drag&Drop.

1. Перетащите файл TEXT.TXT.FCRPT в окно программы FileCrypt32.
2. Выполните пункты 3-4 указанные выше.

Дешифрование папок с файлами

Дешифровать папку с файлами можно только с помощью технологии Drag&Drop.

1. Выделите на Рабочем столе созданную Вами папку и перетащите ее при нажатой левой клавише мыши.
2. В окне Drag&Drop выберите команду Расшифровать нажмите кнопку Начать.
3. В окне Дешифрование введите пароль.
4. По окончании дешифрования нажмите кнопку ОК.
5. Откройте папку и вы увидите в ней три дешифрованных файла.
6. Просмотрите содержимое файла и убедитесь в том, что файл дешифрован.

Примечание: Используя команды Файл - Зашифровать или Файл - Расшифровать обработать папку невозможно.

В случае возникновения затруднений при выполнения заданий используйте помощь программы.

Стеганография. Общие сведения о BDVDataHider

Этот класс продуктов, называемых стеганографическими, позволяет прятать данные в графических файлах .jpg, .jpeg, bmp, .ico, .emf, .wmf и предназначен для тех случаев, когда пользователь не хочет, чтобы у кого-либо создавалось впечатление, что он пользуется средствами криптографии. Пример подобной программы - BDVDataHider.

Внешне графический файл остается практически неизменным, меняются лишь кое- где оттенки цвета.

Запуск программы BDVDataHider

Запустите программу BDVDataHider (Пуск - Программы - Тема Защита и преодоление - Защита информации - BDVDataHide). Откроется окно программы.

Шифрование информации:

1. Выбрать файл для шифрования. Нажмите кнопку (Open data file...) в поле Data File.

Выберите на рабочем столе файл TEXT.TXT

2. Выберите файл изображения. Нажмите кнопку (Open image file.) в поле Image File.

Выберите в паке D:\Мои документы файл S37.BMP

3. Введите пароль. Щелкните кнопкой мыши на слово <None> в строке Password.

В окне Set Password введите пароль в поле Password и повторите ввод пароля в поле Confirm. Нажмите ОК.

4. Сохраните изображение. Нажмите кнопку

В окне «Сохранить как» выберите Рабочий стол, введите имя файла SEC (или другое) и нажмите кнопку Сохранить.

5. Теперь исходный файл можно удалить для повышения конфиденциальности информации. Удалите с рабочего стола файл TEXT.TXT и очистите Корзину.

В итоге на рабочем столе должен появиться графический файл SEC.BMP, в котором в зашифрованном виде храниться файл TEXT.TXT.

Дешифрование информации

1. Нажмите кнопку
2. Выберите на рабочем столе файл SEC.BMP
3. В поле Password одноименного окна введите пароль и нажмите ОК.
4. В окне Сохранить как нажмите кнопку Сохранить.

5. На рабочем столе появится файл TEXT.TXT

Программа позволяет шифровать не только текстовые файлы, как в нашем примере. Вы можете убедиться в этом самостоятельно.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал - полуторный, поля левое - 3 см., правое - 1,5 см., верхнее и нижнее - 2 см. Абзацный отступ - 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 - Создание подсистемы) и ссылку на него в тексте.

1. Что представляют собой криптографические методы защиты информации?
2. Наличие каких трёх компонентов предполагает криптография?
3. Раскройте суть криптографической защиты файлов с помощью программы FileCrypt32?
4. В каких случаях используется программа BDVDataHider?
5. Как осуществляется стенографическая защита файлов с помощью программ BDVDataHider?
6. Как происходит шифрование информации в программе BDVDataHider?
7. Как происходит дешифрование информации в программе BDVDataHider?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс. - 1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьтерПресс.-1993.-Ы7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- Пресс.- 1991.^10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №3
Защита данных с помощью программы PGP

Цель работы: знакомство с защитой данных с помощью программы PGP

Теоретическая часть

Прикладная криптосистема PGP (Pretty Good Privacy - довольно хорошая

секретность) была разработана и опубликована в Интернет в 1991 году программистом и математиком Массачусетского Политехнического университета Филиппом Циммерманом. По сути, она оказалась первым продуктом подобного уровня, представленным для свободного доступа всему миру (за что впоследствии Циммерман поплатился несколькими годами уголовного преследования со стороны Таможенной службы США - в то время экспорт стойких криптотехнологий за пределы Штатов был запрещён). Изначальной целью разработки была защита гражданских прав пользователей глобальной сети, а главной задачей программы стала криптографическая защита электронной почты - шифрование.

Программа основана на асимметричной криптографии, использующей взаимосвязанные пары ключей:

- Закрытый ключ, хранящийся только у владельца для расшифровывания данных и их цифрового подписания;
- Открытый ключ, который не нуждается в защите, и используемый для шифрования и сличения цифровых подписей (все эти возможности достигаются за счёт особого математического аппарата).
- Вы можете взять открытый ключ адресата из любого открытого источника, с его Интернет-сайта, например, зашифровать сообщение и отправить. Никто, кроме получателя с соответствующим закрытым ключом, не сумеет прочитать ваше письмо.

Кроме шифрования (дешифрования) информации программа PGP позволяет работать с электронной цифровой подписью, выполнять безвозвратное удаление информации и др.

Программный пакет PGP состоит из утилит:

1. PGPKey - утилита создания ключей;
2. PGPTray - утилита быстрого шифрования/дешифрования данных;
3. PGPTools - утилита "инструментального" меню для запуска различных режимов шифрования/дешифрования.

Сведения об электронной цифровой подписи

Порядок использования электронной цифровой подписи определяет Федеральный закон от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи".

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе.

Для шифрования данных в PGP сначала нужно создать пару ключей.

Запуск PGP

Существует четыре варианта запуска PGP на компьютере:

- через Пуск-Программы. Таким образом можно получить доступ к основным ресурсам PGP: PGPkeys, PGPtools, PGPtray и документации;
- из панели задач, щелкнув левой или правой кнопками на значок замочка в правом нижнем углу рабочего экрана. Этот вариант удобен для шифрования/расшифрования данных в буфере обмена;
- непосредственно из почтового клиента (например, MS Outlook, MS Outlook Express, Eudora и др.), что и предпочитают большинство пользователей;
- в проводнике через строку PGP после правого клика на иконке файла или папки, что является самым быстрым вариантом вызова программы.

Создание пары ключей

Чтобы иметь возможность обмениваться секретными сообщениями с корреспондентами, также использующими PGP, необходимо сгенерировать пару ключей - открытый и секретный, которые будут использованы в дальнейшем для создания цифровой подписи.

Открытый ключ Вы отправляете всем потенциальным получателям зашифрованной корреспонденции. Закрытый ключ должен храниться у Вас в надежном месте.

Для создания и работы с ключами используется утилита PGPKeys (Ключи PGP).

1. Для запуска утилиты нажмите правую кнопку мыши на пиктограмме PG Ptray в правом нижнем углу Панели задач (рядом с часами).
2. Затем выберите пункт меню Ключи PGP
3. Появится окно Мастер генерации ключей, который поможет создать пару ключей. Нажмите кнопку Далее.

Примечание. Если Мастер генерации ключей не запустился автоматически, то выберите в меню программы пункты: Ключи - Создать ключ.

4. Какое имя и адрес должны быть связаны с этой парой ключей? Здесь поле Полное имя: введите свою фамилию, имя, отчество, а в поле Адрес Email - свой Email адрес. Для нашего занятия можно использовать любой email адрес, например, user@pfrap.ru. По этим данным Ваши корреспонденты узнают, что ключ принадлежит именно Вам. Нажмите кнопку. Далее.
5. Ключ какого типа Вы хотите создать? Вам рекомендуют создать пару ключей Diffie-Helman/DSS. Согласитесь с рекомендацией и нажмите кнопку

Далее.

6. Какой величины ключ Вы хотите создать? Ответьте на этот вопрос нажатием кнопки Далее.
7. Срок годности ключа. Нажмите кнопку Далее, тем самым выбрав «Вечный ключ».
8. Ваш закрытый ключ будет защищен паролем. Введите пароль длиной не менее 8 символов в поле Пароль и повторите ввод пароля в поле Подтверждение. Причем в поле Подтверждение пароль не будет виден. Пароль можно (но не нужно, с точки зрения безопасности) сделать видимым, убрав галочку в поле Скрыть. Нажмите кнопку Далее.
9. В следующем окне для создания пары ключей Вам необходимо подвигать мышью до заполнения показателя прогресса. Нажмите кнопку Далее.
10. PGP создает пару ключей. По окончании процесса генерации пары ключей в нижней части окна появится сообщение Завершено. Нажмите кнопку Далее.
11. На этом шаге Вам предлагают отправить открытый ключ на сервер при наличии подключения к Интернету. Так как Ваш компьютер не подключен к Интернет, нажмите кнопку Далее.
12. В последнем окне Вас поздравляют с успешным созданием пары ключей. Нажмите кнопку Готово, чтобы добавить новый ключ в связку.

13. Появится окно PGPkeys со связкой ключей.

14. Итак, Вы создали пару ключей и теперь можете подписывать и шифровать документы и файлы. Закройте окно PGPkeys.

15. Создайте резервную копию ключей, нажав кнопку Резервная копия.

16. Нажмите кнопку Сохранить для сохранения на рабочем столе открытого ключа с именем publing.pkr.

17. Нажмите кнопку Сохранить для сохранения на рабочем столе секретного ключа с именем secring.skr.

После генерации связки ключей на рабочем столе появятся два файла: publing.pkr - открытый ключ secring.skr секретный ключ

Для дополнительной безопасности всегда необходимо делать резервную копию файлов связки (.pkr, .skr) на дискете, флешке или CD-R и хранить носитель в надежном месте. В противном случае Вы можете потерять доступ к защищенной информации.

Файл с расширением *.pkr (открытый ключ) пересылается корреспонденту для последующей шифрации им своих файлов, предназначенных для отправки Вам. Зашифрованные открытым ключом данные можно расшифровать только секретным ключом. Обратное преобразование (т.е. расшифровка открытым ключом) невозможна. В этом и состоит смысл шифрования данных с открытым ключом.

Задание:

> Создайте собственную пару ключей (адрес электронной почты №группы@рйгар.ш, срок действия ключа - неограничен).

> Теперь вам следует отправить свой открытый ключ всем потенциальным получателям зашифрованной корреспонденции. Для этого необходимо пометить мышью строку с вашим ключом в окне PGPkeys и перетащить, удерживая левую клавишу мыши, строку с ключом в окно текстового сообщения почтовой программы, а затем разослать это письмо по адресам.

Можно поступить и по-другому:

> выделить свой ключ в окне PGPkeys, выбрав из меню команды Ключи - Экспорт, сохранить ключ на диске в виде файла с расширением .asc. Полученный файл вы можете затем отправить своим корреспондентам как обычное приложение к письму.

Экспорт ключа

Для экспорта ключа выполните следующее:

1. Нажмите правую кнопку мыши на пиктограмме PGPtray и выберите Инструменты PGP.

2. 2. Появится Панель инструментов.

Панель инструментов:

- переход к PGPkeys;
- выбор файла для шифрования;
- выбор файла документа «на подпись»;
- зашифровать подписанный файл;
- расшифровать данные с подписью;
- удалить так, чтобы невозможно было восстановить;
- создание невосстановимой области.

3. Выберите инструмент PGPkeys.

4. Выделите ключ, выберите в меню команду Ключи - Экспорт и сохраните ключ на рабочем столе в виде файла с расширением .asc

Задание:

> Выполните экспорт созданного ключа на рабочий стол.

> Получив от Ваших корреспондентов публичные ключи, например по электронной почте, Вам необходимо включить их в свой брелок ключей, для чего потребуется воспользоваться пунктом меню PGPkeys Ключи - Импорт.

> После добавления ключей корреспондентов все они появятся в списке ключей в

окне PGPkeys.

Импорт ключа

Для импортирования публичных ключей корреспондентов можно:

1. Запустить ключ.
2. Выполнить в PGPkeys команду Ключи - Импорт.

Подпись ключа

> Затем ключи корреспондентов нужно подписать: следует выделить ключ в окне PGPkeys, нажать правую кнопку мыши, выбрать команду Подписать, выделить подписываемый ключ и в следующем окне ввести свою ключевую фразу.

> После этого рядом с ключом загорится вместо серой зеленая лампочка, свидетельствующая о том, что отныне с этим корреспондентом можно вести переписку.

Шифрование информации

Существует несколько вариантов шифрования информации:

1. Шифрование текста в буфере обмена данными.
2. Шифрование текста в открытом документе.
3. Шифрование файла.

Шифрование текста в буфере обмена:

> На рабочем столе создайте текстовый файл, например, с именем TEXT.TXT.

> Откройте этот файл, введите свою фамилию, имя, отчество, сохраните и закройте файл.

> Откройте созданный файл.

> Выделите только фамилию, скопируйте ее в буфер обмена (правая кнопка мыши - копировать).

> Нажмите правую кнопку мыши на пиктограмме PGPtray последовательно выберите Буфер обмена - Зашифровать.

Появится окно PGPtray - Key Selection Dialog.

> Выберите ключ (двойным щелчком мыши по ключу или перетащите его в нижнюю часть окна) и нажмите ОК.

> После этого вставьте из буфера обмена в ваш документ ниже строки с ФИО зашифрованный текст. Пример такого преобразования приведен на рисунке 22.

Примечание. Зашифрованный текст начинается со строк ----BEGIN PGP MESSAGE---- и заканчивается строкой --- END PGP MESSAGE -----

Дешифрование текста в буфере обмена

Дешифрование текстового фрагмента выполняется в обратном порядке:

последовательно выберите Буфер обмена - Расшифровать и Проверить.

- В окне PGPtray - Enter Passphrase введите пароль, который Вы вводили ранее при создании ключей (см. раздел Создание пары ключей пункт 8). Нажмите ОК.
- Если пароль введен правильно в отдельном окне будет показан расшифрованный фрагмент, который для дальнейшей работы также можно поместить в буфер (кнопка Copy to Clipboard).

Шифрование текста в открытом документе

1. На рабочем столе создайте текстовый файл, например, с именем TEXT.TXT.
2. Откройте этот файл, введите свою фамилию, имя, отчество, сохраните файл, не закрывая его.
3. Нажмите правую кнопку мыши на пиктограмме PGPtray и последовательно выберите Текущее окно - Зашифровать.
4. Появиться окно PGPtray - Key Selection Dialog (рис. 21).
5. Выберите ключ (двойным щелчком мыши по ключу или перетащите его в нижнюю часть окна) и нажмите ОК.
6. Весь текст документа в текущем окне будет зашифрован.

Дешифрование текста в открытом документе

1. Откройте зашифрованный файл, если перед этим Вы его закрыли.

2. Нажмите правую кнопку мыши на пиктограмме PGPtray и последовательно выберите Текущее окно - Расшифровать и Проверить.

В окне PGPtray - Enter Passphrase введите пароль, который Вы вводили ранее при создании ключей (см. раздел Создание пары ключей пункт 8). Нажмите ОК.

Весь текст документа в текущем окне будет расшифрован. Дешифрование документа осуществляются в обратном порядке.

Примечание. Программа PGP осуществляет шифрование только текстовых фрагментов. Если в выделенном фрагменте (в случае работы с буфером обмена данными) или в открытом документе (в случае работы с текущим окном) содержатся графические объекты (например, рисунки), то прирасшифровывании преобразованного фрагмента восстанавливается только текст!

Шифрование файла

Процедура шифрования файла аналогична шифрованию данных в буфере обмена или в текущем окне. Разница заключается в том, что в результате данной процедуры получается не зашифрованный набор символов, а файл с расширением .pgp .

1. Нажмите правую кнопку мыши на пиктограмме PGPtray и выберите Инструменты PGP.
2. Появится Панель инструментов. Выберите инструмент Encrypt (Зашифровать)
3. Выберите файл D:\Договор\06_1.doc.
4. Появиться окно PGPtray - Key Selection Dialog (рис. 20).
5. Выберите ключ (двойным щелчком мыши по ключу или перетащите его в нижнюю часть окна) и нажмите ОК.
6. В нижней части окна выберите, установив галочку, опцию Wipe Original (удалить оригинал) и нажмите кнопку ОК.

Примечание. Опция Text Output предназначена для включения шифрованного содержимого в другой файл. В результате получается файл с расширением .asc.

7. Файл 06_1.doc зашифрован с удалением оригинала. Имя зашифрованного файла - 06_1.doc.pgp.

Дешифрование файла

Дешифрование файла осуществляется в обратном порядке:

1. Выберите инструмент Decrypt/Verify (Расшифровать/Проверить)

Примечание. Тоже самое действие можно выполнить, открыв файл двойным щелчком мыши в проводнике.

2. Выберите файл 06_1.doc.pgp.
3. Введите пароль, который Вы вводили при создании ключей. Нажмите ОК.
4. Файл расшифрован.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал - полуторный, поля левое - 3 см., правое - 1,5 см., верхнее и нижнее - 2 см. Абзацный отступ - 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и

описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 - Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

криптосистема PGP?

5. На чем основана программа PGP?
6. Какие ключи использует программа PGP
7. Из каких утилит состоит программный пакет PGP?
8. Для чего предназначена утилита PGPKey?
9. Для чего предназначена утилита PGPTray?
10. Для чего предназначена утилита PGPTools?
11. Что такое электронная цифровая подпись?
12. Какие варианты запуска PGP на компьютере вам известны?
13. Как в PGP осуществляется создание пары ключей?
14. Как в PGP осуществляется экспорт ключа?
15. Как в PGP осуществляется импорт ключа
16. Как происходит шифрование текста в буфере обмена?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс. - 1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-Ы7.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- пресс.-1991.-N10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №4
Защита жестких дисков с помощью программы BESTCRYPT

Цель работы: Ознакомление с защитой жестких дисков с помощью программы

BESTCRYPT

Теоретическая часть

Общие сведения о BestCrypt

Среди программ защиты данных наибольшей популярностью пользуются программы, создающие на внешнем или фиксированном носителе шифруемые «на лету» области хранения данных, называемые «виртуальными приватными дисками». Существует несколько аналогичных программ криптографирования данных «на лету», имеющих ряд исключительных особенностей и во многом похожих друг на друга. К ним следует отнести: BestCrypt, PGPDisk, Decart Private Disk, SafeDisk, StrongDisk Pro и др. Отличие этих программ заключается в надежности алгоритмов шифрования и в удобстве пользования. К программам, реализующим надежные алгоритмы, следует отнести программы BestCrypt и PGPDisk. Далее будет рассмотрена программа BestCrypt.

Принцип работы программы BestCrypt заключается в следующем. Сразу же после инсталляции программа предлагает создать на жестком (или на любом другом) диске файл, называемый «контейнером». В процессе создания файла-контейнера задается его размер, алгоритм шифрования, пароль и ряд других параметров. После создания уже зашифрованного программой BestCrypt файла-контейнера на вашем компьютере появится новый логический виртуальный диск, с которым можно работать совершенно так же, как и с остальными дисками. В нужный момент диск можно отключить или подключить, введя пароль. Программа BestCrypt позволяет создавать несколько виртуальных дисков. Данные, хранящиеся на виртуальном диске, «на лету» криптографируются одним из алгоритмов шифрования, выбираемых пользователем при создании файла-контейнера:

- DES - федеральный стандарт США;
- ГОСТ 28147-89 - федеральный стандарт России;
- Twofish или Blowfish алгоритм шифрования, который был разработан в 1993 Брюсом Шнеиером и считается самым быстрым и надежным алгоритмом шифрования в мире.

Кроме того, BestCrypt позволяет отключать «виртуальные» диски при нажатии заданной комбинации клавиш или при длительной пассивности пользователя. После отключения виртуального диска он исчезает из перечня логических дисков вашего компьютера. Таким образом, для получения доступа к виртуальному диску нужна программа BestCrypt, файл-контейнер и пароль. Программа BestCrypt позволяет подключать виртуальный диск к любому компьютеру с установленной программой. После создания файла-контейнера, его и саму программу можно записать на CD-RW диск и быть уверенным, что ваши данные останутся приватными.

Обратите внимание: Если вы забудете пароль, доступ к вашим данным будет закрыт навсегда!!!

Как запустить BestCrypt

Щелкните левой кнопкой мыши на кнопке Пуск, далее выберите:

Программы - BestCrypt - BestCrypt Control Panel.

Создание файла-контейнера

Сначала вы должны создать файл - контейнер.

Для создания файла - контейнера выполните следующее:

- Выберите диск, где вы хотите создавать контейнер в левой панели, нажав левую кнопку мыши на выбранном диске. Выберите диск DISK_D (D:).
- Выберите команду Container - New Container (Создать новый контейнер) или нажмите кнопку для создания нового контейнера. Появится окно New container (Новый контейнер).
- В поле FileName (Имя файла) наберите имя файла, в котором будет создан ваш контейнер. Вы можете набрать любые символы. Например, PROBA.
- В поле Size (Размер) выберите размер контейнера. Наберите: 500 и выберите размер Kb.

Примечание: размер контейнера зависит от размера защищаемой информации и размера диска, используемого для хранения контейнера. В нашем примере максимальный размер контейнера - количество свободного места на диске.

- В поле Description (Описание) наберите некоторую фразу, которая описывает вид информации предназначенной для хранения в Контейнере и напомнит вам о содержании контейнера. Наберите: Документ.
- В поле Algorithm (Алгоритм) вы можете выбрать алгоритм шифрования данных - Blowfish, GOST, DES или Twofish. Выберите: Blowfish.
- В поле Key generator (Генерируемый ключ) вы можете выбрать алгоритм, который будет использоваться для преобразования вашего пароля в псевдослучайную двоичную последовательность. Доступны два алгоритма преобразования - SHA-1 и GOST. Выберите любой из них.

В поле Hold drive (Диск хранения) выберите диск, на котором будет создан файл - контейнер. Выберите диск: D:.

Примечание: в принципе, можно создавать контейнер и на сменных носителях информации (дискетах, флешках), но на практике более удобным диском для хранения файла-контейнера является жесткий диск по причине большего размера и более быстрого доступа к данным.

- Перед использованием контейнера необходимо отформатировать логический диск созданный BestCrypt. Для этого установите флажок Mount and format now (Монтировать и форматировать заново).
- В поле Mount drive (Монтировать диск) выберите одну из букв предлагаемого списка устройств. В этом поле вы выбираете имя секретного диска. Запомните имя этого диска.

После заполнения всех полей нажмите кнопку Create (Создать). Появится диалоговое окно для ввода пароля.

Вы должны ввести пароль длиной не менее шести символов дважды: в поле Password (Пароль) и в поле Confirm Password (Подтверждение пароля). Введите один и тот же пароль в оба поля: 123456 (или любой другой) и нажмите кнопку OK.

Примечание: существуют программы подбора паролей, которые, как правило, выполняют подбор пароля либо перебором всех существующих символов, либо перебором слов из словаря. Поэтому, пароль длиной менее шести символов считается не достаточно надежным.

Вот некоторые рекомендации по выбору пароля:

1. Не используйте очевидные фразы, которые легко угадать, например, имена своих знакомых и близких, даты рождения и т.п.
2. Используйте в пароле пробелы и комбинации цифр, символов и букв.
3. Используйте максимально длинные пароли - чем длиннее пароль, тем труднее его угадать.

В следующем диалоговом окне Seed value generation вы увидите сообщение о том, что вам необходимо нажать любую клавишу для генерирования случайного ключа. Нажмите и удерживайте любую клавишу до появления кнопки OK и до заполнения шкалы индикатора прогресса.

Нажмите кнопку OK. вы увидите окно с сообщением о создании файла - контейнера Proba.jbc.

Далее, появится окно Формат M, в котором необходимо установить флажок в поле Быстрое (очистка оглавления диска) и нажать кнопку Начать.

Обратите внимание! В окне Формат обязательно нужно выбрать файловую систему FAT.

Нажмите кнопку OK, подтвердив сообщение о форматировании диска. Через несколько секунд появится окно с сообщением об окончании форматирования. Нажмите кнопку OK и далее закройте окно Формат M:.

BestCrypt создаст на дискете файл PROBA.JBC, и в правом окне покажет строку с

описанием файла-контейнера: именем файла, размером, и выбранным алгоритмом.

Теперь вы можете выходить из программы. С этого момента на вашем компьютере появился новый виртуальный диск.

Работа с виртуальным диском

С помощью Проводника или Total Commander просмотрите список дисков на вашем компьютере и выберите диск созданный BestCrypt. Этот диск можно определить по пиктограмме в виде дискеты и по имени, выбранному вами ранее при создании файла - контейнера. Найдите и скопируйте на виртуальный диск любой файл размером не более 500К.

Для отключения виртуального диска переключитесь в BestCrypt, щелкните мышкой в левом окне BestCrypt по значку +, расположенному слева от пиктограммы DISK_D (D:). Ниже появится пиктограмма с изображением ключа и обозначением Proba.jbc. Щелкните мышкой по этой пиктограмме. Из главного меню программы выберите команды Container - Dismount (Размонтировать контейнер).

Вновь Проводником или Total Commander просмотрите список дисков, виртуальный диск должен исчезнуть из списка дисков. Теперь виртуальный диск вместе с файлом не доступен вам и другим пользователям компьютера до тех пор, пока вы не смонтируете (подключите) виртуальный диск.

Для подключения виртуального диска переключитесь в BestCrypt, щелкните мышкой в левом окне BestCrypt по значку +, расположенному слева от пиктограммы DISK_D (D:). Ниже появится пиктограмма с изображением ключа и обозначением Proba.jbc. Щелкните мышкой по этой пиктограмме. Из главного меню программы выберите команды Container - Mount (Смонтировать контейнер).

Появится окно Enter password, в котором вы должны ввести пароль в поле Password. Введите пароль: 123456 (или ваш пароль) и нажмите кнопку OK. Проводником или Total Commander просмотрите список дисков и выберите виртуальный диск. Удалите файл с виртуального диска.

Закрытие виртуального диска по Time out и Hot key

BestCrypt позволяет закрывать виртуальный диск автоматически через определенный момент времени (Time out) и по нажатию “горячих” клавиш (Hot key).

- Для выбора промежутка времени автоматического закрытия виртуального диска выберите из главного меню BestCrypt команды Option - Time out.
- В появившемся окне Option установите флажок Timeout Enable и установите время Time out в минутах. Например, установите время - 1 мин.
- Нажмите кнопку OK. Подождите одну минуту и убедитесь в том, что виртуальный диск размонтирован. Вновь смонтируйте виртуальный диск.
- Для подключения “горячих” клавиш выберите из главного меню BestCrypt команды Option - Hot key. В появившемся окне Option установите флажок Disconnect Hot Key Enable и выберите комбинацию “горячих” клавиш. Например, выберите клавиши Alt, Control и F1. Нажмите кнопку OK. Нажмите выбранные клавиши и убедитесь в том, что виртуальный диск размонтирован.
- Удалите файл - контейнер PROBA.JBC. Для этого размонтируйте виртуальный диск, щелкните мышкой в правом окне BestCrypt и выберите команду Container - Delete Container. В появившемся окне Remove container

нажмите кнопку Да. В окне Enter password введите пароль: 123456 (или ваш пароль) и нажмите кнопку OK.

- Закройте BestCrypt.

Скрытые контейнеры

BestCrypt создает виртуальные диски на вашем компьютере. Все данные, которые будут записаны на виртуальный диск, помещаются в контейнер в зашифрованной форме. Алгоритмы кодирования , используемые в BestCrypt надежны, и контейнер не может быть расшифрован без правильного пароля.

Но вся защита с помощью программы BestCrypt становится бесполезной, если

пользователь контейнера с защищенными данными, при некоторых обстоятельствах, будет вынужден раскрыть пароль к контейнеру. В нашей криминогенной действительности эту ситуацию можно себе легко представить.

Разработчики BestCrypt предусмотрели и этот момент. Дело в том, что BestCrypt позволяет создавать два вида контейнеров: внешний и скрытый (который спрятан во внешнем контейнере). Упрощенно скрытый контейнер можно сравнить с двойным дном в чемодане. Использование этого способа свободно от вышеперечисленных недостатков, потому что:

- параметры скрытого контейнера такие же, как и внешнего;
- сокрытие контейнеров этим способом не требует такого большого дискового пространства;
- потенциальный злоумышленник не может доказать, действительно ли дополнительный (скрытый) контейнер существует.

Принцип защиты данных с использованием скрытых контейнеров

Первоначально, до создания скрытой части, создается внешний контейнер, в который записываются какие-либо данные для маскировки.

Затем создается скрытый контейнер и в него записываются защищаемые данные.

Доступ к каждому из контейнеров осуществляется по отдельному паролю.

Данные в скрытом контейнере могут быть безвозвратно потеряны, в следующих случаях:

- если во внешний контейнер записываются какие-либо данные;
- при любом изменении свойств внешнего контейнера (перекодирование, изменение алгоритма или генератора ключей и т.д.)

Когда программа BestCrypt устанавливает контейнер, она не знает, существует в нем скрытая часть или нет. При создании скрытого контейнера программа BestCrypt ведет себя таким образом, как будто никаких скрытых контейнеров не существует. Это сделано для того, чтобы максимально скрыть существование скрытой части. В противном случае потенциальный злоумышленник, получивший пароль для вашего первоначального контейнера, сможет использовать средства отладки, чтобы определить, есть ли скрытая часть в контейнере.

Таким образом, если пользователь контейнера по каким-либо причинам вынужден будет раскрыть пароль, то он должен назвать пароль к внешнему контейнеру. В результате злоумышленник увидит данные во внешнем контейнере и при записи данных в контейнер или изменении свойств контейнера может сам же удалить скрытую часть контейнера.

Создание скрытого контейнера:

1. Создайте внешний контейнер

Обратите внимание! В окне Формат обязательно нужно выбрать файловую систему FAT или FAT32.

Хотя возможно отформатировать контейнер-оболочку с использованием любой файловой системы (FAT, FAT32, NTFS), все же рекомендуется использовать FAT или FAT32. Использовать NTFS не рекомендуется (файловая система NTFS располагает свои таблицы размещения файлов не только в начале диска, но также в средних и в последних секторах диска; следовательно, когда Вы записываете информацию в скрытую часть, возможно разрушение файловой системы NTFS в первоначальном контейнере).

2. Убедитесь в том, что контейнер создан. Например, с помощью программы Проводник убедитесь в том, что появился новый диск.
3. Скопируйте в созданный контейнер (на диск) несколько файлов.

Запишите в тетрадь или запомните свободный размер контейнера.

Утилита очистки

Когда Вы удаляете файлы с диска на вашем компьютере, операционная система (Windows 98 или Windows 2000) не стирает содержание этих файлов с диска - она только удаляет 'ссылки' на эти файлы из таблицы размещения файлов. Содержимое удаленного файла (или тело файла) продолжает оставаться на диске и может быть легко восстановлено с использованием специальных дисковых утилит.

Вы должны также принять во внимание проблему так называемого файла подкачки Windows. Файл подкачки - системный файл Windows, который используется для виртуальной поддержки памяти. Размер этого файла изменяется динамически, и он может временно сохранять части файлов или другой информации. Когда Вы открываете ваш секретный документ, файл подкачки может использоваться системой, чтобы сохранить часть документа.

Термин "стирание" используется здесь для обозначения процесса уничтожения содержимого файла или свободного пространства на диске. После выполнения этой процедуры восстановление уничтоженных файлов становится невозможным.

Утилита стирания BestCrypt (BCWipe) предоставляет 3 пути для уничтожения файлов с диска:

1. Удаление с очисткой (Delete with wiping). Используйте команду 'Delete with wiping' для надежного удаления файлов.
2. Очистка свободного пространства (Wipe free disk space). Если Вы удалили файлы, используя стандартную команду операционной системы, Вы можете очистить пространство на диске, где эти файлы были сохранены. Таким образом, содержание всех предварительно удаленных файлов становится уничтоженным.
3. Очистка специальных папок (Swap file wiping). При этом удаляется содержимое служебных папок операционной системы, в которых она хранит временные файлы, протоколы работы и т.д.

Запуск утилиты очистки

Утилиту очистки можно запустить через Менеджер задач BCWipe (Пуск - Программы - Криптография - BCWipe Task Manager). Через пункт меню "Задачи" можно выбрать требуемую процедуру.

Например, для очистки свободного пространства логического диска, необходимо выбрать опцию "Очистка свободного места". При этом открывается диалоговое окно "Свойства задачи очистки .

При выборе дополнительных опций рекомендуется очищать файл подкачки. *ОБРАТИТЕ ВНИМАНИЕ: Перед выполнением операции очистки свободного пространства, рекомендуется закрыть все приложения. Есть две причины сделать это:*

1. некоторые программы создают временные файлы, и содержание этих файлов не будет вытерто во время очистки свободного пространства;
2. файл подкачки Windows может сохранять некоторую информацию, которая используется в настоящее время загруженными приложениями. Эта часть файла подкачки не будет вытерта.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал - полуторный, поля левое - 3 см., правое - 1,5 см., верхнее и нижнее - 2 см. Абзацный отступ - 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о

проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 - Создание подсистемы) и ссылку на него в тексте.

1. Для чего предназначена программа bestcrypt?
2. Какие аналоги программы bestcrypt вы знаете? В чем их отличия?
3. Что необходимо для получения доступа к виртуальному диску?
4. Как осуществляется запуск программы bestcrypt?
5. Как создается файл-контейнер?
6. Какие рекомендации по выбору пароля вы знаете?
7. Как осуществляется работа с виртуальным диском?
8. Как bestcrypt позволяет закрывать виртуальный диск?
9. В чем заключается принцип защиты данных с использованием скрытых контейнеров?
10. Как создается скрытый контейнер?
11. Для чего нужна утилита очистки?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //Компью - терПресс. - 1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьтерПресс.-1993.-Ы7.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- Пресс.-1991.-Ы10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №5 Восстановление удаленных файлов и необратимое удаление информации.

Цель работы: Ознакомиться с общими принципами восстановления удаленной информации.

Теоретическая часть

Общие сведения о восстановлении удаленных файлов

Задумывались ли вы когда-нибудь, насколько ценна информация, которая содержится на жестком диске вашего компьютера? И, что вы будете делать, если вдруг произойдет одна из фатальных неожиданностей таких как, случайное удаление файла с почти готовым текстом курсовой работы или какого-то еще, не менее важного для вас файла; изменение содержимого файла в результате заражения его вирусом; сбоя работы жесткого диска; случайного отключения питания компьютера и др.

Какие можно предпринять профилактические меры, чтобы эти неприятности не постигли ваш компьютер?

Необходимо заблаговременно подготовиться к нештатным ситуациям - установить необходимое программное обеспечение, создать архивы наиболее важных данных. Идеальный вариант - ежедневно делать резервные копии важных данных - тогда никакие вирусы и сбои не страшны. Но иногда роковое стечение обстоятельств не позволяет вовремя зарезервировать бесценные файлы.

Что делать, когда ваши данные все же пропали?

Прежде всего, стоит попробовать восстановить удаленные файлы из «Корзины» стандартными средствами Windows, подробно описанными в учебно-методических материалах «Операционная система Windows».

Однако, если пользователь удалил файл таким образом, что он не попал в «Корзину» Windows, то скорее всего, вам понадобятся специальные программы,

такие как: Recover My Files, R-Studio, Easy Recovery Pro, O&O DiskRecovery и др.

Программы подобного рода позволяют восстанавливать удаленные файлы, благодаря тем следам, что остаются на диске после их удаления. Ведь, как известно, физически сам удаляемый файл не уничтожается - информация, содержащаяся в нем, на диске остается, а операционная система просто отмечает в таблице расположения файлов, что эти кластеры стали свободными, и на их место можно записывать новые файлы.

Таким образом, ваш файл жив до тех пор, пока на его место не будет записано что-то другое. Даже при обычном форматировании область данных на диске не затрагивается - обнуляются только загрузочная запись, таблица размещения файлов и корневая директория. При простом же удалении файла на диске остается практически вся информация для его абсолютно корректного восстановления, надо только уметь ей воспользоваться. Вот этим и занимаются указанные выше программы - берут в структуре директорий сохранившиеся там данные об удаленном файле и предлагают нам его вернуть. Естественно, чем быстрее вы спохватились, тем выше вероятность восстановления ваших файлов.

Среди названных программ следует выделить наиболее популярную программу - Easy Recovery Pro.

Общие сведения о программе Easy Recovery Pro

Easy Recovery Pro на сегодняшний день - это одна из лучших программ своего класса. Облегченный вариант - Easy Recovery Lite - входит в состав пакета комплексного обслуживания системы Fix-It Utilities. Старая версия программы, называвшаяся Tiramisu, стала почти культовой программой среди узкого круга специалистов.

Easy Recovery умеет работать почти со всеми более-менее распространенными файловыми системами: FAT12, FAT16, FAT32, NTFS, Novell, стандартами ZIP и JAZ-приводов, поддерживаются также и SCSI-жесткие диски. Одно из важнейших достоинств программы заключается в том, что у нее не только удобный и понятный Windows-интерфейс, доступный неопытным пользователям, но и есть возможность создать комплект загрузочных дискет с полноценной DOS-версией Easy Recovery. Сделано это для того, чтобы в случае серьезных неполадок, когда нет возможности загрузить Windows (а, соответственно, и "виндовскую" версию Easy Recovery), у вас всегда был бы доступ к жесткому диску, и вы могли бы восстанавливать файлы непосредственно из MS-DOS. Такой режим наиболее предпочтителен при крупных сбоях - на сбойный диск ничего не записывается, Easy Recovery работает для него в режиме Read only («Только чтение»),

поэтому и файлы на нем будут в большей сохранности.

Первое, что бросается в глаза сразу после запуска программы - очень долгий процесс сканирования диска. Однако это не является недостатком, а совсем наоборот - свидетельствует о ее неслабых возможностях. Дело в том, что как уже отмечалось, быстрые, простые программы получают информацию об удаленных файлах и шансах на их восстановление из структуры директорий и таблицы размещения файлов. Времени это, конечно, занимает очень мало, но ведь файл может еще быть на диске даже в том случае, если больше никаких его следов не осталось, да и сама таблица размещения файлов и корневая директория могут быть разрушены. Вот тут-то и спасет вас Easy Recovery - она просканирует целиком весь жесткий диск, кластер за кластером, пытаясь собрать все кусочки каждого файла воедино.

При этом допускается полная потеря обоих копий таблицы FAT, повреждение Root Folder и загрузочного сектора диска. Разумеется, если что-то из этого все-таки сохранилось, то будет в полной мере использовано. Кстати, если вы регулярно дефрагментируете диск, то шансы на успех еще больше увеличиваются - файл, у которого используемые кластеры идут друг за другом, восстановить проще.

Таким образом, Easy Recovery - это одна из немногих программ, которая справляется не только с восстановлением ошибочно удаленных файлов, но и восстанавливает информацию на диске после повреждения его вирусами, форматирования, переразбиения на разделы, порчи при скачках напряжения питания, сбоях аппаратного оборудования или программ.

Из "виндовского" интерфейса вы, разумеется, тоже получите все это богатство возможностей, но только в том случае, если диск с операционной системой невредим. Поэтому целесообразно сделать заранее загрузочные дискеты Easy Recovery - с ними ваши данные будут иметь как бы дополнительный "спасательный круг". Правда, поскольку Easy Recovery с поврежденным диском работает только на чтение, то придется запастись вторым винчестером или другим носителем, прежде чем приступать к восстановлению больших объемов данных. Причем доступ к диску вы, скорее всего, получите, даже если ваша ОС его не обнаруживает.

Конечно, с DOS-вариантом программы работать сложнее, поэтому желательно предварительно изучить инструкцию, чтобы разобраться во всех многочисленных опциях Easy Recovery.

Приятных и полезных дополнительных функций у Easy Recovery немало: так, например, "виндовская" версия умеет проводить диагностический тест диска, аналогичный тому, что используется стандартным ScanDisk. При восстановлении файлов сохраняются длинные имена. В соответствии с последними стандартами, программа способна обновляться через Интернет.

Восстановление удаленной информации

В повседневной работе с компьютером наиболее часто встречаются две ситуации случайного удаления файлов:

1. Файл удален в Корзину.
2. Файл удален без использования Корзины.

Восстановление информации из Корзины

Ситуация №1. Удаленный файл находится в Корзине.

Для восстановления файла из Корзины выполните следующее:

1. Откройте Корзину.
2. Выберите удаленный файл.
3. Восстановите файл, выбрав в меню Файл - Восстановить.

Восстановление информации с помощью специальных программ

Ситуация №2. Вы удалили файл и затем очистили Корзину.

В этом случае можно попытаться восстановить файл специальными программами, которые должны быть установлены заранее. Если вы заранее не установили программы для

восстановления удаленных файлов, то их можно запускать с переносных носителей.

Примечание. Вероятность восстановление файлов будет выше, если вы выполните следующие требования:

1. *Нельзя работать с диском, с которого вы удалили файл. Под работой с диском следует понимать: открытие, удаление, копирование, создание, переименование файлов и папок.*
2. *Регулярная дефрагментация диска до удаления файла. Для восстановления файла воспользуемся EasyRecovery.*

Восстановление файлов с помощью EasyRecovery

Теперь попробуем восстановить удаленный файл.

Запустите EasyRecovery (Пуск - Тема - Осмотр носителя - 4

Восстановление данных - EasyRecovery Professional).

После загрузки программы на экране появляется окно, в левой части которого размещено меню в виде кнопок, обеспечивающих доступ к четырем категориям функций, а также к двум дополнительным сервисам :

- Диагностика диска - утилиты для проверки физических параметров диска и целостности файловой системы;
- Восстановление данных - утилиты для поиска и восстановления удаленных и поврежденных данных;
- Восстановление файлов - специализированные утилиты для восстановления файлов, созданных приложениями из семейства MS Office (кромеOutlook), а также ZIP-архивов;
- Восстановление Email - специализированная утилита для восстановления файлов Outlook;
- Обновление программы - сервисные функции, позволяющие получать информацию и выполнять обновление лицензионной версии EasyRecovery через Интернет;
- Кризисный центр - набор функций, обеспечивающих доступ к сервисным веб-службам компании Ontrack.

В меню выберите Восстановление данных и далее DeletedRecovery. В левой части выберите диск D:\.

Примечание. Если вы удалили один или несколько файлов, быстрое сканирование должно найти эти файлы. Поиск будет производиться только в файловой системе (это должно продолжаться всего несколько секунд). В случае, когда вы удалили целые каталоги, используйте опцию полного поиска. Для этого выберите опцию Complete Scan.

Нажмите кнопку Далее, чтобы начать сканирование диска. Вы увидите окно прогресса сканирования.

- Processing block показан сканированный блок диска и число всех блоков до момента сканирования
- Elapsed time время, которое прошло от момента начала сканирования
- Remaining time предполагаемое время, которое осталось до окончания операции
- Directories found количество найденных на диске каталогов
- Files found количество найденных файлов
- Last file название последнего найденного файла

После окончания сканирования вы увидите список найденных файлов. Однако надо помнить, что не каждый найденный с помощью EasyRecovery файл возможно восстановить. Поле Condition в списке файлов показывает в каком состоянии находится найденный файл. Выберите файлы, которые хотите восстановить и щелкните Далее.

Примечание. Первый сивол имени удаленного файла заменен символом подчеркивания.

В следующем окне в поле Recovery Statistics находится короткая статистика о

восстановленных файлах, включающая количество файлов, которые вы выбрали для восстановления, а также их полный размер. Выберите директорию, в которую их надо записать (Recover to Local Drive). Вы также можете отправить восстановленные файлы непосредственно на сервер FTP (Recover to an FTP Server). Помните, что EasyRecovery не позволит записать файлы в раздел, с которого происходит восстановление данные. Версия Professional предлагает возможность компрессии восстановленных файлов в архив ZIP (Create ZIP). На ваше усмотрение вы можете установить лимит размера файла ZIP (ZIP File Size Limit), а также создать отчет о восстановлении файлов (Generate Recovery Report). Выберите для восстановления диск C:\, нажмите Далее.

В следующем окне нажмите Готово.

EasyRecovery может записать установки восстановления, чтобы потом вы смогли продолжить операцию восстановления других файлов. Нажмите кнопку No.

Вы восстановили данные.

Просмотрите восстановленный файл.

Удаление файлов без возможности восстановления

При удалении файлов из-под DOS или с использованием Windows Recycle Bin информация на диске стирается не полностью и при помощи соответствующего программного обеспечения может быть восстановлена. Такой метод удаления данных не может считаться абсолютно безопасным, поэтому для того, чтобы конфиденциальность данных была сохранена, необходимо использовать специальные утилиты для полного уничтожения данных на диске. Программ подобного рода достаточно много, все они используют различные алгоритмы уничтожения данных, но в целом принцип работы одинаков - удаление информации с перезаписью тех секторов диска, которые были заняты этой информацией, случайными данными много раз подряд.

Ранее были рассмотрены программы защиты данных: PGP и BestCrypt. В состав этих программ входят утилиты для безвозвратного удаления данных. PGPtools - это Wipe (удаление файлов) и Freespace Wipe (очистка диска).

BestCrypt - Wipe drive free space (очистка диска).

Рассмотрим работу утилиты Wipe из комплекта PGPtools.

Защита папок и файлов

В этом разделе будет рассмотрен вопрос - как надежно скрыть папку или файл от посторонних глаз.

Кратко: В сети существует много программ для скрытия отдельных папок и файлов от других пользователей компьютера. Эти программы предлагают простой метод скрытия папок - с помощью фильтрации запросов к файловой системе. Но это не означает 100% защиту данных.

На самом деле скрытые файлы и папки можно увидеть и посмотреть с помощью других средств. Если требуется более надёжная защита, следует обратиться к серьёзным криптографическим пакетам (шифрование).

Как скрыть папку или файл?

Одним из самых больших желаний пользователя зачастую является желание спрятать свои личные документы, программы и прочие данные куда-нибудь подальше от чужих глаз. Самый распространённые способы для этого:

- Использовать программы для скрытия файлов и папок. Таковых сейчас довольно много: Hide Folders XP, Folder Lock и др.
- Использовать стандартные средства в Windows: пометить папку\файл как скрытый, на NTFS томах - запретить доступ к папке/файлу путем указания прав для доступа к объекту.

Директории и файлы, помеченные в Windows как «скрытые»:

- Не видны в Проводнике другим пользователям системы, если у пользователя включен флаг: Не отображать скрытые папки.
- Видны в программах: FAR, Total Commander, и др., которые не используют

стандартный диалог для отображения файлов и папок.

Мы намеренно упустили из виду EFS (встроенное шифрование в Windows 2000/XP), поскольку для настройки этой возможности требуются значительные усилия и квалификация.

Удобство этих методов заключается в том, что для скрытия информации не нужно делать ничего лишнего. Всё довольно просто: достаточно одного клика мыши, чтобы скрыть ту или иную папку/файл.

Защита файлов и папок с помощью Hide Folders XP

Hide Folders XP закрывает доступ к папкам и файлам, скрывая или блокируя их. В первом случае папка или файлы не видны, во втором случае - видны, но заблокированы.

Программу можно настроить на автоматический запуск при старте Windows. Какая степень защиты?

Далеко не все утилиты для скрытия папок надёжно скроют Ваши данные. Ещё меньшее их число кроме того, что скроет их, будет надежно защищать их шифрованием от разных приемов. Множество таких программ скрывают папки и файлы лишь для одной операционной системы. А если на компьютере (ПК) установлено несколько операционных систем (ОС)? Из одной системы данные видно не будет, а из другой - всё, как на ладони!

Простое скрытие папок и ограничение доступа к файлам не спасает в следующих случаях:

- Загрузка ПК в другой операционной системе (если она есть) либо загрузка другой ОС с CD-ROM. Например Linux BLin .
- в другой ОС, которая подключится к вашему HDD диску, все файлы на нем будут видны, поскольку никаких ограничений и защиты не будет.
- Загрузка Windows в SafeMode (безопасный режим).

После такой загрузки все папки будут видны, да же те, которые были скрыты программно. Ведь, при загрузке в безопасном режиме, Windows загружает лишь драйвера, необходимые для работы системы, а все дополнительные пропускает (драйвера-фильтры), чтобы заранее отбросить потенциально возможные сбои.

- Снять HDD диск и подключить его к другому компьютеру.

Если снять жесткий диск (HDD диск) и подключить его к другому компьютеру, то можно увидеть и открыть все скрытые папки и файлы. Будут видны даже те папки, доступ к которым запрещен (на NTFS томах) .

Есть ещё одна возможность просмотреть файлы, скрытые различными программами. Для этого необходимо обладать правами Администратора (Учетная запись с Администраторскими полномочиями). Потому что, если Вы являетесь администратором системы, вы можете деинсталлировать (удалить) программы для скрытия папок, или загрузиться в режиме защиты от сбоев, и тогда все скрытые объекты станут видимыми.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал - полуторный, поля левое - 3 см., правое - 1,5 см., верхнее и нижнее - 2 см. Абзацный отступ - 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 - Создание подсистемы) и ссылку на него в тексте.

1. Какие программы для восстановления удаленных файлов вы знаете?
2. Благодаря чему возможно восстановление удаленных файлов?
3. Перечислите общие сведения о программе Easy Recovery Pro?
4. С какими файловыми системами работает Easy Recovery Pro?
5. В чем заключается достоинство программы Easy Recovery Pro?
6. Справляется ли программа Easy Recovery Pro со своей задачей при повреждения файла вирусами, форматирования, переразбиения на разделы, порчи при скачках напряжения питания, сбоях аппаратного оборудования или программ?
7. Какие две наиболее встречающиеся ситуации случайного удаления файлов вам изветсны?
8. Как происходит восстановление информации из Корзины?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс. - 1993.-N8. -С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьтерПресс.-1993.-ЫЗ.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- Пресс.-1991.^10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СКФУ
СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по организации самостоятельной работы по дисциплине
«Защита программ и данных»
для студентов направления подготовки 10.04.01
«Информационная
безопасность» (направленность (профиль) “Математическое и
программное
обеспечение защиты информации”)

Ставрополь
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ
1. Общая характеристика самостоятельной работы студента
Технологическая карта самостоятельной работы студента
2. Самостоятельное изучение тем лекций
3. Паспорт фонда оценочных средств для проверки самостоятельной работы
3.1 Вопросы для собеседования по практическим занятиям
Вопросы для собеседования по самостоятельному изучению тем дисциплины «Защита программ и данных»
5. Список рекомендуемой литературы
5.1. Основная литература
5.2. Дополнительная литература
5.3. Интернет-ресурсы
5.4. Материально-техническое обеспечение дисциплины

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные и практические работы, самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области защиты программ и данных, развивается логическое мышление, формируется научное мировоззрение. На лабораторных и практических занятийах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным и практическим занятиям и тестовые, завести новую тетрадь для конспектирования лекций и выполнения лабораторных и практических занятий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная - поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы курсантов по учебной дисциплине являются:

— самостоятельное изучение учебного материала по заданным темам;

— подготовка к лабораторным работам, оформление отчета по выполненному практическому занятию и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

— чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

— работа с нормативными документами;

— поиск информации в Интернет;

2) для закрепления и систематизации знаний:

— работа с конспектом лекции (обработка текста);

— повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

— составление плана и тезисов ответа или графическое изображение структуры ответа;

— составление таблиц для систематизации учебного материала;

— изучение нормативных документов;

— ответы на контрольные вопросы;

3) для формирования умений:

— подготовка к практическим и лабораторным занятиям;

— решение задач и практических и лабораторных заданий;

— подготовка отчетов по практическим и лабораторным занятиям;

— рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические и лабораторные занятия, контрольные вопросы и тесты) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим и лабораторным занятиям, а также варианты тестовых заданий.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
1 семестр					
ИД-2 ПК-3 ИД-3 ПК-3 ИД-3 ПК-4 ИД-5 ПК-4	Подготовка к лабораторной работе	Собеседование, проверка конспектов	54		54
Итого за 1 семестр			54		54
Итого			54		54

3. Самостоятельное изучение тем лекций

№ п/п	Темы для самостоятельного изучения				
		Основная	Дополнительная	Методическая	Интернет-ресурсы
	Тема: Особенности ассемблера для исследования работы программ	1			
	Тема: Основные способы ввода/вывода	1	1		
	Тема: Отладчики и дизассемблеры, их достоинства и недостатки	1			
	Тема: Методы противодействия и способы защиты программ от взлома	1	2, 3	1	1
	Тема: Основные способы защиты программ	1	2	1	2

	Тема: Основные способы взлома программ	1	2	1	1

4. Паспорт фонда оценочных средств для проверки самостоятельной работы

	Этап формирования компетенции (№ темы)	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количество элементов, шт.
5 семестр					
	1 - 6	Текущий	Устный	Вопросы для собеседования по практическим занятиям	57
	1 - 18	Текущий	Компьютерное тестирование	Фонд тестовых заданий	307

4.1 Вопросы для собеседования по практическим занятиям

Практическое занятие №1. Защита файлов от несанкционированного доступа с помощью архиваторов и средств Microsoft Office

Базовый уровень:

1. Как осуществляется защита файлов с помощью программ MS Office?
2. Какие в Word существуют возможности ограничения доступа к документу для защиты его от несанкционированных изменений?
3. От какой группы людей осуществляется защита файлов встроенными средствами программ MS Office? Почему?
4. Как осуществляется защита файлов с помощью программы WinRAR?
5. Как подбирается пароль с помощью утилиты Office Key из пакета Passware Kit?

Повышенный уровень:

1. Какую защиту позволяют использовать программы - архиваторы (WinZIP, WinRar)?
2. С какими программами работает программа Office Key?
3. Что понимается под приоритетом процесса?
4. Какие три метода подбора паролей вам известны?
5. В чемсуть метода подбора паролей к файлам Dictionary?
6. В чемсуть метода подбора паролей к файлам Brute-force with sieveoptimization?
7. В чемсуть метода подбора паролей к файлам Brute-force?
8. Какойметод подбора паролей к файлам является самым медленным, а какой самым быстрым?

Практическое занятие №2. Криптография и стеганография

Базовый уровень:

1. Что представляют собой криптографические методы защиты информации?
2. Наличие каких трёх компонентов предполагает криптография?
3. Раскройте суть криптографической защиты файлов с помощью программы

FileCrypt32?

4. В каких случаях используется программа BDVDataHider?
5. Как осуществляется стенографическая защита файлов с помощью программ BDVDataHider?
6. Как происходит шифрование информации в программе BDVDataHider?
7. Как происходит дешифрование информации в программе BDVDataHider?

Повышенный уровень:

1. В чем суть технологии Drag&Drop?
2. Как происходит шифрование папок с файлами в программе BDVDataHider?
3. Как происходит дешифрование файлов в программе BDVDataHider?
4. Как происходит дешифрование папок с файлами в программе BDVDataHider?

Практическое занятие №3. Защита данных с помощью программы PGP

Базовый уровень:

1. В каком году и кем была разработана и опубликована в Интернет прикладная криптосистема PGP?
2. На чем основана программа PGP?
3. Какие ключи использует программа PGP
4. Из каких утилит состоит программный пакет PGP?
5. Для чего предназначена утилита PGPKey?
6. Для чего предназначена утилита PGPTray?
7. Для чего предназначена утилита PGPTools?
8. Что такое электронная цифровая подпись?
9. Какие варианты запуска PGP на компьютере вам известны?
10. Как в PGP осуществляется создание пары ключей?
11. Как в PGP осуществляется экспорт ключа?
12. Как в PGP осуществляется импорт ключа
13. Как происходит шифрование текста в буфере обмена?
14. Как происходит шифрование текста в открытом документе?
15. Как происходит шифрование файла?

Повышенный уровень:

1. Каким федеральным законом определяется порядок использования электронной цифровой подписи?
2. Чему равнозначна электронная цифровая подпись?
3. Как осуществляется дешифрование текста в буфере обмена?
4. Как осуществляется дешифрование текста в открытом документе?
5. Как осуществляется дешифрование файла?

Практическое занятие №4. Защита жестких дисков с помощью программы bestcrypt

Базовый уровень:

1. Для чего предназначена программа bestcrypt?
2. Какие аналоги программы bestcrypt вы знаете? В чем их отличия?
3. Что необходимо для получения доступа к виртуальному диску?
4. Как осуществляется запуск программы bestcrypt?
5. Как создается файл-контейнер?
6. Какие рекомендации по выбору пароля вы знаете?
7. Как осуществляется работа с виртуальным диском?
8. Как bestcrypt позволяет закрывать виртуальный диск?
9. В чем заключается принцип защиты данных с использованием скрытых контейнеров?
10. Как создается скрытый контейнер?
11. Для чего нужна утилита очистки?

Повышенный уровень:

1. От чего зависит размер контейнера?
2. На каком диске лучше всего хранить файл-контейнер? Почему?
3. Пароль какой длины считается достаточно надежным?
4. Какие файловые системы рекомендуются для отформатирована контейнер-оболочки?
5. Каких 3 пути для уничтожения файлов с диска предполагает Утилита стирания BestCrypt (BCWipe)?
6. Почему перед выполнением операции очистки свободного пространства рекомендуется закрыть все приложения?
7. Как ограничить доступ к информации на виртуальном диске?
8. Как получить доступ к информации на виртуальном диске?
9. Назначение команд Hot key и Time out, как можно выполнить эти команды? Какие требования предъявляются к выбору пароля?

Практическое занятие №5. Восстановление удаленных файлов и необратимое удаление информации

Базовый уровень:

1. Какие программы для восстановления удаленных файлов вы знаете?
2. Благодаря чему возможно восстановление удаленных файлов?
3. Перечислите общие сведения о программе Easy Recovery Pro?
4. С какими файловыми системами работает Easy Recovery Pro?
5. В чем заключается достоинство программы Easy Recovery Pro?
6. Справляется ли программа Easy Recovery Pro со своей задачей при повреждения файла вирусами, форматирования, переразбиения на разделы, порчи при скачках напряжения питания, сбоях аппаратного оборудования или программ?
7. Какие две наиболее встречающиеся ситуации случайного удаления файлов вам изветсны?
8. Как происходит восстановление информации из Корзины?
9. Как осуществляется Восстановление файлов с помощью EasyRecovery?
10. Какие утилиты программ защиты данных PGP и BestCrypt для безвозвратного удаления файлов вам известны?
11. Как скрыть папку или файл?
12. Какие программы для скрытия файлов и папок вам известны?

Повышенный уровень:

1. Почему целесообразно сделать заранее загрузочные дискеты Easy Recovery?
2. Почему придется запастись вторым винчестером или другим носителем, прежде чем приступать к восстановлению больших объемов данных?

4.2 Комплект разноуровневых задач и заданий

Базовый уровень:

1. Метод экспериментов с «черным ящиком».
2. Содержание задачи анализа программных реализаций.
3. Этапы решения задачи анализа программных реализаций.
4. Методы решения задачи анализа программных реализаций.
5. Способы восстановления схемы шифрования, реализуемую архиватором ARJ.
6. Особенности анализа оверлейных программ.
7. Особенности анализа графических программ Windows.
8. Особенности анализа параллельного кода.
9. Особенности анализа кода в режиме ядра Windows.
10. Программные и аппаратные точки останова.

11. .Условия работы с Syser.
12. Опасность программных закладок.
13. Определения информационного потока.
14. Операция порождения нового субъекта доступа.
15. Причины НСД в рамках субъектно-ориентированной модели.
16. Общие сведения модель компьютерной системы.
17. Субъектно-ориентированная модель компьютерной системы.
18. Модели взаимодействия программной закладки с атакуемой системой.
19. Отсутствие необходимых проверок входных данных.
20. Некорректный контекст безопасности.
21. Системные окна на рабочем столе пользователя.
22. Устаревшие функции.
23. Методы внедрения программных закладок.
24. Маскировка программной закладки под прикладное программное обеспечение.
25. Маскировка программной закладки под системное программное обеспечение.
26. Подмена системного программного обеспечения.
27. Прямое ассоциирование.
28. Косвенное ассоциирование.
29. Определение компьютерных вирусов.
30. Компьютерные вирусы как особый класс программных закладок.
31. Классификация компьютерных вирусов.
32. Средства и методы защиты от программных закладок.
33. Антивирусный мониторинг информационных потоков.
34. Программные ловушки.
35. Организационные и административные меры антивирусной защиты.
36. Инструктирование пользователей.
37. Общие сведения об аутентификации.
38. Хранение аутентифицирующей информации в открытых компьютерных системах.
39. Протоколы стойкой удаленной аутентификации пользователей.
40. Общие сведения об электронных ключах.
41. Электронные ключи.
42. Защита программного обеспечения от исследования.
43. Вирусы как класс РПВ.
44. Сертификация программного обеспечения по уровню контроля отсутствия НДВ.
45. Статический анализ исходных текстов программ.
46. Защита персональных данных.
47. Состав и содержание персональных данных.
48. Обработка персональных данных.
49. Обеспечение безопасности персональных данных.

Повышенный уровень:

50. Классификация ИСПДн.
51. Средства защиты ПДн
52. Проектирование СЗПДн.
53. Защита ПДн при неавтоматизированной обработке.
54. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации.
55. Уязвимость GetAdmin в Windows NT.
56. Уязвимость AdminTrap в Windows NT.
57. Уязвимость сервера NetDDE в Windows 2000.
58. Уязвимость графического формата WMF в Windows.
59. Уязвимость program.exe.

60. Проверка операционной системы на уязвимость program.exe.
61. Как происходит шифрование информации в программе BDVDataHider?
62. Как происходит дешифрование информации в программе BDVDataHider?
63. Из каких утилит состоит программный пакет PGP?
64. Для чего предназначена утилита PGPKey?
65. Для чего предназначена утилита PGPTray?
66. Для чего предназначена утилита PGPTools?
67. Что такое электронная цифровая подпись?
68. Как происходит шифрование текста в буфере обмена?
69. Как происходит шифрование текста в открытом документе?
70. Как происходит шифрование файла?
71. Для чего предназначена программа bestcrypt?
72. Какие аналоги программы bestcrypt вы знаете? В чем их отличия?
73. Что необходимо для получения доступа к виртуальному диску?
74. Как осуществляется запуск программы bestcrypt?
75. Как создается файл-контейнер?
76. Какие рекомендации по выбору пароля вы знаете?
77. Как осуществляется работа с виртуальным диском?

4.3 Вопросы для собеседования по самостоятельному изучению тем дисциплины «Математические методы защиты информации»

Тема 1: Особенности ассемблера для исследования работы программ

1. Какие области памяти используются ОС?
2. С какого адреса загружается программа?
3. Какой объем памяти доступен для использования прикладными программами?

Тема 2: Основные способы ввода/вывода

1. Перечислите компоненты подсистемы ввода вывода в Windows.
2. Опишите основные структуры данных, участвующие в процессе ввода вывода.
3. Приведите пример ввода вывода с описанием участвующих в нем структур данных и функций Windows Research Kernel.

Тема 3: Отладчики и дизассемблеры, их достоинства и недостатки

1. Отладчики.
2. Дизассемблеры.
3. Статический метод.

Тема 4: Методы противодействия и способы защиты программ от взлома

1. Перечислить программные способы защиты от копирования.
2. Перечислить программно-аппаратные способы защиты от копирования.
3. Перечислить методы взлома систем защиты от копирования, рассказать, как можно противодействовать этим методам?

Тема 5: Основные способы защиты программ

1. Какие методы противодействия дизассемблированию вы можете назвать?
2. В чем заключается сущность метода, основанного на использовании самогенерируемых кодов?
3. Опишите методы защиты программ от исследования.
4. В чем состоит принципиальное отличие вируса от троянской программы?

Тема 6: Основные способы взлома программ

1. Использование взломанной версии файла.
2. Использование эмулятора ключа.

5. Список рекомендуемой литературы

5.1. Основная литература

1. Проскурин В. Г. Защита программ и данных: учеб.пособие для студ. Учреждений высш. проф. образования / В. Г. Проскурин. 2-с изд., стер. - М. : Издательский центр «Академия», 2012. 208 с. - (Сер. Бакалавриат).

5.2. Дополнительная литература

1. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин — М. : Радио и связь, 2006.

2. Панов А.С.. Реверсинг и защита программ от взлома/ А. Панов-Издательство: БХВ-Петербург 2006.

3. Платонов В.В. Программно-аппаратные средства защиты информации / Платонов В.В. М.: Издательский центр "Академия", 2006. — 240 с.

4. Мельников В.П. Информационная безопасность и защита информации / Мельников В.П. Учебное пособие для студ. высш. учеб.заведений 3-е изд., стер. — М.: Издательский центр «Академия», 2008. — 336 с.

5. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

6. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

7. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

8. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.

9. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

10. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс. - 1993.-N8. -С.60-62.

11. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

12. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

13. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-ЫЗ.-С.49-52.

14. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

15. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

16. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

5.3. Интернет-ресурсы

1. http://www.whatis.ru/razn/razn2O.html - Вредоносные программы и вирусы.
2. http://bugtraq.ru/library/internals/admintrap.html - Проблемы защиты сетевых соединений в Windows NT.

5.4. Материально-техническое обеспечение дисциплины Компьютерный класс.