Информационные технологии в области техносферной безопасности

Проф. Растоскуев Виктор Васильевич

Введение в информационные технологии в области техносферной безопасности

Введение в информационные технологии

Пакеты прикладных программ для анализа данных

Сеть Интернет

Системы поддержки принятия решений

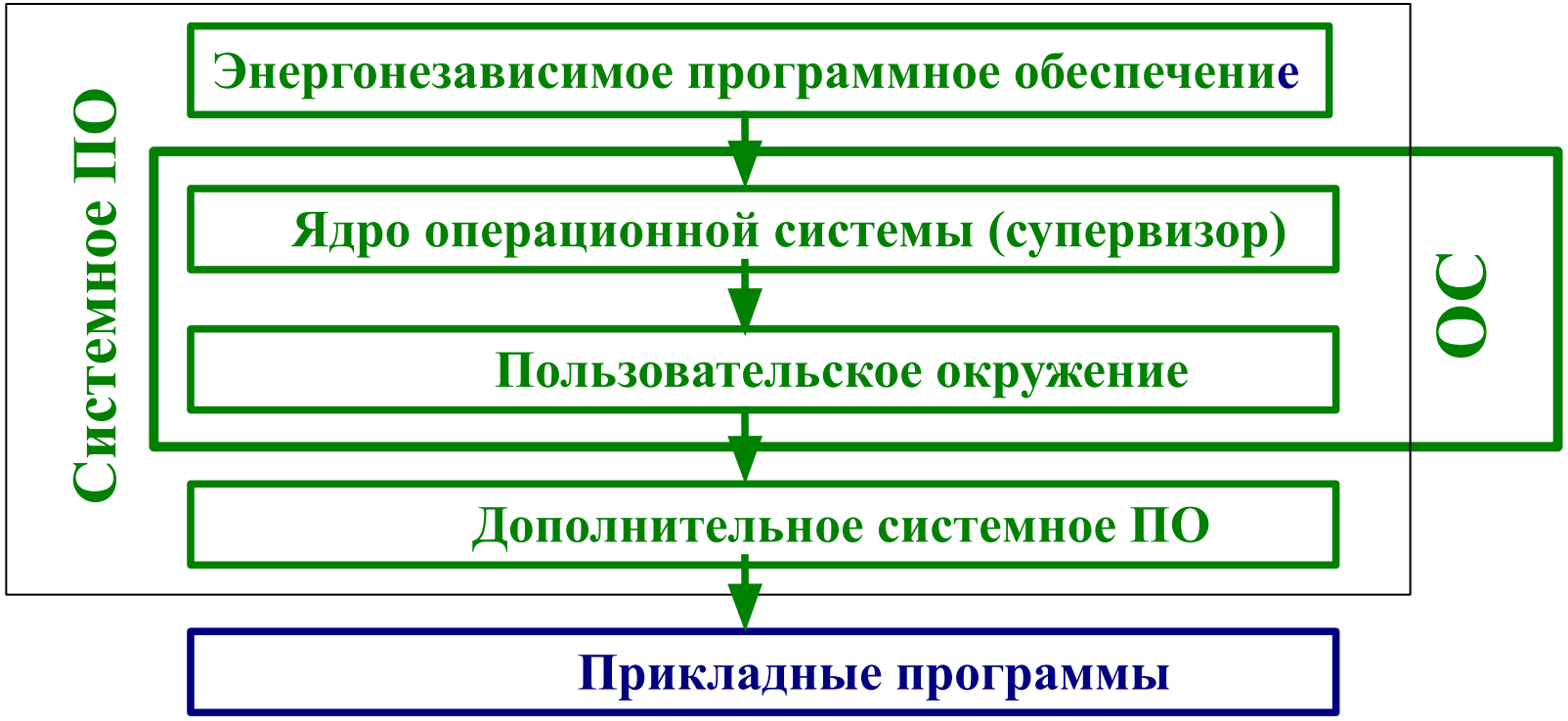
Основные положения

Информационные системы для оперативных и стратегических решений

Экспертные системы для поддержки принятия решений

Назначение операционных систем (ОС)

Место ОС в программном обеспечении



Энергонезависимое программное обеспечение

Энергонезависимое программное обеспечение (микропрограмма) — системное программное обеспечение, встроенное («зашитое») в аппаратное устройство, и хранящееся в его энергонезависимой памяти. Микропрограммы («прошивки») применяются везде, где применяются микропроцессоры: в мобильных телефонах, фотоаппаратах и т. п. В системном ПО персонального компьютера в этом качестве обычно используется BIOS.

BIOS (basic input/output system — «базовая система ввода-вывода») предназначена для обеспечения доступа операционной системы к аппаратуре компьютера и подключенным к нему устройствам.

[*Википедия*]

Операционная система

Операционная система — комплекс программ связывающих прикладное программное обеспечение с аппаратными устройствами (hardware).

Операционная система — комплекс управляющих и обрабатывающих программ, которые, с одной стороны, выступают как интерфейс между устройствами вычислительной системы и прикладными программами, а с другой стороны — предназначены для управления устройствами, управления вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений.

[*Википедия*]

Назначение операционных систем (ОС)

Функции операционных систем

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

[*Википедия*]

Операционная система UNIX

UNIX — семейство переносимых, многозадачных и многопользовательских операционных систем. Первая система UNIX была разработана в **1969 г**.

Некоторые отличительные признаки UNIX-систем включают в себя:

- использование простых текстовых файлов для настройки и управления системой;
- широкое применение утилит, запускаемых в командной строке;
- взаимодействие с пользователем посредством виртуального устройства — терминала и т. п.

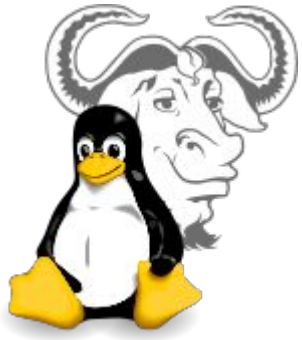
Пример команды UNIX:

```
% ls -l a.out
```

- Дать перечень файлов, находящихся в текущем каталоге. Ключ -l обеспечивает вывод более подробной информации, включая размер файлов, их принадлежность и дату создания.

Впечатления 1996 г.: редактор, регистры и т. п.

Операционная система LINUX



Linux — общее название Unix-подобных операционных систем, библиотек и системных программ, разработанных в рамках проекта GNU (GNU's Not UNIX)

В настоящее время система GNU/Linux, более широко известная как просто **Linux**, достаточно распространена.

В 1991 году, во время обучения в Хельсинкском университете Ли́нус Торвальдс заинтересовался операционными системами в следствие чего начал работать над своей собственной операционной системой которая в итоге стала Linux.

Дистрибутивы на основе Линукс имеют широкое применение в различных областях: от встраиваемых систем до суперкомпьютеров, надёжно удерживают лидирующие позиции на рынке серверов. Также растёт использование Линукс в качестве системы для дома и офиса.

[*Википедия*]

Операционная система MS DOS

MS-DOS — коммерческая операционная система фирмы Microsoft для IBM PC-совместимых персональных компьютеров. **MS-DOS** была создана в 1981 году по заказу IBM и в ходе её развития было выпущено восемь крупных версий (1.0, 2.0 и т. д.)

Версия	Дата	Описание
1.0	март 1979	Поддержка только дисководов 5,25" FAT12.
.....		
8.0	сентябрь 2000	Как часть Windows ME .

Минимальный набор файлов MS-DOS:

Файлы ядра:

BOOT.MBR — загрузчик, находящийся на нулевом секторе и передающий управление на IO.SYS

IO.SYS — расширение BIOS

MSDOS.SYS — обработка прерываний

Командный процессор:

COMMAND.COM — командный процессор (поддержка интерфейса командной строки).

[*Википедия*]

Назначение операционных систем (ОС)

Операционная система Windows

В настоящее время Microsoft Windows установлена более чем на 89 % персональных компьютеров и рабочих станций.

Среди различных версий Microsoft Windows по данным W3Schools на апрель 2011 наиболее популярна Windows XP,

[*Википедия*]

Компьютерные вирусы, трояны, черви

Компью́терный ви́рус — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликация).

Троя́нская программа — вредоносная программа, распространяемая людьми. В отличие от вирусов и червей, которые распространяются самопроизвольно.

Сетевой червь — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Программы шпионы (Spyware) — программное обеспечение, осуществляющее управлением компьютером без согласия самого пользователя. *(рассматриваются в разделе Internet)*

Вирусы

Вирусы распространяются, копируя себя и обеспечивая последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом может быть не только программа (.EXE, .COM), но и пакетные файлы, макросы Microsoft Word и Excel и т. п.

Каналы распространения: дискеты (1980-90 годы), флешки, электронная почта и т. п. Как это происходит.

Примеры:

- Почтовый вирус : "Я новый почтовый вирус-троян ..."
- Первый вирус: (Боб Томас в 1971 г.) Программа «Ползун», которая самостоятельно копировала себя с одного компьютера на другой, перемещаясь таким образом по сети, и выводила на экран каждого терминала следующее сообщение: «Я — Ползун! Если сможешь, поймай меня!».
- Первыми вирусами для ПК являются Virus 1,2,3 и Elk Cloner. Оба вируса очень схожи по функциональности и появились независимо друг от друга с небольшим промежутком во времени в 1981 году.

История вирусов

1981 г. Ричард Скрента написал один из первых **загрузочных вирусов**, который обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение.

1985 г. Ги Вонг написал программу DPROTECT — первый резидентный вирус.

1987 г. - первая эпидемия была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Алви. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

История вирусов

1988 г. Первая пандемия (вирус Jerusalem). Долго не проявлял себя, но в пятницу 13 мая 1988 вирус по всему миру начал уничтожать файлы при их запуске.

1989 г. Был создан первый вирус, противодействующий антивирусному программному обеспечению — The Dark Avenger. Он заражал новые файлы, пока антивирусная программа проверяла жёсткий диск компьютера.

1990 г. Первый полиморфный вирус — Chameleon, который формировал программный код «на лету».

1991 г. Разразилась эпидемия вируса **Dir-II**.

1991 - 1995 гг. отработка стелс- и полиморфных технологий (OneHalf и др.)

1996 г. Появился первый вирус для Windows 95 — Win95.Boza

1998 г. CIH, или «Чернобыль» резидентный вирус, работающий только под операционной системой Windows 95/98.

История вирусов

Вирусом может быть не только исполняемая программа (.EXE, .COM), но и объектные модули (.OBJ), пакетные файлы (.BAT), макросы Microsoft Word и Excel и т. п.

Вирусы сейчас встречаются сравнительно редко. Они вытесняются всевозможными **сетевыми червями и шпионскими программами**. При этом вирусы заражают сетевых червей и распространяются вместе с ними.

Новый всплеск численности вирусов связан с повсеместным использованием флешек

Трояны

Троянские программы распространяются людьми — непосредственно загружаются в компьютерные системы злоумышленниками, или побуждают пользователей загружать и/или запускать их на своих системах.

Для достижения последнего, троянские программы помещаются злоумышленниками на открытые ресурсы (файл-серверы и т.п.), присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов полученных одним из перечисленных способов.

[*Википедия*]

Примеры троянских коней

1986 г. Троянский конь **pc-write**: первый троянский конь, маскирующийся под известную условно бесплатную программу (в данном случае - текстовый процессор pc-write).

1989 г. Троянский конь AIDS. Вирус маскировался под антивирусную программу и рассылался на дискетах. Делал недоступными всю информацию на жёстком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес». Автор программы был арестован в момент обналичивания чека и осуждён за вымогательство.

.

Примеры троянских коней

1998 г. Back Orifice — троянская программа удаленного администрирования. Программа предназначена для дистанционного контроля над компьютером с операционной системой Windows 95/Windows 98. Существует много разновидностей этого трояна.

2010 г. trojan-ransom.win32 — троянская программа-вымогатель. Маскируется под различные выполняемые файлы (.EXE). Отключает диспетчер задач, безопасный режим и т. п. Существует несколько разновидностей.

Спасибо за внимание!!