МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-КАВКАЗСКИЙ ФИЛИАЛ ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СВЯЗИ И ИНФОРМАТИКИ»

А.Г. ЖУКОВСКИЙ
Д.А. ЖУКОВСКИЙ
С.А. ШВИДЧЕНКО

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ

Учебное пособие

Ростов-на-Дону
2022

УДК 004
ББК 32.97
Ж 86

Жуковский А.Г., Жуковский Д.А., Швидченко С.А. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. *Учебное пособие*. – Ростов-на-Дону: СКФ МТУСИ, 2022. – 52 с.

В учебном пособии, предназначенном для студентов, изучающих дисциплины «Основы информационной безопасности сетей и систем» и «Основы информационной безопасности», изложены краткие теоретические сведения об особенностях защиты информации.

Приводятся сведения о видах и особенностях применения идентификации и аутентификации. Рассмотрены возможности антивирусной защиты и правила ее использования. Показаны методы шифрования и стеганографии и области их применения, а также методы восстановления информации на компьютере и способы ее резервного копирования.

Изложен порядок проведения исследований по порядку хранения, резервирования, шифрования, и защиты компьютерных данных, содержание требования к отчету, приведен перечень контрольных вопросов по проведенному лабораторному исследованию.

Лабораторные исследования позволят студентам, обучающимся по направлениям подготовки бакалавров: 11.03.02 «Инфокоммуникационные технологии и системы связи», 09.03.01 «Информатика и вычислительная техника», 10.03.01 «Информационная безопасность» более глубоко изучить дисциплины «Основы информационной безопасности сетей и систем» и «Основы информационной безопасности», соответственно, закрепить полученные знания, а также получить практические навыки в работе с информационно-коммуникационными системами.

Пособие также будет интересно широкому кругу студентов технических специальностей и инженерам, интересующимся принципами защиты цифровых данных.

Рецензенты:
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи», д.т.н., доцент А.В. Елисеев;
Ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи», д.т.н. доцент В.А. Погорелов;

СОДЕРЖАНИЕ

1 Защита и сокрытие файлов, папок

1.1 Краткие теоретические сведения

Проблема защиты конфиденциальных данных при работе за компьютером всегда остается актуальной. Можно с уверенностью утверждать, что у большинства пользователей имеется информация, которой бы они не хотели делиться с остальными. Это может быть как важная финансовая или деловая документация, так и сведения личного характера. В любом случае, если не позаботиться о безопасности этих данных заранее, то вполне возможно, что они совершенно случайно или в результате целенаправленных действий могут попасть к тому лицу, которое может их использовать в личных интересах. Особенно часто это бывает тогда, когда за компьютером работают несколько человек или он остается включенным без присмотра.

Для решения данной проблемы используются специализированные утилиты, работающие как с установкой на компьютер, так и с флеш-памяти.

1.2 Лабораторное исследование № 1. Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок

Цель исследования:

изучить возможности специализированного программного обеспечения по защите и сокрытию файлов и папок. Выяснить, какие из утилит наиболее эффективны.

Время работы: 2 часа

Задания на выполнение лабораторного исследования

1. По указанию преподавателя выбрать 3 программы из прилагаемого списка:

1. Anvide Seal Folder
2.Wise Folder Hider
3. Secure Folders
4. Anvide Lock Folder
5. Folder Lock
6. Easy File Locker
7. Folder Guard
8. DEKSI USB Security
9. Locker (защита папок и дисков)

10. Advanced Hider
11. Hide Folders XP
12. Hide Files
13. Secret Disk 5.01
14. NYSMNYD
15. SecretFolder

Если студент желает провести анализ аналогичных по функционалу программ, не входящих в предложенный список, то это можно сделать по согласованию с преподавателем.

2. Установить на компьютер программное обеспечение по защите и сокрытию файлов и папок в соответствии со своим вариантом (при возможности).

3. На сайте производителя данного ПО или из других источников в сети Интернет, узнать основные характеристики и возможности установленного ПО.

4. Произвести запуск основных модулей программы и исследовать, каким функционалом обладает данное ПО (при возможности).

5. Провести сравнительный анализ с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Сделать выводы по работе.

1.3 Содержание отчета

Отчет должен содержать:
1. Цель работы

2. Назначение программного обеспечения по защите и сокрытию файлов и папок.

3. Перечень исследуемых программ с указанием сайта производителя.

4. Скриншоты с кратким описанием основных функций и настроек для каждой из 3-х программ. Данный пункт может выполняться непосредственно при установке программ на компьютер или требуемые

данные выбираются из технических описаний программ на сайтах производителей или других информационных ресурсов.

5. Результаты сравнительного анализа с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Выводы по проведенному исследованию.

1.4 Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Какими альтернативными способами можно скрыть или защитить файлы и папки?
2. Как можно защитить папки и файлы встроенными средствами Windows путем изменения атрибутов?

3. Как можно защитить папки и файлы встроенными средствами Windows путем использования шифрованной файловой системы?

4. Как можно защитить папки и файлы встроенными средствами Windows путем использования функции BitLocker?

5. Какие механизмы сокрытия или защиты файлов и папок предусмотрены средствами ОС Linux?

2 Шифрование, безвозвратное удаление данных, стеганография

2.1 Краткие теоретические сведения

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Под **шифрованием** понимается такое преобразование информации, которое делает исходные данные нечитаемыми и трудно раскрываемыми без знания специальной секретной информации – **ключа.** В результате шифрования открытый текст превращается в шифрограмму и становится нечитаемым без использования дешифрирующего преобразования. **Шифрограмма** может называться иначе: зашифрованный текст, криптограмма, шифровка или шифртекст. Шифрограмма позволяет скрыть смысл передаваемого сообщения.

Сфера интересов **криптоанализа** противоположная – разработка и исследование методов дешифрования (раскрытия) шифрограммы даже без знания секретного ключа.

Под **ключом** понимается секретная информация, определяющая, какое преобразование из множества возможных шифрующих преобразований выполняется в данном случае над открытым текстом.

Дешифрование – обратный шифрованию процесс. При дешифрировании на основе ключа зашифрованный текст (шифрограмма, шифровка) преобразуется в исходный открытый текст.

Процесс получения криптоаналитиками открытого сообщения из шифрованного сообщения без заранее известного ключа называется **вскрытием** или **взломом** шифра.

Существует несколько классификаций шифров.

По характеру использования ключа алгоритмы шифрования делятся на два типа: **симметричные** (с одним ключом, по-другому – с секретным ключом) и **несимметричные** (с двумя ключами или с открытым ключом).

Несимметричные алгоритмы шифрования и дешифрования порой называют **асимметричными.**

В первом случае в шифраторе отправителя и дешифраторе получателя используется один и тот же ключ (Ключ 1, см. рисунок 2.1). Шифратор образует шифрограмму, которая является функцией открытого текста. Конкретный вид функции преобразования (шифрования) определяется секретным ключом. Дешифратор получателя сообщения выполняет обратное преобразование по отношению к преобразованию, сделанному в шифраторе. Секретный ключ хранится в тайне и передается отправителем сообщения получателю по каналу, исключающему перехват ключа криптоаналитиком противника или коммерческого конкурента.

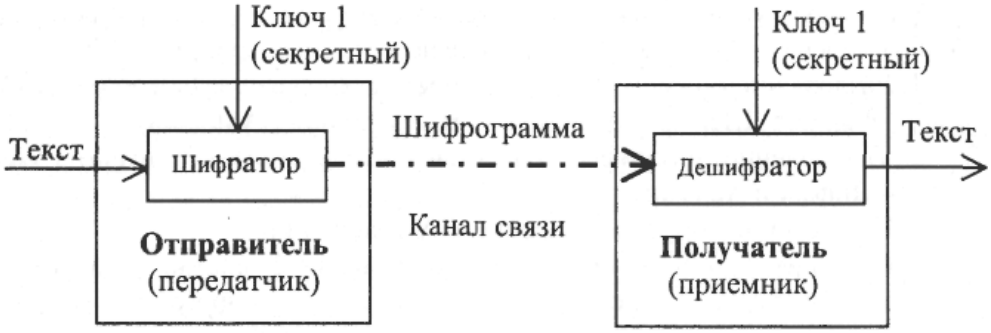

Рисунок 2.1

Во втором случае (при использовании асимметричного алгоритма), представленного на рисунке 2.2, получатель вначале по открытому каналу передает отправителю открытый ключ (Ключ 1), с помощью которого отправитель шифрует информацию.

При получении информации получатель дешифрирует ее с помощью второго секретного ключа (Ключ 2). Перехват открытого ключа (Ключ 1) криптоаналитиком противника не позволяет дешифровать закрытое сообщение, так как оно рассекречивается лишь вторым секретным ключом (Ключ 2). При этом секретный Ключ 2 практически невозможно вычислить с помощью открытого Ключа 1.

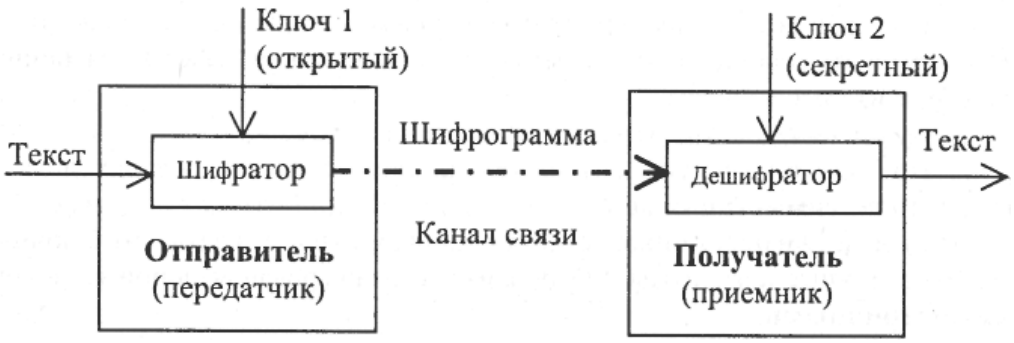

Рисунок 2.2

При оценке эффективности шифра обычно руководствуются правилом голландца Огюста **Керкхоффа** (1835 – 1903), согласно которому стойкость шифра определяется только секретностью ключа, т.е. криптоаналитику известны все детали процесса (алгоритма) шифрования и дешифрования, но неизвестно, какой ключ использован для шифрования данного текста.

Криптостойкостью называется характеристика шифра, определяющая его устойчивость к дешифрованию без знания ключа (т.е. устойчивость к криптоанализу). Имеется несколько показателей криптостойкости, среди которых количество всех возможных ключей и среднее время, необходимое для криптоанализа.

Алгоритмы шифрования с открытым ключом используют так называемые **необратимые или односторонние функции.** Эти функции обладают следующим свойством: при заданном значении аргумента *x* относительно просто вычислить значение функции *f(x).* Однако если известно значение функции *y = f(x),* то нет простого пути для вычисления значения аргумента *x.*

Все используемые в настоящее время криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований.

1. Разложение больших чисел на простые множители (алгоритм **RSA**, авторы – Райвест, Шамир и Адлеман – **R**ivest, **S**hamir, **A**dleman).
2. Вычисление логарифма или возведение в степень (алгоритм **DH**, авторы – Диффи и Хелман).
3. Вычисление корней алгебраических уравнений.

Рассмотрим простейший пример необратимых функций. Легко в уме найти произведение двух простых чисел 11 и 13. Но попробуйте быстро в уме найти два простых числа, произведение которых равно 437. Такие же трудности возникают и при использовании вычислительной техники для отыскания двух простых сомножителей для очень большого числа: найти сомножители можно, но потребуется много времени.

Таким образом, в системе кодирования, основанной на разложении на множители, используются два разных ключа: один для шифрования сообщения, а второй – отличный от первого, но связанный с ним – для дешифрования. Ключ шифрования основан на произведении двух огромных простых чисел, а ключ дешифрования – на самих простых числах.

Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

Стеганография это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Выделяют несколько направлений стеганографии:

- классическая стеганография;
- компьютерная стеганография;
- цифровая стеганография.

Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры — стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д.

Одним из наиболее распространенных методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т.д.).

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Но, как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

2.2 Лабораторное исследование №2. Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии

Цель:

изучить возможности специализированного программного обеспечения по шифрованию, безвозвратному удалению, стеганографии. Выяснить, какие из утилит наиболее эффективны.

Время работы: 2 часа

Задания на выполнение лабораторного исследования

1. По указанию преподавателя выбрать 3 программы из прилагаемого списка:

1. TrustPort Tools
2. Cryptic Disk
3. Locker (скрытие файлов)
4. Max File Encryption
5. Secure Disk
6. Masker 7.1
7. Fox Secret
8. HideInPicture 1.0
9. Шифровальщик
10. Advanced Encryption Package
11. Gpg4win
12. Cryptic Disk Professional
13. CyberSafe Files Encryption
14. Steganos Privacy Suite
15. Lavasoft Privacy Toolbox
16. pkiImage Free Edition

Если студент желает провести анализ аналогичных по функционалу программ, не входящих в предложенный список, то это можно сделать по согласованию с преподавателем.

2. Установить на компьютер программное обеспечение по шифрованию, безвозвратному удалению, стеганографии в соответствии со своим вариантом (при возможности).

3. На сайте производителя данного ПО или из других источников в сети Интернет, узнать основные характеристики и возможности установленного ПО.

4. Произвести запуск основных модулей программы и исследовать, каким функционалом обладает данное ПО (при возможности).

5. Провести сравнительный анализ с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Сделать выводы по работе.

2.3 Содержание отчета

1. Цель работы

2. Назначение программного обеспечения по шифрованию, безвозвратному удалению, стеганографии.

3. Перечень исследуемых программ с указанием сайта производителя.

4. Скриншоты с кратким описанием основных функций и настроек для каждой из 3-х программ. Данный пункт может выполняться непосредственно при установке программ на компьютер или требуемые данные выбираются из технических описаний программ на сайтах производителей или других информационных ресурсов.

5. Результаты сравнительного анализа с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Выводы по проведенному исследованию.

2.4 Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Дать определение криптографии.

2. Дать определение шифрованию.

3. Дать определение криптостойкости.

4. Дать определение хеш-функции.

5. Дать определение ключа.

6. В чем отличие симметричного и несимметричного методов шифрования?

7. Дать определение стеганографии.

8. Изложить принцип цифровой стеганографии.

3 Механизмы идентификации и аутентификации

3.1 Краткие теоретические сведения

Основой любых систем защиты информационных систем (ИС) являются ***идентификация и аутентификация***, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами ИС. В качестве субъектов ИС могут выступать как пользователи, так и процессы, а в качестве объектов ИС – информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам личного идентификатора и сравнение его с заданным перечнем называется *идентификацией.* Идентификация обеспечивает выполнение следующих функций:

- установление подлинности и определение полномочий субъекта при его допуске в систему;
- контроль установленных полномочий в процессе сеанса работы;
- регистрация действий пользователя и др.

Аутентификацией (*установлением подлинности)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Общая процедура идентификации и аутентификации пользователя при его доступе в ИС представлена на рисунке 3.1. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

Способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. Аутентификация партнеров по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация источника данных – это подтверждение подлинности источника отдельной порции данных.

По направленности аутентификация может быть односторонней (пользователь доказывает свою подлинность системе, например при входе в систему) и двусторонней (взаимной).

Рисунок 3.1 - Классическая процедура идентификации и аутентификации

Обычно методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

1. Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой секретной информации – пароля;
2. Основанные на использовании уникального предмета: жетона, электронной карточки и др.;
3. Основанные на измерении биометрических параметров человека – физиологических или поведенческих атрибутах живого организма;
4. Основанные на информации, ассоциированной с пользователем, например, с его координатами.

Рассмотрим эти группы.

Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на *паролях* – секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам ИС.

Парольные методы следует классифицировать по степени изменяемости паролей:

- методы, использующие постоянные (многократно используемые) пароли;

- методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве ИС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известно множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т. д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы. В последнем случае, возможно запустить программу по подбору паролей – «дробилку».

Более надежный способ – использование одноразовых или динамически меняющихся паролей.

Известны следующие методы парольной защиты, основанные на одноразовых паролях:

- методы модификации схемы простых паролей;
- методы «запрос-ответ»;
- функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования $f(x)$. Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

- для заданного пароля x легко вычислить новый пароль $y = f(x)$;
- зная x и y, сложно или невозможно определить функцию $f(x)$.

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод «рукопожатия».

Идея метода функционального преобразования состоит в периодическом изменении самой функции $f(x)$. Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например, функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и

периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданных n-периодах времени будут следующие: x, $f(x)$, $f(f(x))$, ..., $f(x)^{n-1}$.

Метод «рукопожатия» состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в ИС подсистема аутентификации генерирует случайную последовательность x, которая передается пользователю. Пользователь вычисляет результат функции $y=f(x)$ и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой ИС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод «рукопожатия», так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

В последнее время получили распространение комбинированные методы идентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

К достоинству использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

Недостатки пассивных карточек следующие: они существенно дороже паролей, требуют специальных устройств чтения, их использование подразумевает специальные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, и, естественно, не оставлять в устройствах чтения. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты: многоразовые пароли, динамически меняющиеся пароли, обычные запрос-ответные методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

Методы аутентификации, основанные на измерении биометрических параметров человека (см. таблицу 3.1), обеспечивают почти 100 % идентификацию, решая проблемы утраты паролей и личных идентификаторов. Однако такие методы нельзя использовать при идентификации процессов или данных (объектов данных), так как они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах.

Таблица 3.1 - Примеры методов биометрии

Физиологические методы	Поведенческие методы
Снятие отпечатков пальцев Сканирование радужной оболочки глаза Сканирование сетчатки глаза Геометрия кисти руки Распознавание черт лица	Анализ подписи Анализ тембра голоса Анализ клавиатурного почерка

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК.

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине

предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Назовем наиболее используемые биометрические атрибуты и соответствующие системы:

- *отпечатки пальцев.* Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10^{-5} %. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев;

- *геометрия руки.* Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2 %;

- *радужная оболочка глаза.* Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 10^{78};

- *термический образ лица*. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок;

- *голос.* Проверка голоса удобна для использования в телекоммуникационных приложениях. Вероятность ошибки составляет 2 – 5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу – возбужден, болен, говорит правду, не в себе и т.д.;

- *ввод с клавиатуры.* Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями;

- *подпись.* Для контроля рукописной подписи используются дигитайзеры.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет возможность их перехвата. Аппаратура GPS проста и надежна в использовании и

сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

1. Статическая аутентификация;
2. Устойчивая аутентификация;
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от несанкционированного доступа (НСД) в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т.д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и пытаться использовать ее в следующих сеансах работы. Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

Парольная система как неотъемлемая составляющая системы защиты информации является частью “переднего края обороны” всей системы безопасности. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Пароль пользователя - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя-совокупность его идентификатора и его пароля.

База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под *парольной системой* будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей ИС на основе одноразовых или многоразовых паролей. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Некоторые элементы парольной системы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем.

1. Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте;

2. Вмешательство в функционирование компонентов парольной системы через:

- внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием, так называемого, человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Еще одним важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Возможны следующие варианты хранения паролей:

- в открытом виде;
- в виде свёрток (хеширование);
- зашифрованными на некотором ключе.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей.

Хеширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хеширования, который будет использован для вычисления сверток паролей, необходимо гарантировать несовпадение значений сверток, полученных на основе различных паролей пользователей. Кроме того, следует предусмотреть механизм, обеспечивающий уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли. Для этого при вычислении каждой свертки обычно используют некоторое количество "случайной" информации, например, выдаваемой генератором псевдослучайных чисел

При шифровании паролей особое значение имеет способ генерации и хранения ключа шифрования базы данных учетных записей. Перечислим некоторые возможные варианты:

- ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки;
- ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске;
- ключ генерируется на основе выбранного администратором пароля. который вводится в систему при каждом запуске.

Во втором случае необходимо обеспечить невозможность автоматического перезапуска системы, даже если она обнаруживает носитель с ключом. Для этого можно потребовать от администратора подтверждать продолжение процедуры загрузки, например, нажатием клавиши на клавиатуре.

Наиболее безопасное хранение паролей обеспечивается при их хешировании и последующем шифровании полученных сверток, т.е. при комбинации второго и третьего способов.

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей (таблица 3.2).

Таблица 3.2 - Требования к выбору пароля

Требования	Получаемый эффект
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом "тотального опробования"
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом "тотального опробования"
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника по подбору паролей методом тотального опробования, в том числе без непосредственного обращения к системе защиты
Установление минимального срока действия пароля	Заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала	добрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самим пользователем и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом "тотального опробования"
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи

Какой пароль можно однозначно назвать слабым во всех отношениях (за исключением запоминаемости)?

Типичный пример: пароль из небольшого количества (до 5) символов/цифр. По некоторым данным, из 967 паролей одного из взломанных почтовых серверов сети Интернет 335 (почти треть) состояла исключительно из цифр. Количество паролей включающих буквы и цифры оказалось равным 20. Остальные пароли состояли из букв в основном в нижнем регистре за редким исключением (в количестве 2 паролей) включающих спецсимволы (“*”, “_”). Символ “_”, однако, часто встречался в именах пользователей. В 33 случаях имя и пароль пользователя совпадали. Самым популярным оказался пароль 123 (встречался 35 раз, почти каждый 27 пароль). На втором месте пароль qwerty (20 паролей). Как удобно он набирается, не правда ли? Далее следуют: 666 (18 раз), 12 (17 раз), xakep (14 раз) и 1, 11111111, 9128 (по 10 раз). 16 паролей состояли из одного символа/цифры.

Какой же пароль может оказать достойное сопротивление попыткам его подбора? Длинный, состоящий из букв разного регистра, цифр и спецсимволов. При этом он должен быть случайным, т.е. выбор символов осуществляется произвольно (без какой бы то ни было системы) и более нигде не использоваться, при этом единственным местом фиксации пароля должна быть голова единственного человека. Однако необходимо учитывать и вопросы практического использования пароля. Очень длинный пароль сложно запомнить, особенно, если учесть тот факт, что пользователю приходится иметь не один пароль. Осуществить быстрый ввод длинного пароля также не представляется возможным. Произвольно выбранные символы запомнятся, если их произнесение вслух имеет запоминаемую звуковую форму (благозвучие) или они имеют характерное расположение на клавиатуре, в противном случае без шпаргалки не обойтись.

В случае если пользователю самостоятельно необходимо сформировать пароль, в качестве критериев выбора пароля можно выделить следующие:

- использование букв разных регистров;
- использование цифр и спецсимволов совместно с буквами.

При составлении пароля не рекомендуется использовать:

- свое регистрационное имя в каком бы то ни было виде (как есть, обращенное, заглавными буквами, удвоенное, и т.д);
- свое имя, фамилию или отчество в каком бы то ни было виде;
- имена близких родственников;
- информацию о себе, которую легко можно получить. Она включает номера телефонов, номера лицевых счетов, номер вашего автомобиля, название улицы, на которой вы живете, и т.д.;
- пароль из одних цифр или из одних букв;
- слово, которое можно найти в словарях.

Помочь пользователю составить пароль по определенным критериям могут программы генерации паролей.

Существуют методы количественной оценки стойкости парольных систем (формула Андерсона):

$$4{,}32 \times 10^4 \times (k)\frac{M}{P} \le A^1 \qquad (3.1)$$

где k – количество попыток подбора пароля в минуту;

M – время действия пароля в месяцах;

P – вероятность подбора пароля;

A^1 – мощность пространства (алфавита) паролей (количество символов, которые могут быть использованы при составлении пароля, например, если пароль состоит только из малых английских букв, то A=26, l – длина пароля).

Таким образом, наибольшее влияние на вероятность раскрытия пароля оказывает величина l. Другие составляющие данной формулы чрезвычайно редко оказывают влияние на величину P, превышающее один порядок. Увеличение же длины пароля только на один символ значительно увеличивает требуемое злоумышленнику время для его раскрытия.

Параметры P, V, T и A^1 связаны между собой следующим соотношением:

$$P = \frac{V \times T}{A^1} \qquad (3.2)$$

где P – вероятность подбора пароля в течение его срока действия (подбор осуществляется непрерывно в течение всего срока действия пароля);

V – скорость подбора паролей. Для интерактивного режима определяется как скорость обработки одной попытки регистрации проверяющей стороной. Для режима off-line (на основе свертки пароля) определяется как скорость вычисления значения свертки для одного пробного пароля);

T – срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть сменен);

A^1 – мощность пространства паролей (A – мощность алфавита паролей, l – длина пароля).

В случае, когда неизвестна точная длина искомого пароля, максимальное время подбора пароля (T_{max}) будет вычисляться в соответствии со следующей формулой:

$$T_{max} = \frac{\sum_{i=1}^{l} A}{V} \qquad (3.3)$$

3.2 Лабораторное исследование № 3. Защита информации на основе механизмов идентификации и аутентификации

Цель: изучение процедур идентификации и аутентификации; исследование основных этапов доступа к ресурсам вычислительной системы; использование простого пароля; использование паролей различной степени сложности; изучение рекомендаций по созданию устойчивого к взлому пароля.

Время: 2 часа.

Задания на выполнение лабораторного исследования

1. Рассчитать оценку стойкости парольной системы защиты для индивидуального варианта. Каждый вариант содержит 2 задания (см. таблицу 3.3). Первое характерно для ручного подбора паролей, а второе – для подбора с использованием метода перебора, реализуемого с помощью компьютера. Для каждого задания предложить свой, удовлетворяющий требованиям пароль.

Таблица 3.3 – Варианты задания по расчёту оценки стойкости парольной системы защиты

Вариант	V	T
1	15 паролей/мин 1000000 паролей/сек	2 недели 30 дней
2	3 паролей/мин 500000 паролей/сек	10 дней 1 год
3	10 паролей/мин 10000000 паролей/сек	5 дней 40 дней
4	11 паролей/мин 50000 паролей/сек	6 дней 90 дней
5	100 паролей/день 10000 паролей/сек	12 дней 10 дней
6	10 паролей/день 5000000 паролей/сек	1 месяц 150 дней
7	20 паролей/мин 20000 паролей/сек	3 недели 10 дней
8	15 паролей/мин 1000 паролей/сек	20 дней 3 дня
9	3 паролей/мин 10000000 паролей/сек	15 дней 120 дней

Продолжение таблицы 3.3

10	10 паролей/мин 100000000 паролей/сек	1 неделя 1 год
11	11 паролей/мин 300000 паролей/сек	2 недели 100 дней
12	100 паролей/день 70000 паролей/сек	10 дней 20 дней
13	10 паролей/день 30000000 паролей/сек	5 дней 200 дней
14	20 паролей/мин 80000 паролей/сек	6 дней 60 дней
15	15 паролей/мин 500000000 паролей/сек	12 дней 5 лет
16	3 паролей/мин 10000000 паролей/сек	1 месяц 10 лет
17	10 паролей/мин 50000000 паролей/сек	3 недели 100 лет
18	11 паролей/мин 1000000 паролей/сек	20 дней
19	100 паролей/день 20000 паролей/сек	15 дней 15 дней
20	10 паролей/день 20000000 паролей/сек	1 неделя 365 дней

Для расчета использовать формулу (3.2), приравняв вероятность раскрытия пароля в указанный срок, равной единице.

Занесите проведенные расчеты в отчет по лабораторной работе и **сделайте соответствующие выводы**.

2. В настоящее время существует целый класс программ, позволяющих проверить стойкость пароля любой сложности. Очень удобно пользоваться онлайн программами, которые не требуют загрузки и установки. Для исследования используем программы, расположенные по следующим адресам:

https://password.kaspersky.com/ru/

https://2ip.online/passcheck/

В качестве индивидуального задания предлагается самостоятельно создать несколько категорий паролей:

- пароль, состоящий только из цифр;
- пароль, состоящий только из цифр и букв;
- пароль, состоящий из цифр и букв с различным регистром;
- пароль состоящий из цифр, букв с различным регистром и специальных символов.

По каждой категории паролей предложить 4 разновидности паролей:
состоящий из 5-ти знаков;
состоящий из 7-ми знаков;
состоящий из 9-ти знаков.

С помощью перечисленных выше программных средств провести исследование стойкости паролей для каждой категории и после исследования паролей в каждой из онлайн программ занести полученные данные в таблицу. Пример такой таблицы для программы по адресу https://password.kaspersky.com/ru/ представлен в таблице 3.

Таблица 3 – Исследование стойкости паролей с использованием программы по адресу https://password.kaspersky.com/ru/

Длина пароля	Время подбора пароля на компьютере		
	5 знаков	7 знаков	9 знаков
пароль, состоящий только из цифр			
пароль, состоящий только из цифр и букв			
пароль, состоящий из цифр и букв с различным регистром			
пароль состоящий из цифр, букв с различным регистром и специальных символов			

Такую же таблицу построить при исследовании онлайн программы https://2ip.online/passcheck/

3. Проведите в интернете поиск аналогичной онлайн программы и проведите 3-е исследование для усреднения полученных результатов. Данные занесите в таблицу. **Сделайте соответствующие выводы**.

3.3 Содержание отчета

- название и цель работы;
- расчет количественной оценки стойкости парольной системы. Выводы по исследованию.
- материалы проверки стойкости по времени подбора паролей с помощью специализированных программных средств. Выводы по исследованию

3.4 Контрольные вопросы

1. Что такое идентификация?
2. Что понимается под аутентификацией?
3. Чем определяется стойкость подсистемы идентификации и аутентификации?
4. Перечислите минимальные требования к выбору пароля.
5. Почему парольная защита с динамически изменяющимся паролем выше, чем с долговременным паролем?
6. Аспекты классификации методов идентификации и аутентификации?
7. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
8. Выбором, каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

4 Защита информации от компьютерных вирусов

4.1 Краткие теоретические сведения

Компьютерный вирус - это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

Классификация вирусов:

– по среде обитания;
– по способу заражения среды обитания;
– по воздействию;
– по особенностям алгоритма;

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные.

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

- *неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
- *опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера;
- *очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

вирусы-репликаторы, называемые *червями*, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны *вирусы-невидимки*, называемые *стелс-вирусами*, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Наиболее трудно обнаружить *вирусы-мутанты*, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые *квазивирусные* или *«троянские»* программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Загрузочные вирусы

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего загрузочные носители (например, USB-флеш).

Пусть имеются чистый носитель и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как

только этот вирус обнаружит, что появился не защищенный от записи и еще не зараженный носитель, он приступает к заражению. Заражая носитель, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad);
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору.

Файловые вирусы

Рассмотрим теперь схему работы простого файлового вируса.

В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление «хозяину»

Какие же действия выполняет вирус? Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код - следовательно, заражение исполняемого файла всегда можно обнаружить.

Но, изменяя код файла, вирус не обязательно вносит другие изменения:

- он не обязан менять длину файла;
- неиспользуемые участки кода;
- не обязан менять начало файла;

Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

Загрузочно-файловые вирусы

Основное разрушительное действие - шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а, зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из файлов, надо расшифровать зашифрованную им информацию.

Полиморфные вирусы

Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Стелс-вирусы

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

Троянские кони, программные закладки и сетевые черви

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских

коней или "троянизировать" другие программы – вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в компьютерных сетях, – взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;

– существенное уменьшение размера свободной оперативной памяти;
– вывод на экран непредусмотренных сообщений или изображений;
– подача непредусмотренных звуковых сигналов;
– частые зависания и сбои в работе компьютера.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

– общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
– профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
– специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

– копирование информации - создание копий файлов и системных областей дисков;
– разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Антивирусные программы

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение.

Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска).

Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Доктора-ревизоры, - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Программы-фильтры, располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Программы-вакцины, или *иммунизаторы*, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Действия при заражении вирусом

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать 4-е правила:

1) Прежде всего не торопиться и не принимать опрометчивых решений. Непродуманные действия могут привести не только к потере части файлов, но к повторному заражению компьютера.

2) Немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.

3) Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенного от записи носителя с ОС (обязательное правило).

4) Если пользователь не обладает достаточными знаниями и опытом для лечения компьютера, для решения проблемы необходимо привлечь более опытных коллег.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая защита информации.

4.2 Лабораторное исследование №4. Исследование характеристик и возможностей антивирусного ПО

Цель:

изучить возможности специализированного программного обеспечения по борьбе с компьютерными вирусами. Выяснить, какие из утилит наиболее эффективны.

Время работы: 4 часа

Задания на выполнение лабораторного исследования

1. По указанию преподавателя выбрать 3 программы из прилагаемого списка:

1. AVAST Antivirus
2. AVG AntiVirus
3. Dr.Web Antivirus
4. Антивирус Касперского
5. ESET NOD32 Антивирус
6. AVZ Antivirus
7. Avira Antivirus
8. Norton AntiVirus
9. McAfee Antivirus
10. Emsisoft Anti-Malware
11. BullGuard Antivirus
12. Protector Plus Antivirus
13. Panda Antivirus
14. Ashampoo Anti-Virus

14. G Data AntiVirus
16. K7 AntiVirus
17. VIRUSfighter
18. Twister Antivirus

Если студент желает провести анализ аналогичных по функционалу программ, не входящих в предложенный список, то это можно сделать по согласованию с преподавателем.

2. Установить на компьютер программное обеспечение по борьбе с компьютерными вирусами в соответствии со своим вариантом (при возможности).

3. На сайте производителя данного ПО или из других источников в сети Интернет, узнать основные характеристики и возможности установленного ПО.

4. Произвести запуск основных модулей программы и исследовать, каким функционалом обладает данное ПО (при возможности).

5. Провести сравнительный анализ с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Сделать выводы по работе.

4.3 Содержание отчета

1. Цель работы

2. Назначение программного обеспечения по борьбе с компьютерными вирусами.

3. Перечень исследуемых программ с указанием сайта производителя.

4. Скриншоты с кратким описанием основных функций и настроек для каждой из 3-х программ. Данный пункт может выполняться непосредственно при установке программ на компьютер или требуемые данные выбираются из технических описаний программ на сайтах производителей или других информационных ресурсов.

5. Результаты сравнительного анализа с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Выводы по проведенному исследованию.

4.4 Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Дать определение компьютерного вируса.

2. Классификация вирусов.

3. Какими бывают вирусы в зависимости от среды обитания?

4. Какими бывают вирусы по способу заражения?

5. Какими бывают вирусы по особенностям алгоритма?

6. В чем особенности полиморфных вирусов?

7. В чем особенность вирусов «троянские кони»?

8. Перечислить методы защиты от компьютерных вирусов.

9. Перечислить признаки появления вирусов.

10. Какими по функционалу бывают антивирусные программы?

5 Восстановление потерянных данных на различных носителях

5.1 Краткие теоретические сведения

Данные пропадают по следующим основным причинам: Случайное удаление самим пользователем или какой-либо программой, им запущенной. Из-за воздействия вредоносного ПО или вируса. Физическая неисправность самого диска. Некорректное выключение, которое также приводит к повреждению файловой системы на диске. Первые два случая - это обычное удаление данных, и решение проблемы здесь будет одно. Если же неисправен сам диск, к примеру, нарушена его физическая структура или логическая таблица, то восстановить данные будет сложнее.

Физическую неисправность диска распознать очень легко. Обычно она выражается в исчезновении целого раздела. Флешка может вообще не определяться компьютером, а если поврежден диск с системой, то в итоге машина не будет загружаться, показывая на черном экране отсутствие раздела, с которого бы он мог загрузиться. В таком случае восстановление потерянных данных потребует использования специальных программ и утилит, а то и профессионального оборудования.

Перечислим физические неисправности наиболее распространенных носителей

Накопители CD/DVD/BR

Оптические накопители могут иметь разные причины невозможности чтения данных:

- механические:
    - повреждение прозрачного слоя;
    - повреждение отражающего слоя;
- химические:
    - разложение прозрачного слоя;
    - разложение регистрируемого слоя (у записываемых дисков);
    - коррозия отражающего слоя;
- нарушение организации данных:
    - вследствие аппаратно-программных ошибок при записи данных
    - вследствие неправильных данных.

Самыми частыми причинами нечитаемости дисков являются повреждение отражающего и прозрачного слоя, а также разложение регистрируемого слоя у записываемых дисков. В случае образования царапин на поверхности компакт-диска, возможно применить полирование рабочей поверхности, что приведёт к удалению нежелательных повреждений и улучшит чтение данных, однако при образовании трещин,

использовать данный метод опасно, так как при последующем чтении диск может разрушиться в дисководе под действием центробежной силы. Повреждение фольгированного покрытия диска (старение металла, царапины) больше всего осложняет восстановление данных.

NAND-Flash

К данному типу накопителей можно отнести USB Flash, SSD-диски, карты памяти SD, miniSD, microSD, xD, MS, M2, Compact Flash.

Самые распространенные технические неисправности флеш-памяти :

- логические неисправности. Накопитель не имеет видимых физических повреждений и опознается в системе. Проблема возникает при попытке доступа или записи/считывания данных. Возникают данные неисправности в самых различных случаях. Одна из самых распространенных причин — неправильное извлечение устройства из компьютера. В случае логических неисправностей восстановить данные возможно с помощью программ для восстановления данных.

- механические повреждения. Диск прекратил корректную работу в результате какого-либо физического воздействия (падения, попадания влаги, изгиба, сжатия и т. д.). Причина неисправности, чаще всего, в поломке платы или разрушении контактов и компонентов. Восстановить данные можно, если исправить поломку: заменить неисправный компонент или восстановить нарушенный контакт. Также можно считать данные напрямую с чипа памяти, используя специальное оборудование.

- электрические повреждения. Причина электрических повреждений заключается в статическом ударе либо в проблеме с питанием. В результате могут сгореть стабилизаторы питания, диоды, контроллеры.

Восстановление данных производится как и в предыдущем случае: заменой компонентов либо чтением с чипов памяти напрямую (если сама память не сгорела).

Накопитель на жёстком магнитном диске (НЖМД)

На сегодняшний день эти накопители считаются самыми ёмкими и достаточно быстрыми, но очень уязвимыми к электрическому и механическому воздействиям. При превышении напряжения питания, либо нестабильном напряжении может возникнуть тепловой пробой платы контроллера, а также пробой коммутатора-предусилителя внутри гермоблока. В первом случае выходит из строя плата контроллера жёсткого диска и процедура восстановления данных заканчивается на её замене с переносом адаптивных параметров неисправного накопителя на новую плату. Однако встречаются случаи, когда в результате пробоя выходит из строя электроника гермоблока, в этом случае необходима замена БМГ (блока магнитных головок), что по сути своей является трудоёмкой и дорогостоящей процедурой.

При механических повреждениях, таких как падение, удар, деформация, вмешательство специалиста в гермоблок необходимо, так как для выяснения возможности восстановления данных, необходимо проанализировать состояние магнитных дисков. В случае возникновения концентрических, радиальных царапин или ссадин на поверхности пластин, вероятность восстановления данных уменьшается, так как для успешного считывания данных необходима идеально гладкая и ровная поверхность магнитных дисков. Так же встречаются неисправности, связанные с заклиниванием шпинделя бесколлекторного электродвигателя. В этом случае специалисты прибегают к трансплантации всего пакета магнитных дисков на исправный ШД (шпиндельный двигатель), после чего осуществляется его калибровка и настройка БМГ.

Достаточно часто встречается неисправность, связанная с разрушением так называемой служебной информации накопителя. Некоторые части (далеко не все) служебной информации могут быть взяты от аналогичных накопителей и записаны в неисправный при помощи специального оборудования, которым, как правило, располагают сервисные центры, занимающиеся восстановлением данных на профессиональном уровне. Как показывает практика, попытки неквалифицированного вмешательства в структуру служебной информации накопителя, как ни прискорбно, влекут за собой окончательную и безвозвратную потерю данных.

В случае разрушения магнитного диска восстановление данных невозможно в принципе.

Чтобы полнее понять процесс удаления файла, для начала необходимо ознакомиться со способом хранения файла на компьютерном устройстве хранения данных. Все данные на компьютерном жестком диске хранятся в файлах и папках и имеют строго структурированную форму. Жесткий диск персонального компьютера имеет первоначальную разметку на дорожки, которые в свою очередь делятся на сектора (пронумерованная область жесткого диска, предназначенная для хранения данных). Каждый сектор имеет определенный размер, который можно изменять в определенных границах при форматировании жесткого диска и выборе файловой системы. Минимальный размер сектора «512 байт».

Каждый файл, который вы записываете на компьютерный жесткий диск, также имеет определенный размер, значительно превышающий размер сектора, и занимает определенное количество секторов дорожки. Такие сектора могут располагаться не рядом друг с другом, а быть разбросанными по разным дорожкам диска. В момент записи файла система создает метки файла, в которых она хранит информацию о местоположении файла, его размере и другие важные данные. При обращении пользователя к файлу, на основании метки, система собирает

информацию секторов файла вместе и выдает пользователю необходимый файл.

Когда пользователь удаляет файл, любым ему удобным способом (обычным или безвозвратным удалением), то система только удаляет метку файла и помечает его, как пустое пространство диска, годное для записи новых данных. Фактически, вся информация пользователя, хранившаяся в файле, остается нетронутой, и все еще находится на диске.

Когда системе необходимо записать новый файл, то она проверяет дисковое пространство на наличие свободных ячеек. К ним теперь относятся и те ячейки, в которых хранится информация из удаленного файла. Следуя своей логике, система осуществляет перезапись свободных ячеек новыми данными. И ячейки с информацией из удаленного файла также могут быть использованы для перезаписи данными нового файла. Пока перезапись ячейки не произведена, вся хранимая в ней информация, даже помеченная как удаленная, доступна к полному восстановлению специальными программами для восстановления удаленных данных.

Процесс восстановления удаленных файлов подразумевает под собой выполнение определенных последовательных действий, одно за другим, пока пользователь не восстановит требуемые файлы.

Основные правила, которые повысят вероятность восстановления файлов и папок.

1. Прекратить использовать компьютер!

Необходимо перестать использовать диск, содержащий удаленный файл, для предотвращения его перезаписи.

Как уже упоминалось выше, удаленные файлы скрыты от пользователя, но все еще доступны. Единственный способ, при котором файл, который вы хотите восстановить, полностью исчезнет, – это перезапись того физического пространства, которое он занимает на диске. Поэтому постарайтесь воздержаться или сократить к минимуму количество операций записи, которые могли бы привести к таким последствиям.

Откажитесь от выполнения объемных задач, таких как установка программного обеспечения, загрузка или потоковое воспроизведение музыки или видео и т.д. Выполнение этих действий не обязательно перезапишет ваш файл, но шансы потерять его навсегда существенно повышаются.

По возможности, сократите время (количество обращений к устройству хранения и выполненных с ним операций) с момента удаления файла до начала процесса восстановления. Например, после удаления файла вы не использовали устройство хранения долгое время, но после его подключения вы запустили процесс восстановления. Шанс полностью восстановить такой файл практически стопроцентный, ведь система не

использовала устройство и не могла безвозвратно стереть файл. Особенно это условие актуально для больших файлов. Ведь при хранении система могла расположить фрагменты файла на разных секторах по всей поверхности физического диска, значительно повышая вероятность их перезаписи при последующем использовании.

2. Восстановить удаленные файлы из «Корзины».

Это первое место, которому необходимо уделить свое внимание. В стандартных настройках операционной системы «Windows» функция удаления файлов в «Корзину» предустановлена по умолчанию. И если вы дополнительно не меняли настройки удаления файлов, то с большой долей вероятности, вы сможете обнаружить свой удаленный файл в идеальном рабочем состоянии в «Корзине». Но если у вас задан параметр «Уничтожать файлы сразу после удаления, не помещая их в корзину», или вы уже очистили содержимое «Корзины» ранее, то файл в «Корзине» будет отсутствовать.

Файлы, которые удаляются с карт памяти, «USB» флэш-накопителей, внешних жестких дисков любого типа и сетевых ресурсов, не хранятся в «Корзине» и всегда удаляются напрямую. Это условие, в полной мере, также относится и к таким устройствам, как смартфон и коммуникатор. Опять же, файлы очень больших размеров из любого источника часто удаляются сразу напрямую, без помещения их в «Корзину».

В этом случае - самый простой способ восстановить удаленные или потерянные данные – это воспользоваться специальными программами. Они в основном работают по двум направлениям – устраняют физические и логические ошибки дисков либо восстанавливают данные, которые были случайно удалены или отформатированы. Программы различаются по функционалу, и бывает так, что в разных случаях следует использовать разный софт.

5.2 Лабораторное исследование №5. Исследование характеристик и возможностей программ по восстановлению потерянных данных

Цель:

изучить возможности специализированного программного обеспечения по восстановлению потерянных данных. Выяснить, какие из утилит наиболее эффективны.

Время работы: 4 часа

Задания на выполнение лабораторного исследования

1. По указанию преподавателя выбрать 3 программы из прилагаемого списка:

1. Hetman Partition Recovery
2. Active File Recovery
3. R-Studio 7.6
4. Auslogics File Recovery
5. Active UNDELETE
6. Paragon Rescue Kit
7. Wise Data Recovery
8. Puran File Recovery
9. O&O DiskRecovery
10. Tenorshare Any Data Recovery
11. Power Data Recovery
12. GetDataBack
13. Recover My Files
14. R-Undelete
15. Handy Recovery
16. Ashampoo Undeleter

Если студент желает провести анализ аналогичных по функционалу программ, не входящих в предложенный список, то это можно сделать по согласованию с преподавателем.

2. Установить на компьютер программное обеспечение по восстановлению потерянных данных в соответствии со своим вариантом (при возможности).

3. На сайте производителя данного ПО или из других источников в сети Интернет, узнать основные характеристики и возможности установленного ПО.

4. Произвести запуск основных модулей программы и исследовать, каким функционалом обладает данное ПО (при возможности).

5. Провести сравнительный анализ с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Сделать выводы по работе.

5.3 Содержание отчета

1. Цель работы

2. Назначение программного обеспечения по восстановлению потерянных данных.

3. Перечень исследуемых программ с указанием сайта производителя.

4. Скриншоты с кратким описанием основных функций и настроек для каждой из 3-х программ. Данный пункт может выполняться непосредственно при установке программ на компьютер или требуемые данные выбираются из технических описаний программ на сайтах производителей или других информационных ресурсов.

5. Результаты сравнительного анализа с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Выводы по проведенному исследованию.

5.4 Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Перечислить физические неисправности оптических дисков;

2. Перечислить физические неисправности флеш-памяти;

3. Перечислить физические неисправности накопителей на жестких дисках;

4. Почему нельзя использовать носитель в случае потери и дальнейшего восстановления информации;

5. В каких случаях нельзя восстановить информацию с носителя?

6. Какие два основных метода восстановления файлов которые не были перезаписаны используются в большинстве программ восстановления данных?

6 Резервное копирование данных на компьютере

6.1 Краткие теоретические сведения

Резервное копирование данных одна из важнейших операций которую нужно производить любому пользователю ПК. Резервное копирование данных можно делать как в ручную, так и с помощью специальных программ.

Резервное копирование данных – процесс создание копий важной информации, которые хранятся на других хранилищах данных (флешка, жесткий диск, DVD-диск, облачный сервис и т.д.). Резервное копирование данных очень важная операция, которую должен производить любой пользователь, через определенный промежуток времени.

Необходимость резервного копирования данных

Каждый пользователь хранит на компьютере различную информацию. Практически у каждого пользователя на компьютере хранится важная информация, потеря которой может, как минимум, расстроить пользователя (личные фото, коллекция музыки, рабочие документы и т.д.).

К сожалению, информация не может абсолютно надежно хранится на компьютере. Отказ аппаратной части (жесткий диск) или вирусная атака и даже неаккуратность самого пользователя (случайное удаление информации) могут привести к потере важных данных. Чтобы обезопасить важную информацию необходимо делать резервное копирование данных.

Резервное копирование файлов и информации позволит защитить данные, в случае если произойдет выход из строя основного носителя информации (например, жесткий диск компьютера) или вирусной атаки.

Виды резервного копирования

1. Резервная копия операционной системы.

Очень полезная функция, которой многие, даже опытные пользователи, пренебрегают. Вам нужно всего один раз установить операционную систему, драйвера и необходимые программы. Затем делается резервная копия настроенной операционной системы и если что то происходит (вирусная атака или просто захламление системы), то нужно потратить 10 -15 минут что бы восстановить резервную копию, вместо того что бы тратить не один час на новую установку и настройку системы.

Как правило, для резервного копирования операционной системы используют специальные программы или средства Windows.

2. Резервная копия диска (раздела на винчестере)

Допустим, в разделе жёсткого диска (например, диска “E”), хранится музыка и фотографии. Все эти данные важны и их потеря неприемлема.

Можно сделать резервную копию всего этого диска и если произойдет потеря данных и восстановить все как было.

Резервное копирование диска можно сделать как с помощью специальных программ, так и вручную.

3. Резервная копия отдельных файлов и папок

Самый часто встречающийся способ резервного копирования. В основном пользователи хранят на одном диске фотографии, на другом документы, на третьем любимую музыку. Кроме этого на этих дисках может храниться не очень важная информация, резервную копию которой делать не обязательно.

В таком случае делается только резервная копия этих самых файлов и папок, с разных дисков, а не копия целого диска, а тем более всего жесткого диска компьютера.

Обычно такое резервное копирования пользователь делает в ручную, хотя можно использовать специальные программы или средства Windows.

Как показывает практика, процесс резервного копирования лучше автоматизировать, чтобы исключить такой человеческий фактор, как забывчивость.

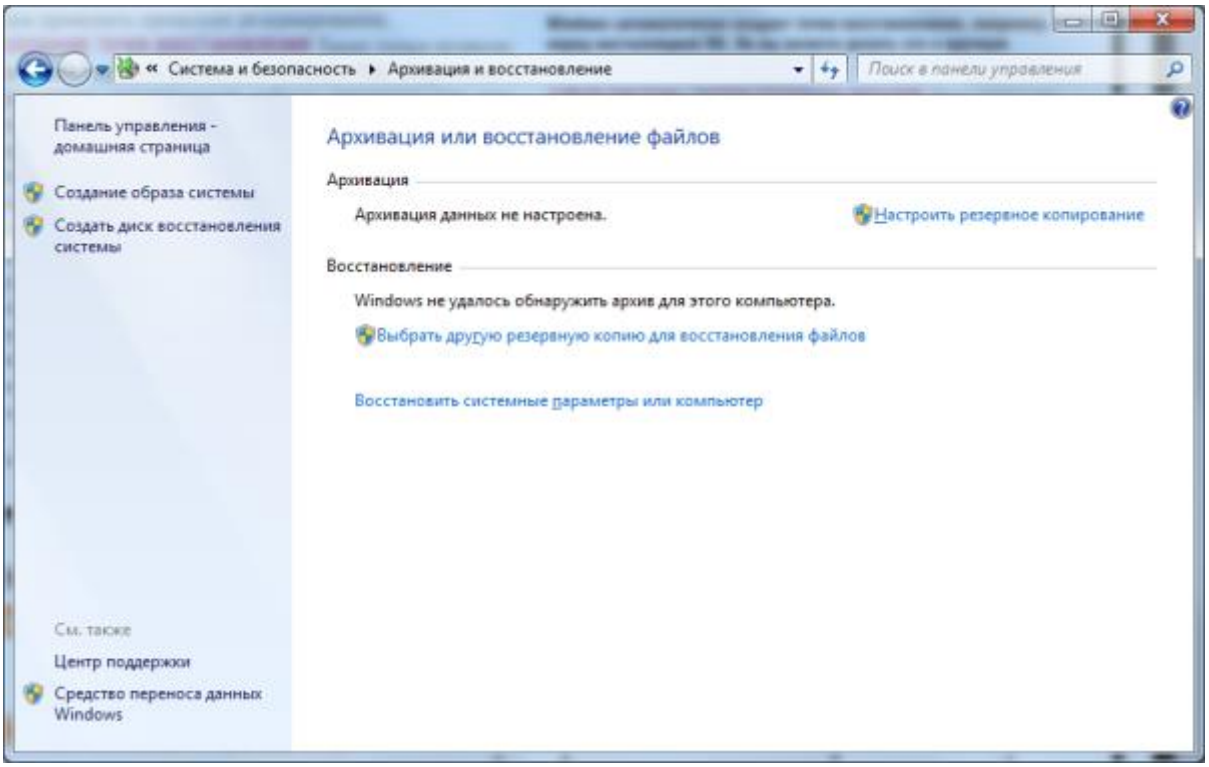

Рисунок 6.1

Резервное копирование средствами Windows

В операционной системе Windows 7 и выше есть средства для создания резервное копии, как самой системы, так и определенных данных.

Что бы перейти в средства резервного копирования Windows откройте панель управления далее “Система и безопасность” и “Архивация и восстановление”, как показано на рисунке 6.1.

Вам будет предложено настроить архивацию данных (указать место хранения копий и что архивировать). Кроме того можно создать образ операционной системы и настроить периодичность создания резервной копии, а так же создать диск для резервного восстановления системы.

После настройки резервного копирования рекомендуется создать диск восстановления системы.

Ручное и программное создание резервных копий

Существует ряд программ, которые помогут быстро и легко настроить резервное копирование всех необходимых данных.

Все программы справляются с задачей резервного копирования данных в той или иной степени.

Далеко не всем пользователям нужно делать резервное копирование операционной системы (хотя это удобно) или целого диска. Достаточно просто раз в неделю или в месяц (в зависимости от периодичности пополнения/изменения информации) вручную копировать важные данные на другие носители. Например, копировать личные фото после каждой поездки в отпуск или отдых, а квартальный отчет копировать раз в 3 месяца.

Рекомендации по резервному копированию данных

Периодичность

Делайте резервные копии периодично. В зависимости от типа данных можно делать резервные копии через промежуток времени (каждую неделю, месяц и т.д.) или по событию (появлению новых фотографий или изменение отчета.)

Если не следить за периодичностью, то в случае потери данных можно только восстановить старую версию резервной копии, в которой не будет хватать недавно измененных данных.

Множество копий

Сделав резервную копию важной информации, размножить эту копию на разных хранилища информации: флешка, внешний жёсткий диск, DVD-диск, облачное хранилище и т.д. Хранение информации в облачном хранилище очень удобно и актуально в наше время.

Защита резервной копии

Копии важных данных необходимо защитить от посторонних. Если делается резервная копия частных фотографий, то они ни в коем случае не должны быть открыты другими людьми.

Лучше всего совместить шифрование и парольную защиту данных. Можно создать зашифрованный контейнер для хранения любых типов данных или создать архив, закрытый паролем.

Хранение резервных копий

Не храните резервные копии даже на разных носителях в одном месте (ящике или шкафу) или в одной квартире (если случится пожар, то все копии будут уничтожены).

Отнесите одну копию на работу и положите в свой сейф или закрывающийся ящик и так же залейте резервную копию в облако. Можно даже дать носитель другу на хранение, но в любом случае не забывайте защитить копию от постороннего доступа.

6.2 Лабораторное исследование №6. Исследование характеристик и возможностей программ по организации резервного копирования

Цель:

изучить возможности специализированного программного обеспечения по организации резервного копирования. Выяснить, какие из утилит наиболее эффективны.

Время работы: 4 часа

Задания на выполнение лабораторного исследования

1. По указанию преподавателя выбрать 3 программы из прилагаемого списка:

1. Iperius Backup
2. FBackup
3. Backup4all
4. Uranium Backup Free
5. Simple Data Backup
6. Personal Backup
7. Back4Sure
8. SyncBackFree
9. Handy Backup
10. EASEUS Todo Backup 8.0 Free Edition
11. Exiland Backup Free 4.0

12. Nero BackItUp
13. Paragon Rescue Kit 14.0 Free
14. Action Backup
15. LimBackup
16. AVSbackup
17. ExtraBackup
18. Cobian Backup
19. Backup & Recovery 10 Build 9169 Free Edition
20. Information Backup System

Если студент желает провести анализ аналогичных по функционалу программ, не входящих в предложенный список, то это можно сделать по согласованию с преподавателем.

2. Установить на компьютер программное обеспечение по организации резервного копирования в соответствии со своим вариантом (при возможности).

3. На сайте производителя данного ПО или из других источников в сети Интернет, узнать основные характеристики и возможности установленного ПО.

4. Произвести запуск основных модулей программы и исследовать, каким функционалом обладает данное ПО (при возможности).

5. Провести сравнительный анализ с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Сделать выводы по работе.

6.3 Содержание отчета

1. Цель работы

2. Назначение программного обеспечения по организации резервного копирования.

3. Перечень исследуемых программ с указанием сайта производителя.

4. Скриншоты с кратким описанием основных функций и настроек для каждой из 3-х программ. Данный пункт может выполняться

непосредственно при установке программ на компьютер или требуемые данные выбираются из технических описаний программ на сайтах производителей или других информационных ресурсов.

5. Результаты сравнительного анализа с аналогичными по функционалу двумя другими выбранными программами из предложенного списка или выбранных студентом самостоятельно.

6. Выводы по проведенному исследованию.

6.4 Контрольные вопросы

При сдаче отчета по лабораторному исследованию студент должен быть готов ответить на следующие вопросы:

1. Перечислить и охарактеризовать виды резервного копирования.

2. Какие виды резервного копирования можно сделать средствами ОС Windows?

3. Какие виды резервного копирования можно сделать средствами ОС Linux?

4.Дать рекомендации по резервному копированию.

5. На какие носители можно делать резервное копирование?

6. Как произвести резервное копирование данных со смартфона?

7. Каковы достоинства и недостатки облачных хранилищ?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: М.: ИД ФОРУМ: ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - ISBN 978-5-8199-0331-5
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат)
3. Е. Б. Белов, В. Лось, Р. В. Мещеряков, Д. А. Шелупанов Основы информационной безопасности М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.
4. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам М.:Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8
5. Ярочкин В.И. Информационная безопасность М. : Академический Проект, 2008. — 544 с. — 978-5-8291-0987-5. — Режим доступа:
6. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации СПб. : Университет ИТМО, 2011. — 112 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/65808.html
7. Шевчук П.С. Методические указания по проведению практических занятий по дисциплине «Основы информационной безопасности сетей и систем»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 36 с.: ил. РнД: СКФ МТУСИ, 2016
8. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с.
9. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. — М.: Гелиос АРВ, 2005. —192 с.
10. Основы информационной безопасности: курс лекций: учебное пособие / Издание третье / Галатенко В. А. Под редакцией академика РАН В. Б. Бетелина / — М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. — 208 с.