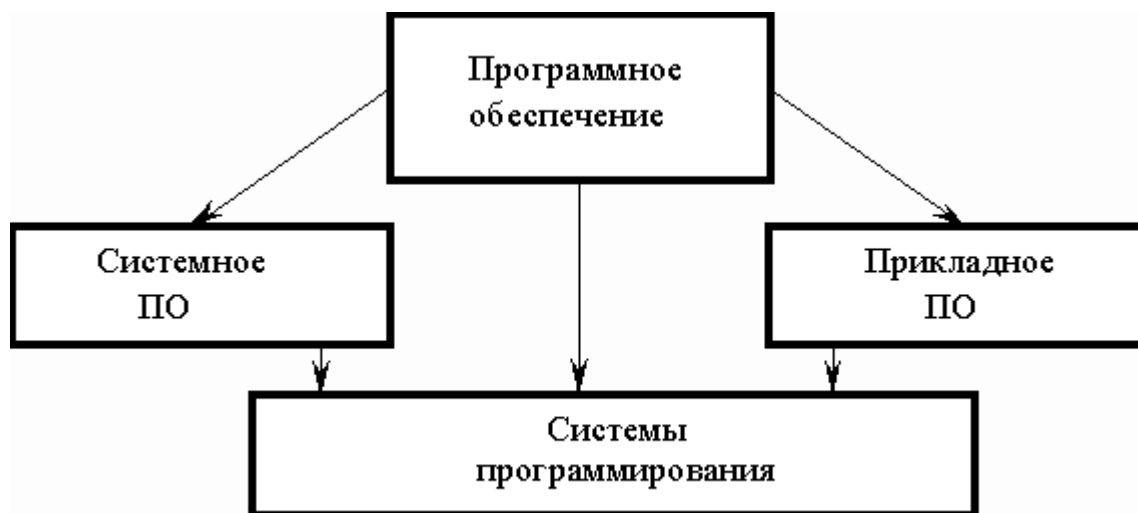


Раздел 2. Программное обеспечение вычислительной техники, базовые системные программные продукты

Программный принцип управления компьютером. Виды программ компьютера. Операционная система: назначение, состав, загрузка

Компьютеры отличаются от других устройств (телевизора, телефона) тем, что они выполняют любые действия по обработке информации с помощью специальной инструкции (программы). Программное обеспечение (ПО) - это совокупность всех программ и соответствующей документации, обеспечивающая использование компьютера в интересах каждого ее пользователя. ПО делится на классы:



- Системное ПО - системные программы, выполняющие различные вспомогательные функции, например: управление ресурсами компьютера; создание копий используемой информации; проверка работоспособности устройств компьютера; выдача справочной информации о компьютере и др.;
- Прикладное ПО; прикладные программы, непосредственно обеспечивающие выполнение необходимых пользователям работ
- Системы программирования; инструментальные программные системы, облегчающие процесс создания новых программ для компьютера.

1. Системное ПО

Системное программное обеспечение разрабатывается так, чтобы компьютер мог эффективно выполнять прикладные программы. Некоторую часть ПО встраивают в ПЗУ. Программы, записанные в микросхемы ПЗУ доступны компьютеру сразу после включения. В ходе запуска на экране появляются сообщения о работе программ проверки, появляется приглашение программы-оболочки или операционной системы или среды, дальнейшая работа происходит под управлением ОС. ОС выполняет роль посредника между аппаратной частью и пользователем и устанавливает комфортную среду. Первые компьютеры были без ОС, только программы в ПЗУ. Необходимость появилась, когда стали использоваться диски для

хранения информации и появилась файловая структура. Операционная система обычно хранится во внешней памяти компьютера, при включении компьютера она считывается с дисковой памяти и размещается в ОЗУ.

Системное ПО

Программы	Пояснение	Примеры
Операционные системы	Комплекс программ, распределяющих ресурсы компьютерной системы и организующих работу других программ	MS-DOS Windows UNIX
Программы-оболочки	Программы, обеспечивающие более комфортное общение пользователя с командами ОС	Norton Commander, Windows Commander, FAR
Программы диагностики	Проверяют работу основных устройств компьютера	Checkit, Sandra
Антивирусные программы	Программы обнаружения компьютерных вирусов и их уничтожения	DrWeb, Антивирус, Касперского, AIDSTEST
Программы обслуживания	Программы проверки целостности логической и физической структуры дисков» дефрагментация	дефрагментация
Архиваторы	Программы упаковки файлов и группы файлов для уменьшения занимаемого ими места на диске	Winrar, PKZIP, ARJ

В функции операционной системы входит:

- осуществление диалога с пользователем;
- ввод-вывод и управление данными;
- планирование и организация процесса обработки программ;
- распределение ресурсов (оперативной памяти и кэша, процессора, внешних устройств);
- запуск программ на выполнение;
- передача информации между различными внутренними устройствами;
- программная поддержка работы периферийных устройств (дисплея, клавиатуры, дисковых накопителей, принтера и др.).

Программы-утилиты (вспомогательное ПО)

Важными классами системных программ являются также программы вспомогательного назначения — утилиты (лат. utilitas — польза). Они либо расширяют и дополняют соответствующие возможности операционной системы, либо решают самостоятельные важные задачи. Кратко опишем некоторые разновидности утилит:

1. **Программы контроля, тестирования и диагностики**, которые используются для проверки правильности функционирования устройств компьютера и для обнаружения неисправностей в процессе эксплуатации; указывают причину и место неисправности;

2. **Программы-драйверы**, которые расширяют возможности операционной системы по управлению устройствами ввода-вывода, оперативной памятью и т.д.; с помощью драйверов возможно подключение к компьютеру новых устройств или нестандартное использование имеющихся;

3. **Программы-упаковщики (архиваторы)**, которые позволяют записывать информацию на дисках более плотно, а также объединять копии нескольких файлов в один архивный файл;

4. **Программы оптимизации и контроля качества дискового пространства**; информация на дисках размещена в кластерах-блоках, может быть разбросана в разных местах диска. Когда информация часто перезаписывается, пространство заполняется неравномерно, появляются пробелы. Дефрагментатор наводит порядок на диске, переносит кластеры так, чтобы они образовывали единые блоки. Эту программу надо использовать время от времени. Дефрагментация увеличивает объем памяти. Проверяет диски на правильность размещения информации. Она сравнивает реальные каталоги с таблицей размещения файлов FAT. Программа выявляет несоответствие, что возникает при аварийном отключении. Утилиту запускают систематически.

5. **Программы восстановления информации**, форматирования, защиты данных; удаление файла не означает полное уничтожение информации на диске. Первая буква имени файла заменяется другим символом (его код означает ненужность). Если сразу ничего не записывать, то можно найти и восстановить свой файл.

6. **Коммуникационные программы**, организующие обмен информацией между компьютерами, соединенных сетью или с помощью модема (телефонная сеть);

7. **Программы для управления памятью**, обеспечивающие более гибкое использование оперативной памяти;

2. Прикладное программное обеспечение

В данный класс входят программные продукты, выполняющие обработку информации различных предметных областей, для решения задач определенного класса конкретной предметной области.

Классификация прикладных программ:

1. Проблемно–ориентированные:

По типам предметных областей; информационным системам; функциям и комплексам задач, реализуемых программным способом: автоматизированного бухгалтерского учета; финансовой деятельности; управления персоналом (кадровый учет); управления материальными запасами; банковские информационные системы и др.

2. Методо–ориентированные:

Программные продукты, обеспечивающие независимо от предметной области и функций информационных систем математические, статистические и другие методы решения задач. Наиболее распространены методы математического программирования, решения дифференциальных уравнений, имитационного моделирования, исследования операций. Примеры: Мезозавр, Эвриста – статистическая обработка данных, Ms Project for Windows – сетевые методы и модели для решения управленческих задач.

3. ПП общего назначения:

Данный класс содержит широкий перечень программных продуктов:

Системы управления базами данных (СУБД), например: FoxPro, Access.

Серверы баз данных – предназначен для создания и использования при работе в сети интегрированных баз данных в архитектуре клиент–сервер. Многопользовательские СУБД в сетевом варианте обработки данных хранят информацию на файл–сервере – специально выделенном компьютере в централизованном виде, но сама обработка данных ведется на рабочих станциях. Примеры: Oracle, Ms QSL Server.

Текстовые процессоры – специальные программы, предназначенные для работы с документами (текстами), позволяющие компоновать, форматировать, редактировать тексты при создании пользователем документа. Признанными лидерами в части текстовых процессоров для ПЭВМ являются MS WORD, WordPerfect, AmiPro.

Табличный процессор (электронные таблицы) – пакеты программ, предназначенные для обработки табличным образом организованных данных (осуществляет разнообразные вычисления, строит графики, управляет форматом ввода–вывода данных, проводит ана-

литические исследования и т.п.). В настоящее время наиболее популярными и эффективными пакетами данного класса являются Excel, Improv, Quattro Pro, 1-2-3.

Средства презентационной графики – специализированные программы, предназначенные для создания изображений и их показ на экране, подготовки слайд-фильмов, мультфильмов, видеофильмов, их редактирования, определения порядка следования изображений. Примеры: PowerPoint, Multimedia Viewer.

Интегрированные пакеты – набор нескольких программных продуктов, функционально дополняющих друг друга. Компоненты интегрированных пакетов могут работать изолированно друг от друга. Примеры: Ms Office, Borland Office.

ПП автоматизированного проектирования. Программы этого класса предназначены для поддержания работы конструкторов и технологов, связанных с разработкой чертежей, схем, диаграмм, мультфильмов. Примеры: AutoCad, Visio.

Программы-переводчики, средства проверки орфографии и распознавания текста: FineReader, Lingvo, Promt.

Коммуникационные ПП – предназначены для организации взаимодействия пользователя с удаленными абонентами или информационными ресурсами сети: браузеры, средства для создания WWW-страниц, электронная почта.

Программные средства мультимедиа. Этот класс является относительно новым, он сформировался в связи с изменением среды обработки данных. Основное назначение таких ПП – создание и использование аудио- и видеоинформации для расширения информационного пространства пользователя. Программные продукты мультимедиа заняли лидирующие положение на рынке в сфере библиотечного информационного обслуживания, процессе обучения, организации досуга. Примеры: Multimedia.

Настольные издательские системы. Данный класс программ включает программы, предназначенные для профессиональной издательской деятельности и позволяющие осуществлять: форматирование и редактирование текстов; автоматическую разбивку текста на страницы; создание заголовков; компьютерную верстку печатной страницы; монтирование графики; использование всевозможных шрифтов; подготовку иллюстраций и т.д. Например: Adobe Page Maker, CorelDraw.

3. Системы программирования.

Назначение систем программирования – разработка программ для решения различных задач. **Система программирования** – это программное обеспечение компьютера, предназначенное для разработки, отладки и исполнения программ, записанных на определенном языке программирования.

Системы программирования используются для создания программ, если имеющиеся не удовлетворяют потребности. Самая простая – Basic, входит в состав операционной системы MS DOS как приложение, средство программирования на языке высокого уровня.

Системы программирования, в зависимости от языка программирования, бывают высокого уровня и низкого. Системы высокого уровня: Pascal, Basic, Turbo. Наиболее приближенный язык к машинному – Ассемблер, программирование в машинных кодах – самое низкоуровневое программирование. Чем более язык приближен к человеческому, тем выше уровень языка. У каждого языка свои достоинства и недостатки, чем легче его изучать, тем проще программы можно создавать. В состав систем программирования входят:

- **Компилятор** (транслятор)– программа-переводчик для преобразования программы с языка высшего уровня в программу в машинных кодах.
- **Интерпретатор** (транслятор) – выполняет программу прямо на языке высокого уровня. После того, как программа откомпилирована, ни сама исходная программа, ни компилятор более не нужны. В то же время программа, обрабатываемая интерпретатором, должна заново переводиться на машинный язык при каждом очередном запуске программы.
- **Библиотеки подпрограмм.**
- **Отладчики** – программы для отладки.

- **Линковщик** – для установки связей, перекрестных ссылок.

В современных программных системах (Turbo Basic, Turbo Pascal, Turbo C и др.) отладка осуществляется часто с использованием специальных программных средств, называемых отладчиками. Эти средства позволяют исследовать внутреннее поведение программы.

Программа-отладчик обычно обеспечивает следующие возможности:

- пошаговое исполнение программы с остановкой после каждой команды (оператора);
- просмотр текущего значения любой переменной или нахождение значения любого выражения, в том числе, с использованием стандартных функций; при необходимости можно установить новое значение переменной;
- установку в программе "контрольных точек", т.е. точек, в которых программа временно прекращает свое выполнение, так что можно оценить промежуточные результаты, и др.

При отладке программ важно помнить следующее: в начале процесса отладки надо использовать простые тестовые данные; возникающие затруднения следует четко разделять и устранять строго поочередно; не нужно считать причиной ошибок машину, так как современные машины и трансляторы обладают чрезвычайно высокой надежностью.

К системам предъявляются следующие требования:

- наглядный интерфейс;
- оснащённость справочниками,
- помощью;
- надёжность;
- способность решать широкий круг задач.

Операционная система: назначение и состав

Операционная система — комплекс управляющих и обрабатывающих программ, которые, предназначены для управления устройствами, вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и обеспечения надёжности вычислений. Это определение применимо к большинству современных операционных систем общего назначения.

Предшественником операционных систем следует считать служебные программы (загрузчики и мониторы), а также библиотеки часто используемых подпрограмм, начавшие разрабатываться с появлением универсальных компьютеров 1-го поколения (конец 1940-х годов). В 1950—1960-х годах сформировались и были реализованы основные идеи, определяющие функциональность ОС: пакетный режим, разделение времени и многозадачность, разделение полномочий, реальный масштаб времени, файловые структуры и файловые системы.



ОС обеспечивает несколько видов интерфейсов:

1. Пользовательский – между пользователем и компьютером;

2. Аппаратно-программный - между ПО и аппаратным обеспечением;

3. Программный – между разными видами ПО.

ОС обычно хранится во внешней памяти компьютера – на диске. При включении компьютера она считывается с дисковой памяти и размещается в ОЗУ. Этот процесс называют загрузкой ОС.

Основные функции ОС:

1. Загрузка программ в оперативную память и их выполнение.
2. Выполнение запросов программ (ввод и вывод данных, запуск и остановка других программ, выделение и освобождение дополнительной памяти и др.).
3. Стандартизованный доступ к периферийным устройствам (устройства ввода-вывода).
4. Управление оперативной памятью (распределение между процессами, организация виртуальной памяти).
5. Управление доступом к данным на энергонезависимых носителях (таких как жёсткий диск, оптические диски и др.), организованным в файловой системе.
6. Обеспечение пользовательского интерфейса.
7. Сохранение информации об ошибках системы.

Компоненты операционной системы

1. Загрузчик.
2. Ядро, содержащее планировщик; драйверы устройств, файловую систему. Традиционные ядра UNIX, Linux; ядро MS-DOS.
3. Командный процессор (интерпретатор). Расшифровывает и исполняет команды пользователя, поступающие через клавиатуру.
4. Интерфейс.

Для того чтобы успешно решать свои задачи, современный пользователь может обойтись без досконального знания аппаратного устройства компьютера. Ему не обязательно быть в курсе того, как функционируют различные электронные блоки и электромеханические узлы компьютера.

Так, например, при работе с диском программисту, конечному пользователю ОС достаточно представлять его в виде некоторого набора файлов, каждый из которых имеет имя. Последовательность действий при работе с файлом заключается в его открытии, выполнении одной или нескольких операций чтения или записи, а затем в закрытии файла. Такие частности, как используемая при записи частотная модуляция или текущее состояние двигателя механизма перемещения магнитных головок чтения/записи, не должны волновать пользователя. Именно операционная система скрывает от пользователя или программиста большую часть особенностей аппаратуры и предоставляет возможность простой и удобной работы с требуемыми файлами.

Если бы программист работал непосредственно с аппаратурой компьютера, без участия ОС, то для организации чтения блока данных с диска программисту пришлось бы использовать более десятка команд с указанием множества параметров: номера блока на диске, номера сектора на дорожке и т. п. А после завершения операции обмена с диском он должен был бы предусмотреть в своей программе анализ результата выполненной операции. Учитывая, что контроллер диска способен распознавать более двадцати различных вариантов завершения операции, можно считать программирование обмена с диском на уровне аппаратуры не самой тривиальной задачей. Не менее обременительной выглядит и работа пользователя, если бы ему для чтения файла с терминала потребовалось задавать числовые адреса дорожек и секторов.

Операционная система берет на себя все рутинные операции, связанные с управлением другими аппаратными устройствами компьютера: физической памятью, таймерами, принтерами и т.д.

В результате реальная машина, способная выполнять только небольшой набор элементарных действий, определяемых ее системой команд, превращается в виртуальную машину, выполняющую широкий набор гораздо более мощных функций. Виртуальная машина тоже управляется командами, но это уже команды другого, более высокого уровня: удалить файл с определенным именем, запустить на выполнение некоторую прикладную программу, повысить приоритет задачи, вывести текст из файла на печать. Таким образом, назначение ОС состоит в предоставлении пользователю/программисту некоторой расширенной виртуальной машины, которую легче программировать и с которой легче работать, чем непосредственно с аппаратурой, составляющей реальный компьютер или реальную сеть.

ОС как система управления ресурсами

Операционная система является механизмом, распределяющим ресурсы компьютера. К числу основных ресурсов современных вычислительных систем могут быть отнесены такие ресурсы, как процессоры, основная память, таймеры, наборы данных, диски, накопители на магнитных лентах, принтеры, сетевые устройства и некоторые другие. Ресурсы распределяются между процессами. Процесс (задача) представляет собой базовое понятие большинства современных ОС и часто кратко определяется как программа в стадии выполнения. Программа — это статический объект, представляющий собой файл с кодами и данными. Процесс — это динамический объект, который возникает в операционной системе после того, как пользователь или сама операционная система решает «запустить программу на выполнение», то есть создать новую единицу вычислительной работы. Например, ОС может создать процесс в ответ на команду пользователя `run prgl.exe`, где `prgl.exe` — это имя файла, в котором хранится код программы.

Например, мультипрограммная операционная система организует одновременное выполнение сразу нескольких процессов на одном компьютере, поочередно переключая процессор с одного процесса на другой, исключая простои процессора, вызываемые обращениями процессов к вводу-выводу. ОС также отслеживает и разрешает конфликты, возникающие при обращении нескольких процессов к одному и тому же устройству ввода-вывода или к одним и тем же данным. Критерий эффективности, в соответствии с которым ОС организует управление ресурсами компьютера, может быть различным. Например, в одних системах важен такой критерий, как пропускная способность вычислительной системы, в других — время ее реакции. Соответственно выбранному критерию эффективности операционные системы по-разному организуют вычислительный процесс. Управление ресурсами включает решение следующих общих, не зависящих от типа ресурса задач:

- планирование ресурса — то есть определение, какому процессу, когда и в каком количестве (если ресурс может выделяться частями) следует выделить данный ресурс;
- удовлетворение запросов на ресурсы;
- отслеживание состояния и учет использования ресурса — то есть поддержание оперативной информации о том, занят или свободен ресурс и какая доля ресурса уже распределена;
- разрешение конфликтов между процессами.

Для решения этих общих задач управления ресурсами разные ОС используют различные алгоритмы, особенности которых, в конечном счете и определяют облик ОС в целом,

включая характеристики производительности, область применения и даже пользовательский интерфейс. Например, применяемый алгоритм управления процессором в значительной степени определяет, может ли ОС использоваться как система разделения времени, система пакетной обработки или система реального времени.

Чтобы процесс мог быть выполнен, операционная система должна назначить ему область оперативной памяти, в которой будут размещены коды и данные процесса, а также предоставить ему необходимое количество процессорного времени. Кроме того, процессу может понадобиться доступ к таким ресурсам, как файлы и устройства ввода-вывода.

Важной задачей операционной системы является защита ресурсов, выделенных данному процессу, от остальных процессов. Одним из наиболее тщательно защищаемых ресурсов процесса являются области оперативной памяти, в которой хранятся коды и данные процесса. Совокупность всех областей оперативной памяти, выделенных операционной системой процессу, называется его адресным пространством. Говорят, что каждый процесс работает в своем адресном пространстве, имея в виду защиту адресных пространств, осуществляемую ОС. Защищаются и другие типы ресурсов, такие как файлы, внешние устройства и т. д. Операционная система может не только защищать ресурсы, выделенные одному процессу, но и организовывать их совместное использование, например разрешать доступ к некоторой области памяти нескольким процессам.

Управление памятью

Управление памятью включает распределение имеющейся физической памяти между всеми существующими в системе в данный момент процессами, загрузку кодов и данных процессов в отведенные им области памяти, настройку адресно-зависимых частей кодов процесса на физические адреса выделенной области, а также защиту областей памяти каждого процесса.

Функциями ОС по управлению памятью являются отслеживание свободной и занятой памяти; выделение памяти процессам и освобождение памяти при завершении процессов; защита памяти; вытеснение процессов из оперативной памяти на диск, когда размеры основной памяти недостаточны для размещения в ней всех процессов, и возвращение их в оперативную память, когда в ней освобождается место, а также настройка адресов программы на конкретную область физической памяти.

Управление файлами и внешними устройствами

Для удобства работы с данными файлы группируются в каталоги, которые, в свою очередь, образуют группы — каталоги более высокого уровня. Пользователь может с помощью ОС выполнять над файлами и каталогами такие действия, как поиск по имени, удаление, вывод содержимого на внешнее устройство (например, на монитор), изменение и сохранение содержимого. Чтобы представить большое количество наборов данных, разбросанных случайным образом по цилиндрам и поверхностям дисков различных типов, в виде хорошо всем знакомой и удобной иерархической структуры файлов и каталогов, операционная система должна решить множество задач. Файловая система ОС выполняет преобразование символьных имен файлов, с которыми работает пользователь или прикладной программист, в физические адреса данных на диске, организует совместный доступ к файлам, защищает их от несанкционированного доступа.

При выполнении своих функций файловая система тесно взаимодействует с подсистемой управления внешними устройствами, которая по запросам файловой системы осуществляет передачу данных между дисками и оперативной памятью. Подсистема управления

внешними устройствами, называемая также подсистемой ввода-вывода, исполняет роль интерфейса ко всем устройствам, подключенным к компьютеру. Спектр этих устройств очень обширен. Номенклатура выпускаемых накопителей на жестких, гибких и оптических дисках, принтеров, сканеров, мониторов, плоттеров, модемов, сетевых адаптеров и более специальных устройств ввода-вывода, таких как, например, аналого-цифровые преобразователи, может насчитывать сотни моделей. Эти модели могут существенно отличаться набором и последовательностью команд, с помощью которых осуществляется обмен информацией с процессором и памятью компьютера, скоростью работы, кодировкой передаваемых данных, возможностью совместного использования и множеством других деталей.

Программа, управляющая конкретной моделью внешнего устройства и учитывающая все его особенности, обычно называется драйвером этого устройства (от английского *drive* — управлять, вести). Драйвер может управлять единственной моделью устройства или группой устройств определенного типа. Для пользователя очень важно, чтобы операционная система включала как можно больше разнообразных драйверов, так как это гарантирует возможность подключения к компьютеру большого числа внешних устройств различных производителей. От наличия подходящих драйверов во многом зависит успех операционной системы на рынке.

Созданием драйверов устройств занимаются как разработчики конкретной ОС, так и специалисты компаний, выпускающих внешние устройства. Операционная система должна поддерживать хорошо определенный интерфейс между драйверами и остальной частью ОС, чтобы разработчики из компаний-производителей устройств ввода-вывода могли поставлять вместе со своими устройствами драйверы для данной операционной системы.

Защита данных и администрирование

Безопасность данных вычислительной системы обеспечивается средствами отказоустойчивости ОС, направленными на защиту от сбоев и отказов аппаратуры и ошибок программного обеспечения, а также средствами защиты от несанкционированного доступа. В последнем случае ОС защищает данные от ошибочного или злонамеренного поведения пользователей системы.

Первым рубежом обороны при защите данных от несанкционированного доступа является процедура логического входа. Операционная система должна убедиться, что в систему пытается войти пользователь, вход которого разрешен администратором. Функции защиты ОС вообще очень тесно связаны с функциями администрирования, так как именно администратор определяет права пользователей при их обращении к разным ресурсам системы — файлам, каталогам, принтерам, сканерам и т. п. Кроме того, администратор ограничивает возможности пользователей в выполнении тех или иных системных действий. Например, пользователю может быть запрещено выполнять процедуру завершения работы ОС, устанавливать системное время, завершать чужие процессы, создавать учетные записи пользователей, изменять права доступа к некоторым каталогам и файлам. Администратор может также урезать возможности пользовательского интерфейса, убрав, например, некоторые пункты из меню операционной системы, выводимого на дисплей пользователя.

Важным средством защиты данных являются функции аудита ОС, заключающиеся в фиксации всех событий, от которых зависит безопасность системы. Например, попытки удачного и неудачного логического входа в систему, операции доступа к некоторым каталогам и файлам, использование принтеров и т. п. Список событий, которые необходимо отслеживать, определяет администратор ОС.

Поддержка отказоустойчивости реализуется операционной системой, как правило, на основе резервирования. Чаще всего в функции ОС входит поддержание нескольких копий данных на разных дисках или разных дисковых накопителях. Резервируются также принтеры и другие устройства ввода-вывода. При отказе одного из избыточных устройств операционная система должна быстро и прозрачным для пользователя образом произвести реконфигурацию системы и продолжить работу с резервным устройством. Особым случаем обеспечения отказоустойчивости является использование нескольких процессоров, то есть мультипроцессирование, когда система продолжает работу при отказе одного из процессоров, хотя и с меньшей производительностью. В состав ОС обычно входят утилиты, позволяющие администратору выполнять регулярные операции резервного копирования для обеспечения быстрого восстановления важных данных.

Вывод:

ОС должна удовлетворять следующим требованиям:

- ОС должна быть развиваемой (д. уметь работать с различными приложениями);
- ОС должна стать посредником между различными видами какой-либо аппаратуры;
- ОС должна быть настраиваемой на разную периферию;
- ОС должна быть дружелюбной – понятной и удобной (язык, для людей с дефектами);
- ОС должна быть надежной, не допуская потери данных;
- Применительно к сетям ОС должна обеспечивать безопасность информации, защиту от повреждения и похищения.

Контрольные вопросы

1. Что такое программа?
2. Приведите классификацию ПО.
3. Какие программы относят к системным?
4. Что такое утилиты?
5. Назначение ОС.
6. Функции ОС.
7. Требования к ОС.
8. Какие программы относят к прикладным?

Раздел 2. Программное обеспечение вычислительной техники, базовые системные программные продукты.

Операционная система Windows: основные функции, базовые элементы графической оболочки, работа с окнами, файловая система.

Windows XP — операционная система семейства Windows NT корпорации Microsoft, выпущенная в 2001 году. Она совместила возможности и простоту версий Win9x и надежности Windows NT.

Достоинства ОС семейства Windows:

- Единый унифицированный пользовательский интерфейс Windows-программ;
- Многозадачность – возможность выполнения нескольких программ;
- Возможность обмена данными между Windows-программами;
- Поддержка масштабируемых шрифтов;
- Простота подключения новых устройств.

В современных компьютерах при включении питания сразу начинается загрузка операционной системы Windows. На экране появится главное окно программы – Рабочий стол.

Элементы интерфейса:

Пользовательский интерфейс – средства взаимодействия человека с компьютером. Его основные элементы: рабочий стол, окна, меню, диалоговые окна; вспомогательные элементы: панели инструментов, пиктограммы, полосы прокрутки и др.

Рабочий стол – вся поверхность экрана во время работы операционной системы.

Окно – структурный и управляющий элемент интерфейса, прямоугольная область экрана, где изображается документ, программа.

Меню – список команд, из которых надо сделать выбор.

Файл – однородная совокупность информации на диске, имеющая имя.

Каталог (папка) – группа файлов, объединенных по определенному признаку, имеющая имя. Понятие папки в Windows отличается от понятия каталога. Существуют специальные папки, содержимое которых не имеет реального расположения на диске, а зависит от настроек операционной системы. К таким папкам можно отнести:

- **«Мой компьютер»** — содержит доступные пользователю устройства хранения данных, а также ссылки на папки «Мои документы» разных пользователей, на папку «Панель управления», а также на некоторые устройства ввода информации (сканеры, камеры и т. д.)
- **«Панель управления»** — содержит список ссылок на программы, с помощью которых осуществляется настройка операционной системы.
- **«Корзина»** — системная папка для предотвращения случайного удаления файлов. Файлы, перемещённые в «Корзину» удаляются после выполнения команды «Очистить корзину».
- **«Рабочий стол»** — содержит как список файлов, находящихся в каталоге «Рабочий стол» текущего пользователя, так и другие папки: «Мой компьютер», «Мои документы», «Корзина» и «Сетевое окружение».

Значок – графический объект, соответствующий папке, документу, программе. Это пиктограмма – графическое представление объекта в свернутом виде. На рабочем столе появляются значки: Мой компьютер, Корзина и др.

Ярлык – указатель объекта, специальный файл, где содержится ссылка на объект. Отличается от значка стрелкой в левом углу.

Панель задач – элемент управления, располагается в нижней части экрана, содержит кнопку **Пуск**. При нажатии кнопки Пуск открывается **Главное меню**. Содержание панели задач: справа – часы, регулятор громкости и др.; слева – панель быстрого запуска программ. Настраивается панель с помощью контекстного меню правой кнопкой.



Различают следующие виды меню:

- **Системное меню** – для управления размером, формой представления окна, для его закрытия. Кнопка системного меню находится в левой части заголовка окна. Справа – кнопки, дублирующие команды системного меню (свернуть, развернуть, восстановить);
- **Главное меню** – открывает доступ ко всем программам, вызывается щелчком по кнопке Пуск. Настраивается с помощью Пуск→Настройка→Панель задач→Настройка меню. После раскрытия меню раскрываются вложенные меню, например Программы→Стандартные→.... Данный способ удобен, когда отсутствует ярлык на столе. Пункт меню Документы обычно содержит 15 последних файлов. Пункт Поиск предназначен для поиска папки или файла. Справка предназначена для работы со справочной системой операционной системы.
- **Горизонтальное меню (окна программы)** – находится под строкой заголовка, важнейший элемент управления. При выборе пункта горизонтального меню выводится ниспадающее меню. Пункты меню текстового редактора: **Файл, Правка, Вид, Вставка, Формат, Сервис, Таблица, Окно...**
- **Контекстное меню (меню объекта)** – в нем отражаются операции, которые можно выполнить с данным объектом, от этого зависит набор команд.
- **Пиктографическое меню** – панель инструментов, располагается под строкой горизонтального меню. Настраивается с помощью: **Вид→Панели инструментов**.



Разновидности окон в ОС семейства Windows

1. **Стартовый экран «Рабочий стол»** - системный объект, на котором отображаются другие объекты и элементы управления.

2. **Окно папки** – графический объект, отображающий содержимое открытой папки.

3. **Окно приложения** – отображает интерфейс программы и рабочий документ.

4. **Диалоговое окно** – элемент интерфейса, появляющийся при вводе команды. С помощью окна диалога вводятся данные, необходимые для работы. Окно имеет название, совпадающее с командой. Диалоговые окна могут содержать элементы:

- **Вкладки** – характерны для многофункциональных диалоговых окон. Например: диалоговое окно, в текстовом редакторе, Шрифт содержит вкладки: Шрифт, Интервал, Анимация.
- **Счетчик** – для изменения значения параметра с помощью стрелок.
- **Кнопки выбора (радиокнопки)** – для выбора одного из вариантов, переключатели и др.

Навигация в системе Windows.

Выделяют 4 способа навигации в системе Windows:

1. **С помощью Главного меню (самый грамотный).** Начинается работа с кнопки Пуск. Рассмотрен выше.
2. **С помощью пиктограмм на Рабочем столе (самый простой).** Двойным щелчком открывается приложение. Способ не удобен, если Рабочий стол закрыт окнами.
3. **С помощью программы Проводник (самый мощный).**
4. **С помощью программы Мой компьютер.** Удобен для работы с дисками.

Windows XP обладает большей функциональностью по сравнению с предшествующими версиями:

1. Надежная платформа — стабильная работа компьютера поддерживается даже в самых сложных условиях. Это достигается за счет:

- Использования файловой системы NTFS, которая позволяет назначать права доступа к различным файлам.
- Для сохранности самой системы существует кэш защищенных системных файлов. Это папка, в которой хранятся оригинальные копии важных файлов операционной системы. Если какой-либо из компонентов windows повреждается, то происходит его автоматическое восстановление из кэша. Размер этой папки составляет около 400 Мб.
- Функция восстановления системы. Эта функция поможет вернуть операционную систему в то состояние, каким оно было до появления неполадок. Объем, занимаемый информацией по предыдущим состояниям windows, может достигать 20% от вместимости каждого из логических дисков.

2. Мастер установки сети — помогает легко подключать и совместно использовать компьютеры и устройства, применяемые в домашних условиях.

3. Центр справки и поддержки — упрощает решение текущих проблем и помогает своевременно получать необходимую техническую поддержку.

4. Встроенный архиватор, типа Zip для файлов и папок. Имеется средство для запуска инструмента архивации данных: «Пуск» - «Все программы» - «Стандартные» - «Служебные» - «Архивация данных».

5. Изменения во внешнем виде и приемах работы: более привлекательное цветовое решение, при нажатии на кнопку Пуск появляется "двухстворчатое" Главное меню. Слева располагаются наиболее часто используемые программы, а справа список команд.

Сбой ОС windows

При некорректной работе windows используется Безопасный режим. Он создан специально для отладки работы системы. В нем убраны многие дополнительные функции и на него почти не влияет основной режим работы системы. В Безопасном режиме Windows использует настройки по умолчанию (минимальный набор драйверов устройств, необходимых для запуска Windows: драйверы мыши, монитора, клавиатуры, дисков, видеоадаптера; стандартные системные службы; поддержка сети отсутствует).

Для того чтобы попасть в безопасный режим windows выполняем следующие шаги. При запуске компьютера периодически нажимаем клавишу F8 до появления – (Меню дополнительных вариантов загрузки windows). Если вход в безопасный режим происходит удачно, то с помощью него, можно применить такие методы как, восстановление системы либо ко-

манду CHKDSK. И после запуститься в нормальном режиме. Если необходимо проверить системный диск (C:\), открываем меню **Пуск > Все программы > Стандартные > Командная строка**. В появившемся окне вводим **chkdsk /r** и нажимаем клавишу **Enter**. После завершения проверки компьютер сам перезагрузится, после загрузки Windows ошибки на разделе должны быть исправлены. Пример: если требуется проверить диск в дисковом D и исправить все обнаруженные ошибки в Windows, введите следующую команду: `chkdsk d: /f`.

Контрольные вопросы

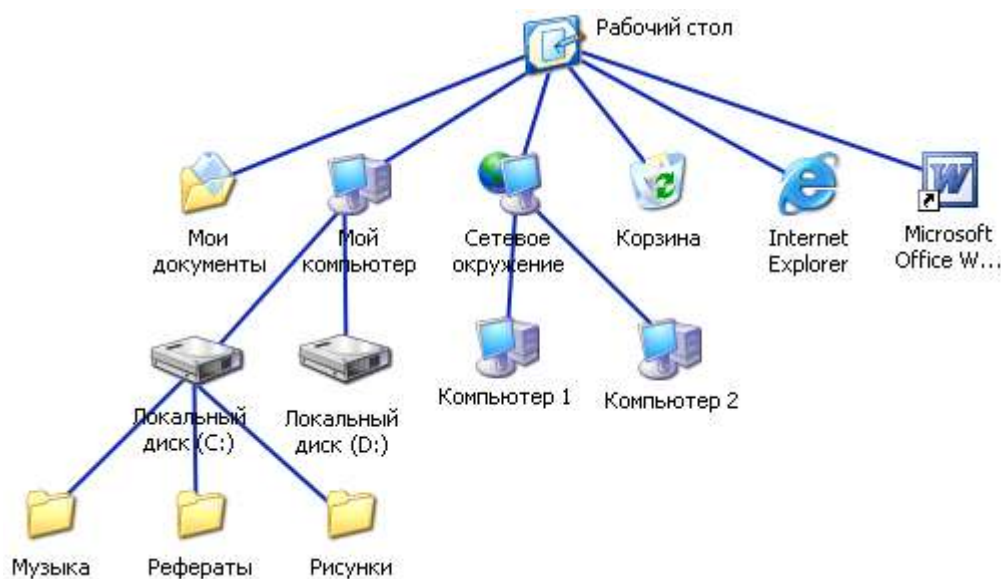
1. Характерные особенности ОС Windows.
2. Интерфейс ОС Windows.
3. Навигация в ОС Windows.

Раздел 2. Программное обеспечение вычислительной техники, базовые системные программные продукты

Файловые менеджеры. Программы-архиваторы. Пакеты утилит для Windows: назначение, возможности, порядок работы

Файловые системы

Файл – однотипный набор данных на машинном носителе, имеющий имя. Файлы объединены в каталоги. Каталог – группа файлов на диске, имеющая имя. Это место на диске, где хранятся имена и сведения о файлах. Всегда есть главный, корневой каталог и каталоги 1-го и 2-го уровней, получается вложенная структура каталогов.



В операционной системе Windows вместо каталогов используется понятие «папка». Папка – это объект Windows, предназначенное для объединения файлов и других папок в группы. Понятие папки шире, чем понятие «каталог». В Windows на вершине иерархии папок находится папка Рабочий стол. (Следующий уровень представлен папками Мой компьютер, Корзина и Сетевое окружение (если компьютер подключен к локальной сети)).

Файловой системой называется совокупность файлов и каталогов, организованных в древовидную структуру. Файловая система – это способ организации данных на носителях информации. Основные функции любой файловой системы: именование файлов; программный интерфейс работы с файлами для приложений; отображения логической модели файловой системы на физическую организацию хранилища данных; организация устойчивости файловой системы к сбоям питания, ошибкам аппаратных и программных средств. В многопользовательских системах появляется ещё одна задача: защита файлов одного пользователя от несанкционированного доступа другого пользователя. К современным файловым системам предъявляют дополнительные требования: возможность шифрования файлов, разграничение доступа для файлов, дополнительные атрибуты. Физическое размещение файлов на диске может быть различным:

1. Непрерывное размещение — простейший вариант физической организации, при котором файлу предоставляется последовательность кластеров диска, образующих непрерывный участок дисковой памяти. Достоинства: быстрый доступ, минимален объем адресной информации. Недостатки: при увеличении файла надо предусмотреть место.

2. Размещение в нескольких несмежных областях диска. Файл может изменять свой размер, наращивая число кластеров. Недостатком является сложность реализации доступа к произвольно заданному месту файла.

Обычно файловая система записана в начале жесткого диска. С точки зрения ОС, жесткий диск – это набор кластеров. Кластер – это область диска определенного размера для хранения данных. Минимальный размер кластера – 512 байт. Поскольку используется двоичная система счисления, то размеры кластеров кратны степени двойки. Для жестких дисков в ПК в данный момент наиболее распространены две файловые системы: FAT или NTFS. Сначала появилась FAT12, 16, затем FAT32, а потом NTFS. FAT в переводе Таблица Размещения Файлов. В таблице размещения файлов хранится информация о кластерах логического диска. Каждому кластеру в FAT соответствует отдельная запись, которая показывает, свободен ли он, занят ли данными файла, или помечен как сбойный (испорченный). Если кластер занят под файл, то в соответствующей записи в таблице размещения файлов указывается адрес кластера, содержащего следующую часть файла. Из-за этого FAT называют файловой системой со связанными списками.

Структура FAT была разработана Биллом Гейтсом и Марком Мак Дональдом в 1977 году. Использовалась в качестве основной файловой системы в операционных системах DOS и Microsoft Windows (до версии Windows ME). Сейчас существуют три типа файловой системы FAT:

FAT12 – поддерживает очень небольшие объемы дисков, поэтому сейчас она применяется только на дискетах.

FAT16 – используется на винчестерах и поддерживает диски объемом до 2 Гб, поэтому сейчас данная файловая система практически не используется.

FAT32 – теоретически поддерживаются диски объемом до 2 Тб, начиная с операционной системы Windows 95. Она использует 32-разрядную адресацию кластеров. На современных жестких дисках с объемом более 32 Гб размер кластера равен 32 Кб. Преимуществом этой файловой системы является ее простота и совместимость со старыми операционными системами. FAT изначально проектировалась для однопользовательской операционной системы, то она не предусматривает хранения такой информации, как сведения о владельце или полномочия доступа к файлу/каталогу.

Для оптимального использования дискового пространства применяют файловую систему NTFS. Все файловые системы построены на принципе: один кластер – один файл. Т.е.

один кластер хранит данные только одного файла. Основное отличие для обычного пользователя между этими системами – размер кластера. Рассмотрим на примере одного тома на диске объемом 120 Гб и файла размером 10 Кб. Для FAT32 размер кластера – 32Кб, а для NTFS – 4Кб. В FAT32 такой файл займет 1 кластер, при этом останется $32-10=22$ Кб незанятого места. В NTFS такой файл займет 3 кластера, при этом останется $12-10=2$ Кб незанятого места. По аналогии с блокнотом кластер – это клетка. И поставив точку в клетку, мы уже логически занимаем ее всю, а в действительности остается много свободного места. Неиспользованная часть кластера называется потерянным местом (slack). В небольших файлах почти весь кластер может быть потерянным местом, а в среднем потери составляют половину размера кластера. Таким образом, переход от FAT32 к NTFS позволяет более оптимально использовать жесткий диск при наличии большого количества мелких файлов в системе.

Файловая система NTFS является самой популярной и применяется практически на всех современных компьютерах, где используется программное обеспечение Microsoft, во всех операционных системах, созданных на базе Windows NT. Сегодня NTFS это одна из самых надежных и сложных файловых систем. Она способна автоматически восстанавливать нормальное функционирование после сбоя. Если в работе диска обнаруживается повреждение, это место маркируется как битое и данные с него перезаписываются в другое место.

В случае непредвиденного отключения питания система запоминает своё состояние и при включении компьютера перезагружается в своём последнем состоянии. В том, в котором она находилась на момент сбоя. Кроме этого, система NTFS имеет технологию сжатия дисков. Запутанность файловой структуры системы, делает её одной из самых безопасных файловых систем, поскольку в ней предусмотрена система прав доступа, защита от взлома, средства для шифрования дисков.

На данном этапе компания Microsoft внедряет в Windows 8 новую файловую систему — ReFS (отказоустойчивая файловая система), демонстрирующую необыкновенную надежность в работе. Пока ReFS будет использоваться как диспетчер данных для сервера. Основной недостаток файловой системы - неэффективная упаковка данных на диске.

В таблице приведены сравнительные характеристики файловых систем FAT16, FAT32, NTFS, ReFS. Различие между файловыми системами заключается в способах распределения пространства между файлами на диске и организации на диске служебных областей.

	FAT16	FAT32	NTFS	ReFS
Операционные системы	Большинство	Windows 95/98/ME, 2000/XP, Linux	Windows NT/2000/XP, Linux	Windows 8
Максимальный раздел диска	4 Гб	2 Тбайт	16 Эбайт	402 Эбайт
Максимальный размер файла	2 Гб	4 Гб	16 Тбайт	18,3 Эбайт
Максимальная длина имени	255	255	32767	32767

Восстановление	нет	нет	да	да
Максимальное число файлов в корневом каталоге	Задается при форматировании	Нет ограничений	4,3 млрд	18 трлн
Максимальное число кластеров	$\sim 2^{16}$	$\sim 2^{28}$	$\sim 2^{48}$	-
Размер кластера	512 байт- 64 Кб	512 байт- 64 Кб	512 байт- 64 Кб	64 кб

Файловые менеджеры

Файловый менеджер — компьютерная программа, предоставляющая интерфейс пользователя для работы с файловой системой и файлами. Файловый менеджер позволяет выполнять наиболее частые операции над файлами — создание, открытие/проигрывание/просмотр, редактирование, перемещение, переименование, копирование, удаление, изменение атрибутов и свойств, поиск файлов и назначение прав. Помимо основных функций, многие файловые менеджеры включают ряд дополнительных возможностей, например, таких как работа с сетью (через FTP, NFS и т. п.), резервное копирование, управление принтерами и пр. Выделяют различные типы файловых менеджеров, например:

Навигационные и двухпанельные — в общем случае имеют две равноценные панели для списка файлов, дерева каталогов и т. п. Двухпанельные файловые менеджеры DOS: Norton Commander, DOS Navigator, Volkov Commander; Microsoft Windows: FAR Manager, Total Commander. Навигационные файловые менеджеры Microsoft Windows: Проводник Windows (англ. Windows Explorer) — встроен в Windows.

Файловые менеджеры начинают свою историю со специальных программ - оболочек, разработанных для операционной среды DOS. В свое время эти программы были настоящим прорывом в IT-индустрии. Они позволили значительно расширить возможности ПК и способствовали массовой интеграции компьютеров во все отрасли делопроизводства. Первым, ставшим самым известным файловым менеджером, стал Norton Commander. Двухпанельный интерфейс и синий цвет для многих стал синонимом «работающего компьютера». На смену Norton Commander у пришел не менее известный Dos Navigator, который можно уверенно назвать первым профессиональным файловым менеджером. Новая программа позволила одновременно открывать несколько файловых панелей и текстовых файлов, имела удобные клавиатурные сокращения и мощный текстовый редактор. В файловом менеджере появилось несколько полезных утилит, в том числе калькулятор, телефонная книжка, CD-проигрыватель. Dos Navigator был написан под DOS, и переносить его на платформу Win32 разработчики не стали. Немало файловых менеджеров, появившихся после Dos Navigator, претендовало на звание лучшего файлового менеджера. Но они имели недостатки: работали в текстовом режиме, другие были ненадежны в работе, интерфейс третьих был недостаточно гибким и удобным.

Файловый менеджер Total Commander — двухпанельный файловый менеджер для Windows. Он позволяет экономить время на рутинных операциях (сохраняем, копируем, удаляем или перемещаем файлы или папки). Возможности:

1. Позволяет переносить и копировать файлы и папки.
2. Позволяет сравнивать содержимое различных папок между собой, сравнивать содержимое отдельных файлов.

3. Обладает мощным инструментом поиска файлов. Можно искать файлы по маске в любых указанных папках и подкаталогах. Обнаруживает отдельные файлы, соответствующие условиям поиска, внутри архивов всех поддерживаемых форматов. Можно искать файлы: содержащие, указанный пользователем текст, созданные и изменявшиеся в указанный пользователем интервал времени, определенного размера и обладающие определенными атрибутами (архивный, скрытый, только для чтения, системный).

4. Облегчает работу с архивированными файлами. В него встроены распаковщики нескольких архивных форматов: ZIP, ARJ, LZH, RAR, TAR, GZ, CAB и ACE. Для извлечения файлов из архивов перечисленных форматов никакого дополнительного программного обеспечения не требуется.

5. Total Commander показывает объем файлов или их группы, а также место, которое эти файлы фактически занимают на диске.

6. Total Commander позволяет разбивать большие файлы на фрагменты, чтобы хранить их или переносить на другой компьютер с помощью различных носителей: дискет, ZIP-дисков и CD-R.

7. Total Commander позволяет увидеть скрытые папки при заражении флэш-накопителя вирусом. Для этого в нем надо включить показ скрытых и системных файлов, открыть флэш-накопитель, удалить незнакомые файлы и папки. Подлежат удалению файлы: autorun.~ex, autorun.bat, autorun.bin, autorun.exe, autorun.ico, autorun.inf, autorun.inf_?????, autorun.ini, autorun.reg, autorun.srm, autorun.txt, autorun.vbs, autorun.wsh; прочие файлы с расширениями .inf .com .sys .tmp .exe; папка RECYCLER. Опасность представляет вирус, который может в этой корзине находиться.

8. Позволяет, выделив нужный файл на панели и нажав Ctrl+Q, увидеть на соседней панели его содержимое: видео, программный, текстовый документ или другой файл распространенного формата. Если при перемещении стрелок на клавиатуре выделять файлы, то в соседнем окне просмотра будет отображаться содержимое этих файлов.

Контрольные вопросы

1. Функции файловой системы.
2. Структура имени файла.
3. Разновидности форматов файлов.
4. Что такое каталог?
5. Что такое путь к файлу?
6. Что такое дерево папок?
7. Что такое файловый менеджер?

Раздел 2. Программное обеспечение вычислительной техники, базовые системные программные продукты

Защита информации от несанкционированного доступа

Потеря информации может нанести существенный ущерб владельцу, а также стороне, интересы которой данная информация затрагивает. Цель информационной безопасности - минимизировать потери при модификации или разрушении информации.

Основные типы угроз информации:

- перехват (становится возможным копирование, чтение, разглашение или использование сведений закрытого характера);
- хищение;
- модификация (угрозы данного типа осуществляются путем несанкционированного доступа, возможно уничтожение информации или фальсификация);
- разрушение (угрозы данного типа имеют, как правило, одноразовый характер проявления);
- непреднамеренные воздействия отказы и сбои устройств или программ;
- угрозы, проявляемые в результате неаккуратности или непрофессионализма сотрудников при обработке, хранении или передаче информации;
- стихийные бедствия.

Источники возникновения угроз потери информации: люди, носители документы и др. Информация может передаваться:

- путем хищения носителей (магнитных дисков, лент, документов и пр.);
- негласного просмотра информации, отображенной на экране монитора компьютера;
- подключения к устройствам передачи, обработки и хранения информации специально разработанных аппаратных средств;
- внедрения резидентных программ;
- регистрации и анализа побочных электромагнитных излучений средств электронно-вычислительной техники, связи и телекоммуникаций;
- установки подслушивающих и передающих устройств.

Защита информации средствами операционной системы.

Существует несколько методов защиты информации средствами операционной системы. Простейшими являются использование паролей. Слабейшим звеном всякой системы защиты является человек. Ниже приведены правила выбора паролей и обращения с ними, несоблюдение которых может свести на нет всю сложную систему защиты:

1. Пароль не должен быть значимым словом или сочетанием слов какого-либо языка.
2. Не должен быть очень коротким.
3. Не содержать сведения личного характера (адрес, имя, дату рождения)
4. Не записывайте свой пароль в файле или на бумажке (запомнить).
5. Не используйте один пароль для нескольких целей.
6. Периодически менять.
7. Менять, при увольнении сотрудника.
8. Для важной информации одноразовый пароль.

Исследования показали, что:

№ п/п	Темы	Частота выбора %	Раскрываемость %
1.	№ документов (паспорта, пропуска, полиса, зачетки)	3,5	100
2.	Последовательность клавиш на клавиатуре	14,1	72,3

3.	№ телефона	3,5	66,6
4.	Адрес или его часть	4,7	55
5.	Ф.И.О.	22,2	54,2
6.	Знак зодиака	11,8	54,5
7.	Хобби	9,5	29,5
8.	Прочее	30,7	5,7

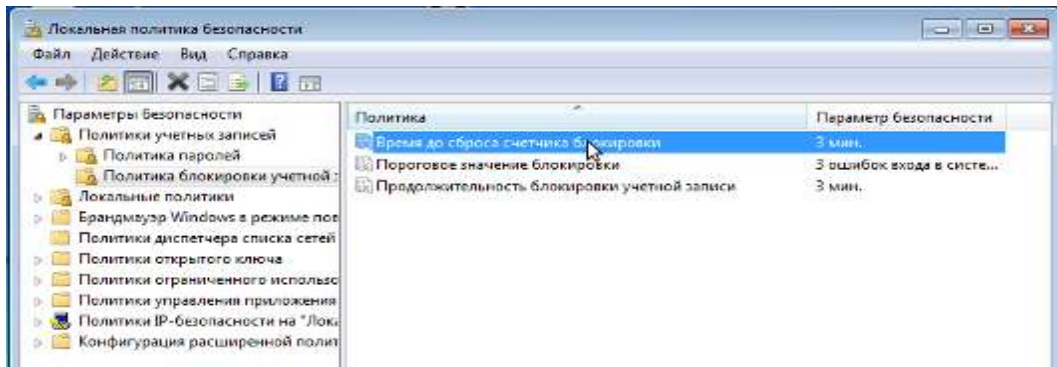
1. Защита паролем экранной заставки. Для этого необходимо из контекстного меню **Рабочего стола** открыть **Свойства экрана**, выбрать заставку, отметить опцию **Пароль**, ввести пароль.

2. Защита паролем учетной записи. По умолчанию учетные записи пользователей в Windows XP не имеют паролей, имеют уровень доступа к компьютеру на уровне администратора, т.е. пользователь учетной записи может устанавливать драйвера, программы, полностью управлять компьютером и данными. Операционная система Windows имеет в своем арсенале простейшие средства защиты от различных воздействий.

Для этого надо зайти в меню «Пуск», выбрать пункт «Панель управления» (Start | Control Panel). Выбрать компонент «Учетные записи пользователей» (User Accounts). Щелкните на пиктограмме учетной записи, для которой требуется задать или сменить пароль. В открывшемся окне выбрать команду «Создание пароля» или «Изменение пароля». В открывшемся диалоговом окне ввести пароль для выбранной учетной записи. Для коллег можно создать «Ограниченную учетную запись», чтобы они не могли просматривать конфиденциальную информацию или изменять настройки компьютера, но могли пользоваться Интернетом, создавать документы.

Для этого заходим в «Панель управления», выбираем ссылку «Учетные записи пользователей», выбираем «Создание учетной записи». В появившемся окне вводим имя новой учетной записи, выбираем тип «Ограниченная запись».

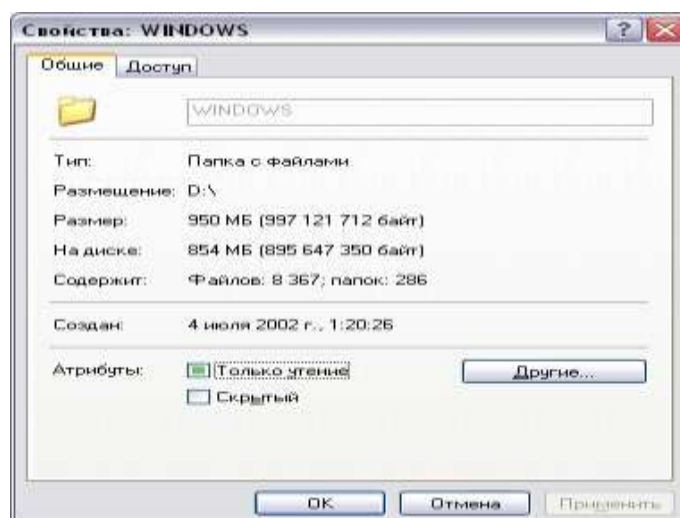
По умолчанию для любого пользователя Windows7 включено неограниченное количество попыток ввода пароля при входе в систему. Такая настройка дает возможность злоумышленникам подобрать пароль (если он не сложный) путем перебора всех наиболее вероятных вариантов. Создание политики блокировки учетной записи (аккаунта) защитит учетную запись от взлома путем ограничения попыток ввода пароля на определенное время. Аккаунт будет автоматически блокироваться на заданное вами после заданного количества неверно введенных паролей. По истечению заданного интервала учетная запись автоматически разблокируется и система снова позволит выполнить ввод пароля. В окне локальных политик безопасности перейти: Политики учетных записей → Политика блокировки учетной записи.



Правой кнопкой мыши по записи “Пороговое значение блокировки” выбрать из меню пункт “Свойства”. Ввести выбранное значение попыток неправильного ввода пароля и нажать ОК. “Время до сброса счетчика блокировки” и “Продолжительность блокировки учетной записи” по умолчанию - по 30 минут.

2. Использование программы «Защитник Windows». Данная утилита входит в стандартный набор компонентов системы Windows. Программа автоматически проверяет и удаляет наиболее опасное ПО.

3. Шифрование папок и файлов. Если файлы или папки расположены на диске с файловой системой NTFS, допускается устанавливать дополнительные атрибуты. Нажмите кнопку Другие (Advanced), и на экране появится диалог настройки дополнительных параметров. С помощью флажков в этом диалоге можно задать или снять некоторые атрибуты файлов и папок. Флажки в группе **Атрибуты** индексирования и архивации (Archive and Index attributes) служат для использования некоторыми вспомогательными программами. Флажок *Сжимать содержимое для экономии места на диске* (Compress contents to save disk space) позволяет сжимать данные при записи на диск.



Флажок *Шифровать содержимое для защиты данных* (Encrypt contents to secure data) позволяет зашифровать файлы, так что никто не сможет прочитать конфиденциальную информацию. Причем, данный вид защиты очень надежен. При шифровании какой-либо папки или файла, их названия отображаются зеленым цветом.

Установив нужные флажки, нажмите кнопку **ОК**, чтобы закрыть диалог и вернуться к предыдущему диалогу. В этом диалоге также нажмите кнопку **ОК**. Если вы изменили атрибуты папки, появится диалог, спрашивающий, хотите ли вы изменить атрибуты только данной папки или нужно изменить атрибуты всех вложенных файлов и папок. Установив переключатель в нужное положение, нажмите кнопку **ОК**, и атрибуты файлов изменятся. Если вы выбрали сжатие или шифрование папки, в этот момент начнется процедура данного преобразования файлов. Это может занять достаточно много времени. В Windows XP можно настроить, чтобы сжатые файлы и папки отображались в списке синим цветом, а зашифрованные - зеленым.

После того, как файл или папка зашифрованы или сжаты, с ними работают так же, как и с другими файлами или папками. Шифрование и сжатие являются прозрачными для пользователя, выполнившего эти операции. Перед использованием не требуется расшифровывать или разархивировать файл. Открытие, редактирование и сохранение файла выполняется как обычно. При этом посторонний человек, пытающийся получить доступ к зашифрованным файлам, не сможет этого сделать. Только пользователь, зашифровавший файл, может открыть его. Естественно, если злоумышленник вошел в Windows XP под вашим именем, система не сможет оградить от него файлы.

Следует помнить, что можно зашифровать только файлы и папки, находящиеся на дисках с файловой системой NTFS. Если вы перенесете файл на другой диск, он может быть расшифрован. Одновременное использование сжатия и шифрования не допускается. Шифрование папки или файла не защищает их от удаления. Любой пользователь, имеющий права на удаление, может удалить зашифрованные папки или файлы.

4. Шифрование при архивировании папок и файлов. При архивировании появится меню, в котором следует выбрать пункт «Добавить в архив». Откроется меню архивирования. Перейти на вкладку «Дополнительно» и нажать на кнопку «Установить пароль». Появится окно, в котором надо дважды ввести выбранную для пароля комбинацию цифр и букв. Можно отметить галочкой пункт «Шифровать имена файлов». Так уровень защиты информации станет максимальным.

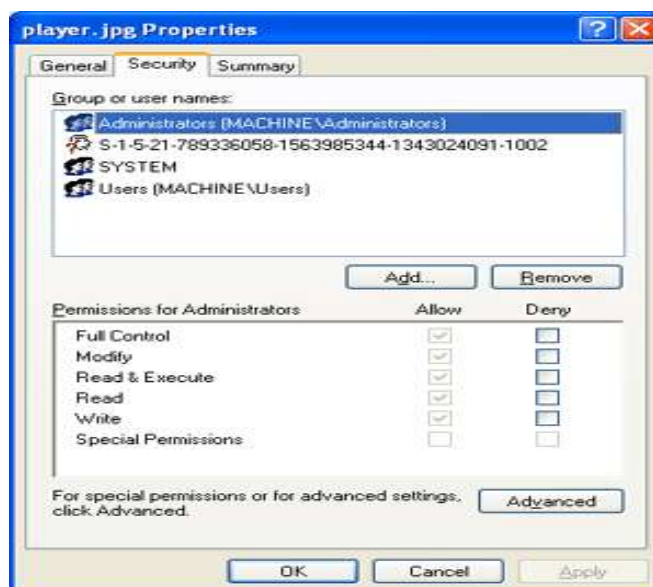
5. **NTFS** - единственная файловая система в Windows, которая позволяет назначать права доступа к различным файлам. Устанавливая другим пользователям определенные разрешения для файлов и каталогов, пользователь может защищать конфиденциальную информацию от несанкционированного доступа. Для назначения пользователю или группе разрешения на доступ к определенному файлу необходимо:

1. Указать файл мышью и нажать правую кнопку. Выбрать пункт **Properties** (Свойства) контекстного меню. В появившемся окне свойств файла перейти на вкладку **Security** (Безопасность). По умолчанию данной вкладки может не быть, чтобы она появилась необходимо в

свойствах папки убрать галочку Simple File Sharing (использовать простой общий доступ к файлам).

2. В группе Name (Имя) показан список пользователей и групп, которым уже предоставлены разрешения для этого файла. Для того, чтобы добавить или удалить пользователей или новые группы, нажать кнопку Add/Remove (Добавить/Удалить) Появится окно диалога Select Users, Groups (Выбрать пользователей, группы). В поле Enter the object names to select (Введите имена выбираемых объектов) написать имя пользователя, кнопка Check Names (Проверить имена) позволяет проверить правильность написания имени.

3. В группе Permissions (Разрешения) устанавливаются разрешения. Присутствуют указатели Deny (запретить) и Allow (Разрешить). Устанавливаются флажки для следующих параметров: Full Control (полный контроль) - пользователь получает неограниченный доступ к файлу, Modify (Изменение) - пользователь может изменять файл, Read & execute (Чтение и выполнение), Read (Чтение) - пользователь может только читать файл, Write (Запись) - пользователь может записывать в файл.



Для более тонкой настройки разрешений необходимо нажать кнопку Advanced. Появляется диалоговое окно Advanced Security Settings for (Дополнительные параметры безопасности). Здесь можно дополнительно указать дополнительные разрешения, настроить политику аудита, изменить (просмотреть) информацию о владельце файла и добавить / удалить пользователей, могущих получить доступ к файлу.

Следующее, очень полезное свойство файловой системы NTFS - это возможность введения квот. Это свойство используется в больших компаниях, где работают большое количество пользователей, у которых нет привычки следить за актуальностью информации, и которые хранят ненужные файлы, тем самым занимая дисковое пространство. Так как администратор не может проследить за всем этим, он может ввести квоту на использование диска определенному пользователю. После установки квот пользователь может хранить на томе

ограниченный объем данных, в то время как на этом диске может оставаться свободное пространство. Если пользователь превысит выданную ему квоту, в журнал событий будет внесена соответствующая запись. Чтобы включить квоты на диске нужно прежде всего, чтобы он был в формате NTFS, затем в свойствах папки Tools-Folder Options-View убрать флажок Simple File Sharing. Это нужно для того, чтобы в свойствах диска появилась вкладка Quota. В ней необходимо установить флажок на Enable quota management (Активизировать управление квотами). Это будет установлена мягкое квотирование, которое выдаст предупреждение, что пользователь, если так случится, превысил квоту, но право на запись у него будет. Чтобы в случае превышения квоты пользователю было отказано в доступе к этому тому необходимо установить флажок на Deny disk space to users exceeding quota limit (Запретить запись на диск пользователям, превысившим размер дискового пространства). На этой же вкладке можно установить размер выделяемой квоты (Limit disk space to) и порог, превышение которого вызывает запись предупреждения в журнале событий (Set Warning level to) - Установить порог выдачи сообщения. Эти параметры устанавливаются по умолчанию для всех пользователей. В окне же Quota Entries можно изменить параметры квоты, задаваемой для конкретного пользователя. Для этого следует выделить конфигурируемую учетную запись с помощью контекстного меню выбрать свойства и сконфигурировать квоту.

Резервное копирование

Несмотря на все повышающуюся надежность современных операционных систем и «железных» компонентов компьютеров, всегда существует вероятность их отказа, выхода из строя или, например, кражи. Кроме того, угрозу сохранности представляют случайное стирание/форматирование, результаты атак вирусов и червей, количество которых в сети продолжает постоянно возрастать. При возникновении таких ситуаций пользователь, как правило, в полной мере осознает всю важность операций резервного архивирования. Действительно, если программное обеспечение в случае отказа можно переустановить, то утрата данных может иметь катастрофические последствия. Безусловно, масштабы катастрофы могут иметь различные размеры, и утеря фотографий красивого отпуска несоизмерима с «падением» БД предприятия. При выполнении «Пуск» - «Все программы» - «Стандартные» - «Служебные» - «Архивация данных», запустится мастер. Помимо обычного архивирования, можно указать еще 4 способа:

- Копирующая архивация. У файлов, добавляемых в архив, атрибут «Архивный» не снимается. Применяем, если вам необходимо сохранить состояние отдельных файлов.
- Ежедневная архивация. Будут сохранены все файлы, которые изменялись в течение дня до выполнения ежедневной архивации. Атрибут «Архивный» не снимается.
- Добавочная архивация. В архив будут добавлены только те файлы, которые были созданы или изменены со времени последнего обычного или добавочного архивирова-

ния. Атрибут «архивный» снимается (система понимает это как уже архивированный файл). Если кроме обычного архивирования использовалось добавочное, для восстановления файла понадобятся архивы последнего обычного архива и всех добавочных.

- Разностная архивация. В архив будут добавлены все файлы, созданные или измененные после обычной или добавочной архивации. Файлы не будут отмечены как архивированные (атрибут «Архивный» остается). Для восстановления необходим последний обычный архив и последний разностный.

Помимо типа архивации, можно задать и ее способы. Например, произвести проверку данных после копирования.

Контрольные вопросы

1. Для чего необходима защита информации?
2. Перечислите типы угроз информации?
3. Меры защиты информации.
4. Методы шифрования информации.

Раздел 2. Программное обеспечение вычислительной техники, базовые системные программные продукты

Защита информации от компьютерных вирусов

Антивирусные программы

Модификация и разрушение информации может произойти под воздействием компьютерного вируса. Общее определение компьютерного вируса можно дать как самораспространяющийся в информационной среде компьютеров программный код. Он может внедряться в исполняемые и командные файлы программ, распространяться через загрузочные секторы дискет и жестких дисков, документы офисных приложений, через электронную почту, Web-сайты, а также и по другим электронным каналам. Компьютерный вирус — это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере. Размеры вирусных программ 156 байт, 256 байт. Своим названием компьютерные вирусы обязаны определенному сходству с биологическими вирусами по:

- способности к саморазмножению (особенность алгоритма);
- высокой скорости распространения;
- избирательности поражаемых систем (каждый вирус поражает только определенные системы);
- способности «заражать» еще незараженные системы;
- быстрота появления модификаций и новых поколений;
- трудности борьбы с вирусами.

История возникновения компьютерных вирусов

Период	Событие
1949 г.	Джон фон Нейман читал серию лекций «Теория и организация сложных автоматов», которая и легла в основу теории самовоспроизводящихся автоматов.
1961 г.	сотрудники компании Bell разработали игру Darwin. Программы, называемые «организмами», загружались в память компьютера и сражались за ресурсы. Они захватывали жизненное пространство, пытаясь уничтожить противника. За этим процессом наблюдала программа-«судья», определявшая правила. Программист, разработка которого захватывала всю память компьютера, побеждал.
начало 1970-х г.	Самоперемещающаяся программа Creeper с целью продемонстрировать возможность самопроизвольного перемещения программ между компьютерами. Creeper не приносил вреда: предыдущая копия уничтожалась, а программа перемещалась на следующий компьютер.
1973 г.	Был впервые использован термин «компьютерный вирус» в значении, привычном для современного человека, — «вредоносная программа, внедрившаяся в компьютерную систему».
В 1980-х годах	Вирусы появились на пользовательских компьютерах.
1988 г.	Червь Морриса стал первым сетевым червем, успешно распространившимся в сети.
1991 г.	Появился полиморфный вирус, видоизменявший свое тело.

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, «засоряет» оперативную память и т. д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий.

Файловые вирусы заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы.

Загрузочные вирусы заражают загрузочные сектора дисков (boot-сектор).

Макро-вирусы - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов. Макровирусы являются программами, написанными на макросах – последовательностях команд, используемых в некоторых системах обработки данных, например текстовых редакторах и электронных таблицах. Наибольшее распространение получили макровирусы для Microsoft Word и Excel. Такой вирус активизируется при открытии зараженного документа и переносится на компьютер, как правило, внедряясь в шаблон Обычный (файл Normal.dot). После этого каждый сохраняемый документ заражается вирусом, а когда другие пользователи открывают его, их компьютеры также инфицируются. Существуют также макровирусы, заражающие базы данных Microsoft Access.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Среди них выделяют почтовые черви, распространяющиеся посредством электронной почты. Черви способны очень быстро поражать файлы, диски и оперативную память.

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;

Предлагается условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

Основными путями проникновения вирусов в компьютер являются съемные диски, компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода и перезагрузили компьютер, при этом дискета может быть и несистемной. На дискету вирус может попасть, даже если ее просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Способы заражения программ:

- метод приписывания. Код вируса приписывается к концу файла заражаемой программы, и тем или иным способом осуществляется переход вычислительного процесса на команды этого фрагмента;
- метод оттеснения. Код вируса располагается в начале зараженной программы, а тело самой программы приписывается к концу.
- метод вытеснения. Из начала (или середины) файла «изымается» фрагмент, равный по объему кода вируса, и приписывается к концу файла. Сам вирус записывается в освободившееся место.

Сетевые вирусы. К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере. Пример сетевых вирусов – так называемые черви.

«Хулиганские» вирусы в последние годы становятся все менее актуальными, их доля около 5%. 95% современных вирусов связано с интернет-преступностью. С появлением интернет-сервисов возник интерес к получению доступа в сеть за чужой счет, т.е. посредством кражи чьего-либо логина и пароля с применением специально разработанных троянских программ. Троянские программы не относятся к самовоспроизводящимся программам, могут маскироваться под обычные программы. Троян может прокрасться под видом ускорителя Интернета, программы работы с диском, видеокодека, исполняемого файла, имеющего двойное расширение.

В начале 1997 года зафиксированы первые случаи создания и распространения троянских программ, ворующих пароли доступа, регистрационные данные и ключевые файлы раз-

личных программных продуктов, использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т.п. Часто используются троянские программы, которые воруют коды доступа к банковским счетам, рекламируют какие-либо товары или услуги, незаконно используют ресурсы зараженного компьютера для обслуживания спам-бизнеса, звонят на платные телефонные номера, следят за действиями и привычками хозяина компьютера и читают электронную почту.

Принципы работы антивирусных программ

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры.

До 1990-х годов антивирусные программы работали на основе сравнения кода вируса с другими программами. **Программы-детекторы** осуществляли поиск характерного для конкретного вируса кода в оперативной памяти и в файлах и при обнаружении выдавали соответствующее сообщение. Этот алгоритм был эффективен, когда коды вирусов были статичны.

Позже появились полиморфные вирусы, которые изменяли свое тело по непредсказуемым заранее алгоритмам. Для обнаружения таких вирусов используется эвристический анализ. При этом анализируется работа программы, если есть отступление от ее алгоритма, делается вывод о наличии вируса.

Программы-доктора - «лечат», т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. Так как постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.

Фильтры – небольшие программы для обнаружения подозрительных действий компьютера.

Блокираторы - анализируют поведение других программ и при обнаружении подозрительных действий блокируют их (для работы в сети).

Наиболее распространенные антивирусные программы:

1. **Антивирус Касперского** (Разработчик: «Лаборатория Касперского»). Содержит следующие компоненты: поведенческий блокиратор; ревизор отслеживает все изменения в компьютере и при обнаружении несанкционированных изменений в файлах или в системном реестре позволяет восстановить содержимое диска и удалить вредоносные коды; эвристический анализатор дает возможность защитить компьютер даже от неизвестных вирусов; фоновый перехватчик вирусов, постоянно присутствующий в памяти компьютера, проводит антивирусную проверку всех файлов непосредственно в момент их запуска, создания или копирования, что позволяет контролировать все файловые операции и предотвращать заражение даже самыми технологически совершенными вирусами; модуль фильтрации электронной почты не только удаляет вирусы из тела письма, но и полностью восстанавливает содержимое электронных писем. Программа позволяет проверять архивные файлы, изолировать подозрительные программы.

2. **NOD32**, антивирусный пакет, выпускаемый словацкой фирмой ESET . Содержит компоненты пакета: автоматического сканирования всех USB-носителей, карт памяти, CD/DVD-дисков; сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером; модуль защиты от нежелательной почты фильтрует нежелательную почту; резидентный сканер, препятствующий попаданию зараженных файлов на диски компьютера.

Важной характеристикой антивирусной программы является отсутствие ложных срабатываний. Ложные срабатывания могут нанести не меньший вред пользователю, чем вирусное заражение: заблокировать работу нужных программ, перекрыть доступ к сайтам.

Контрольные вопросы

1. Для чего необходима защита информации?
2. Что такое компьютерный вирус?
3. Меры защиты информации.
4. Перечислите признаки заражения компьютера.
5. Классификация антивирусных программ.
6. Принцип работы антивирусных программ.