BOOT-вирусы

А.В. Неверов

Структура дискового пространства в MS DOS

Параметры диска
Программа начальной загрузки

Таблица размещения файлов

Копия таблицы размещения файлов
В MS DOS 4.0 и выше может быть несколько

Массив записей о файлах и других каталогах

Пространство диска, используемое для хранения информации

BOOT-сектор (MS DOS 3.x)

(0)	2	sect_siz	Количество байтов в одном секторе диска.
(+2)	1	clustsiz	Количество секторов в одном кластере.
(+3)	2	res_sect	Количество зарезервированных секторов.
(+5)	1	fat_cnt	Количество таблиц FAT.
(+6)	2	root_siz	Максимальное количество дескрипторов файлов, содержащихся в корневом каталоге диска.
(+8)	2	tot_sect	Общее количество секторов на носителе данных (в разделе DOS).
(+10)	1	media	Байт-описатель среды носителя данных.
(+11)	2	fat_size	Количество секторов, занимаемых одной копией FAT.

BOOT-сектор (MS DOS 4 и старше)

(+0)	3	Команда JMP xxxx - переход типа NEAR на программу начальной загрузки
(+3)	8	Название фирмы-производителя операционной системы и версия, например: "IBM 4.0"
(+11)	25	Extended BPB - расширенный блок параметров BIOS
(+36)	1	Физический номер дисковода (0 -флоппи, 80h - жесткий диск)
(+37)	1	Зарезервировано
(+38)	1	Символ ')' - признак расширенной загрузочной записи DOS 4.0
(+39)	4	Серийный номер диска (Volume Serial Number), создается во время форматирования диска
(+43)	11	Метка диска (Volume Label)
(+54)	8	Зарезервировано, обычно содержит запись типа 'FAT12 ', которая идентифицирует формат таблицы размещения файлов FAT

Расширенный блок параметров BIOS

(0)	2	sect_siz	**Количество байтов в одном секторе диска.**
(+2)	1	clustsiz	**Количество секторов в одном кластере.**
(+3)	2	res_sect	**Количество зарезервированных секторов.**
(+5)	1	fat_cnt	**Количество таблиц FAT.**
(+6)	2	root_siz	**Максимальное количество дескрипторов файлов, содержащихся в корневом каталоге диска.**
(+8)	2	tot_sect	**Общее количество секторов на носителе данных (в разделе DOS).**
(+10)	1	media	**Байт-описатель среды носителя данных.**
(+11)	2	fat_size	**Количество секторов, занимаемых одной копией FAT.**
			---- Расширение стандартного BPB -----
(+13)	2	sectors	**Количество секторов на дорожке**
(+15)	2	heads	**Количество магнитных головок**
(+17)	2	hidden_l	**Количество скрытых секторов для раздела, который по размеру меньше 32 мегабайтов.**
(+19)	2	hidden_h	**Количество скрытых секторов для раздела, превышающего по размеру 32 мегабайта. (Только для DOS 4.0).**
(+21)	4	tot_secs	**Общее количество секторов на логическом диске для раздела, превышающего по размеру 32 мегабайта.**

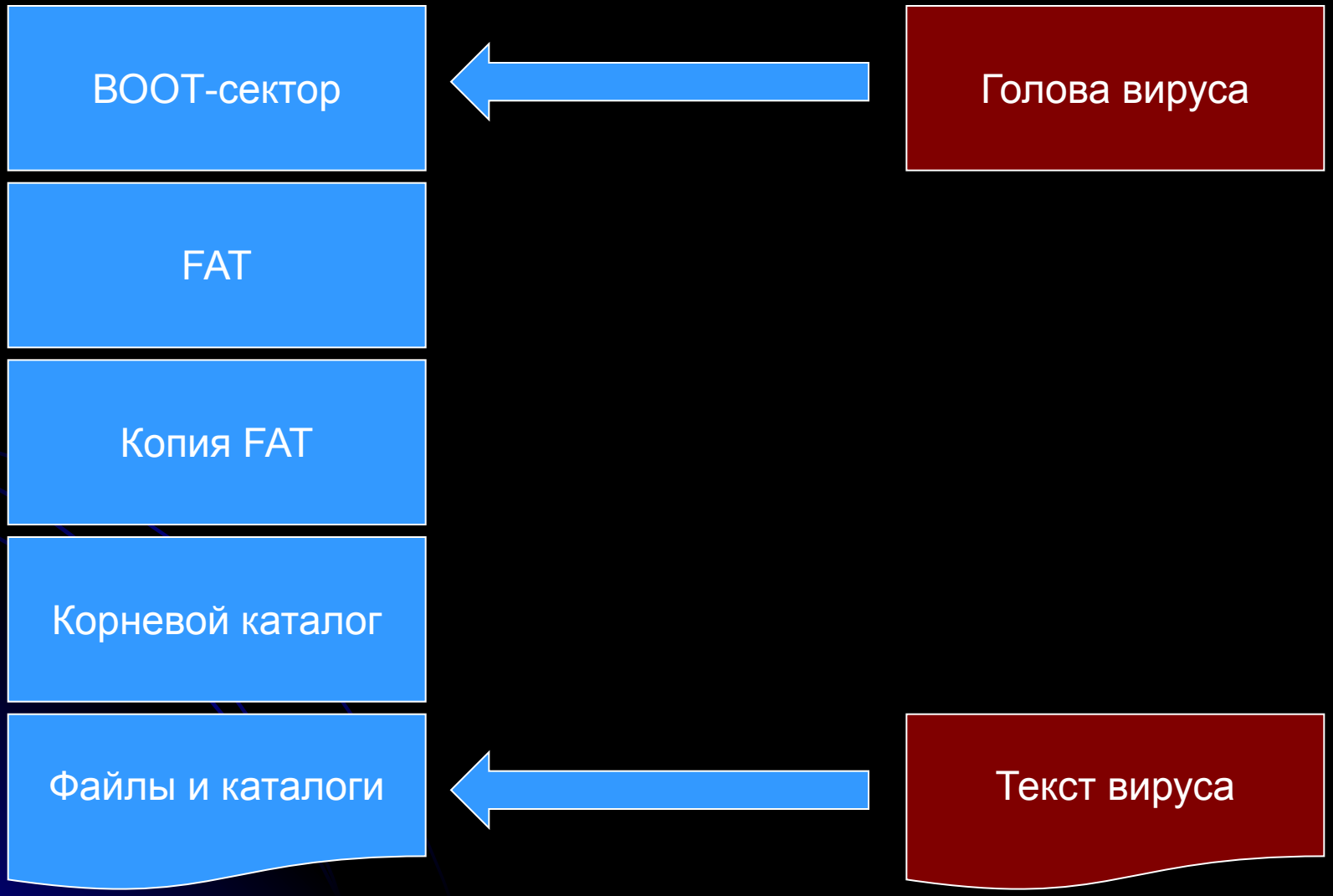
Элементы FAT

FAT12	FAT16	Значение
000h	0000h	Свободный кластер
ff0h - ff6h	fff0h - fff6h	Зарезервированный кластер
ff7h	fff7h	Плохой кластер
ff8h - fffh	fff8h - ffffh	Последний кластер в списке
002h - fefh	0002h - ffefh	Номер следующего кластера в списке

Корневой каталог

Смещение	Размер	Содержимое
(+0)	8	Имя файла или каталога, выравненное на левую границу и дополненное пробелами.
(+8)	3	Расширение имени файла, выравненное на левую границу и дополненное пробелами.
(+11)	1	Атрибуты файла.
(+12)	10	Зарезервировано.
(+22)	2	Время создания файла или время его последней модификации.
(+24)	2	Дата создания файла или дата его последней модификации.
(+26)	2	Номер первого кластера, распределенного файлу.
(+28)	4	Размер файла в байтах.

Структура BOOT-вируса



Внедрение BOOT-вируса

- Голова BOOT-вируса размещается
  - В BOOT-секторе дискеты и занимает всегда один сектор
  - В BOOT-секторе или главной загрузочной области (MBR) диска
- Тело BOOT-вируса размещается
  - В произвольных кластерах диска, обычно помеченных как плохие или зарезервированные
  - В конце файлов (в этом случае BOOT-вирус при внедрении должен модифицировать запись о файле в каталоге и информацию о файле в FAT)

Содержание головы вируса

- Размещение в оперативной памяти нового блока
- Получение физического адреса хвоста вируса на диске
- Размещение хвоста вируса в памяти
- Перехват прерываний (как правило 21h, 13h – прерываний по работе с дисками)
- Установка векторов перехваченных прерываний на точку входа вируса

Содержимое хвоста вируса

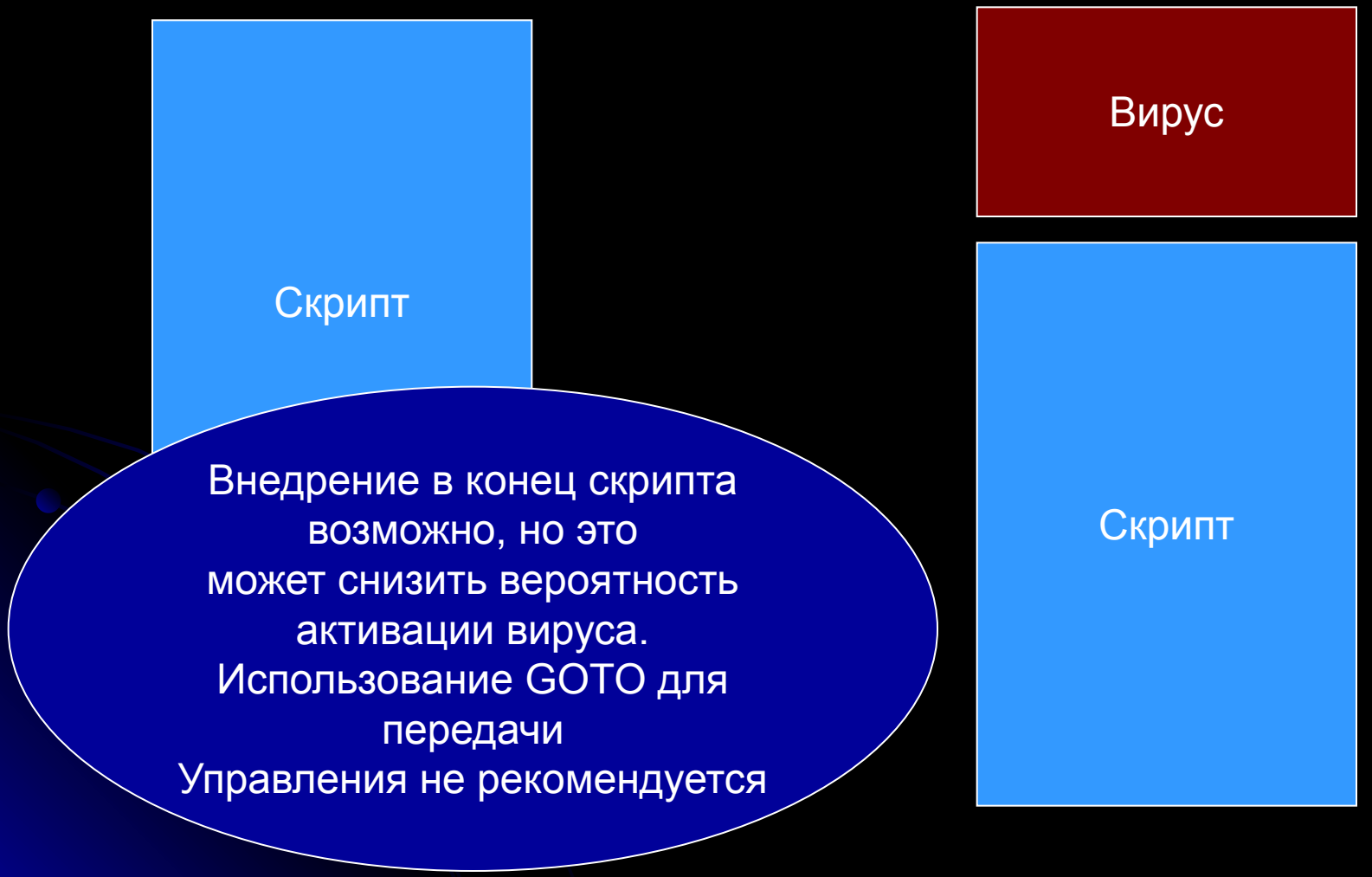
- Вредоносные действия
- Механизм размножения, основанный на изменении BOOT-секторов подключаемых дисков (за счет перехвата прерываний 13h и 21h)

Скрипт-вирусы

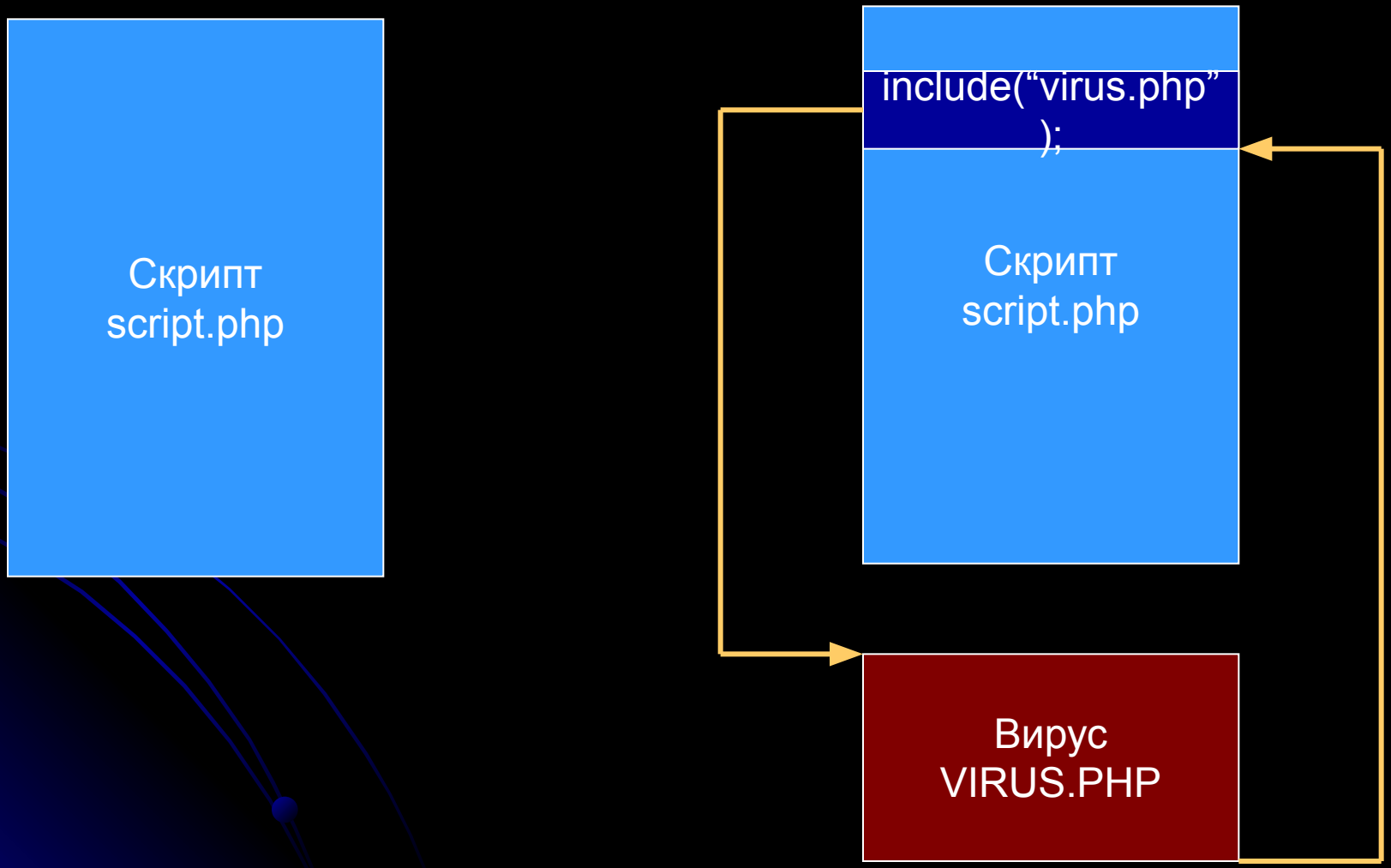
Основные отличия скрипт-вирусов от вирусов в байт-коде

- Разрабатываются на скриптовых языках
  - Perl, PHP, shell и т.д.
- Используют небольшой набор механизмов внедрения
- Для сокрытия своего присутствия обычно используют обфускацию программного кода – использовать шифрование могут только некоторые вирусы, в основном, написанные на языке Perl

Прямое внедрение скрипт-вируса



Внедрение вызовом



Макровирусы

Необходимые условия существования макровирусов

- Наличие программных пакетов, имеющих возможности написания внутренних программ на встроенных языках, использующих, в первую очередь, возможности самого программного пакета - макроязыках
- Возможность встраивания и/или привязки макропрограмм к файлам (документам), обрабатываемых пакетом
- Возможность копирования макропрограмм из одной инсталляции пакета в другую или из одного документа в другой
- Возможность автоматической активации макропрограмм

Макровирусы

- являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.), а также на скрипт-языках, таких как VBA (Visual Basic for Applications), JS (Java Script)

Принципы работы макровирусов

- макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (Word, Excel, Access);
- макроязык позволяет копировать файлы (AmiPro) или перемещать макропрограммы в служебные файлы системы и редактируемые файлы (Word, Excel);
- при работе с файлом при определенных условиях (открытие, закрытие и т.д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (Word, Excel).

Общие принципы работы Office-вирусов

- При работе с документами программы Office выполняют большое количество стандартных макрокоманд – Open, FileSave, FileSaveAs и т. д.
- При выполнении стандартных операций могут выполняться автоматические макросы – AutoSave, AutoClose, AutoExit, AutoNew и т.д.
- Макровирусы используют эти возможности
  - Создание нового авто-макроса
  - Переопределение стандартного авто-макроса
  - Переопределение стандартного макроса (чаще всего Open)

Макровирусы для Microsoft Word

- Макровирусы копируют свой код в область глобальных макросов
  - Использование макроса MacroCopy
  - Использование редактора макросов – создание нового макроса, копирование кода и сохранение
- При закрытии Word автоматически сохраняет макросы в шаблоне документов NORMAL.DOT
- При запуске Word автоматически загружает вредоносный код (видоизменненые макросы)
- При выполнении этих макросов код записывается в обрабатываемые файлы

Макровирусы для Microsoft Excel

- Аналогично Microsoft Word
- Из-за отсутствия шаблона NORMAL.DOT текст вируса сохраняется в файлах каталога STARTUP
- Для создания вирусов могут использоваться язык VBA или встроенный язык электронных таблиц Excel 4