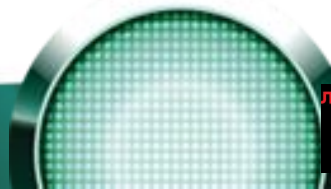
# Вредоносное программное обеспечение и методы борьбы с ним





# Вредоносное ПО

- ПО, наносящее вред
  - программно-аппаратному обеспечению атакуемого компьютера (сети)
  - данным пользователя ПК
  - самому пользователю ПК (косвенно)
  - пользователям других ПК (опосредованно)

# Основные компьютерные угрозы

- Вредоносные программы
- Спам
- Сетевые атаки

---

- утечка/потеря информации
- нештатное поведение ПО
- резкий рост входящего/исходящего трафика
- замедление или полный отказ работы сети
- потеря времени
- доступ злоумышленника в корпоративную сеть
- риск стать жертвой мошенников

# Современные интернет-угрозы

- Похищение конфиденциальной информации
- Зомби-сети
  - рассылка спама
  - DDoS-атаки
  - троянские прокси-сервера
- Шифрование пользовательской информации с требованием выкупа
- Атаки на антивирусные продукты

# Основные виды современных вредоносных программ

# Разнообразие классификаций

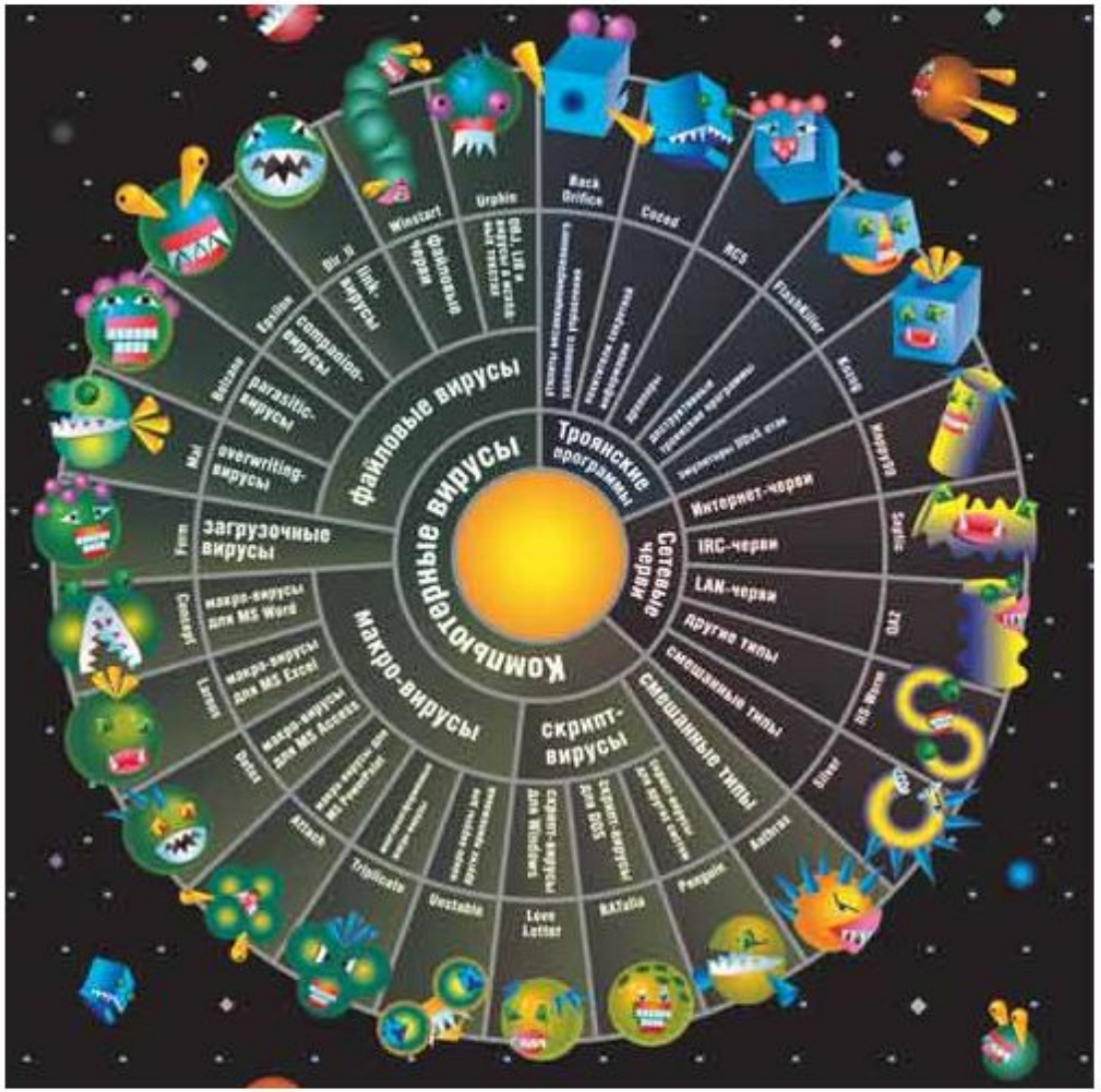



*Рис. 1. Классификация вредоносных программ (источник: «Лаборатория Касперского»)*

# Актуальность вопроса

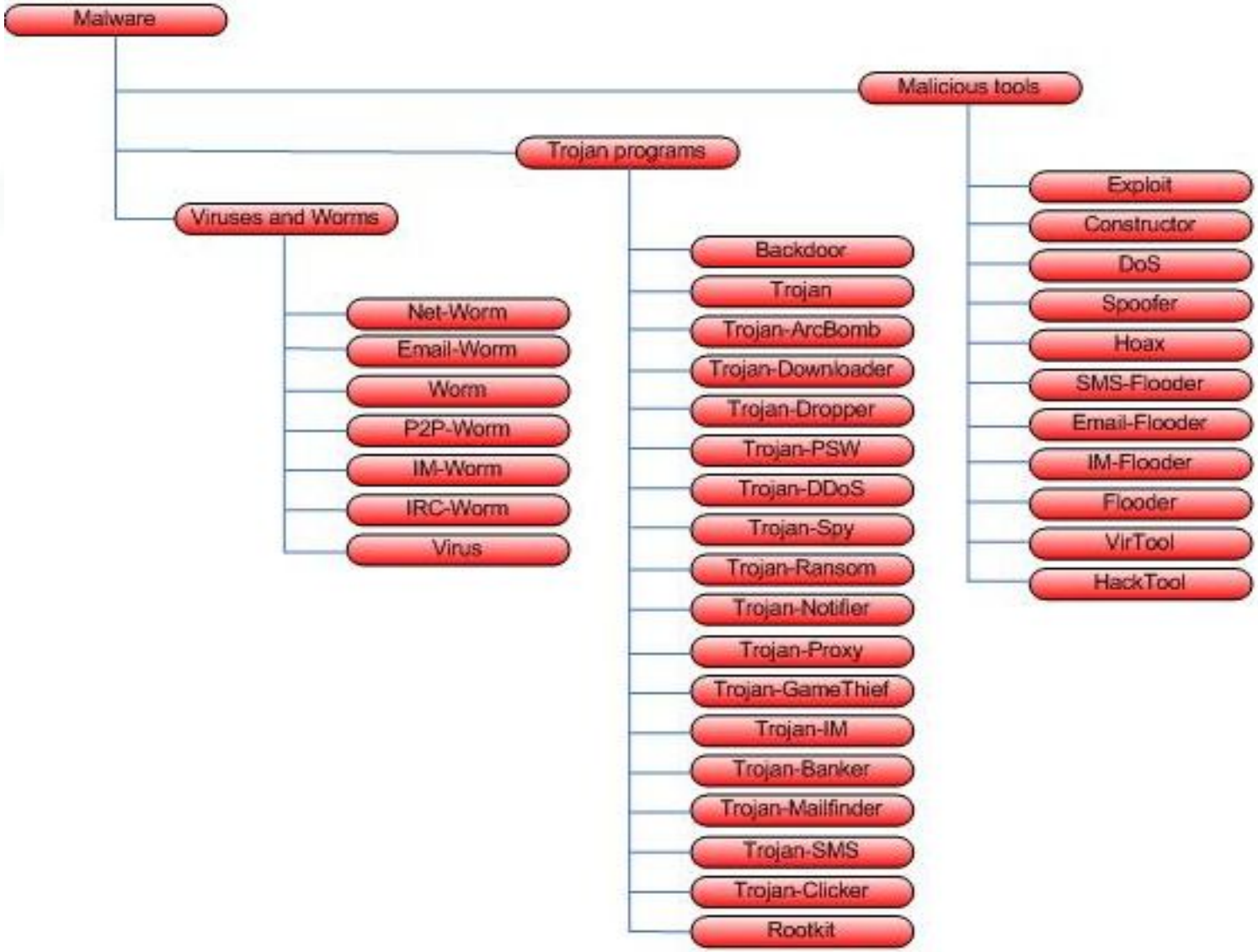
- Разнообразие классификаций
- Многообразие понятий
- Неоднозначность определений
- Сложность в понимании
- Проблемы с переводами на иностранные языки
- Сложности при именовании вредоносных объектов
- Многообразие понятий при создании аналитической и маркетинговой информации

# Malware

***Malware***

Вредоносные программы, созданные специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы, черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников (инструменты для взлома, конструкторы полиморфного вредоносного кода и т.д.).

# Дерево классификации детектируемых объектов



# Сетевые черви

# Сетевые черви

- Программы, распространяющие свои копии через сеть с целью
  - проникновения на удаленные компьютеры
  - запуска на них своих копий
  - возможного выполнения деструктивных действий
  - дальнейшего распространения по сети

# Классификация сетевых червей

**Email-Worm**
(почтовые черви)

**IRC-Worm**
(черви в IRC-каналах)

**IM-Worm**
(черви, использующие интернет-пейджеры)

**P2P-Worm**
(черви для сетей обмена файлами)

**Net-Worm**
(прочие сетевые черви)

# Классические компьютерные вирусы

# Классические компьютерные вирусы

- Программы, заражающие объекты ОС
  - секторы
  - программы
  - документы и др.
- Цель
  - получить управление при их запуске
- Задачи
  - запуск себя при определенных действиях пользователя
  - дальнейшее внедрение в ресурсы системы
  - выполнение деструктивных действий

# Классификация вирусов

- По среде обитания
  - Файловые вирусы
  - Загрузочные вирусы
  - Макро-вирусы
  - Скриптовые вирусы

# Троянские программы

# Троянские программы

- Программы, действующие без ведома пользователя
  - сбор информации и ее разрушение
  - злонамеренное изменение данных и/или передача их злоумышленнику
  - нарушение работоспособности системы
  - использование ресурсов компьютера в злоумышленных целях

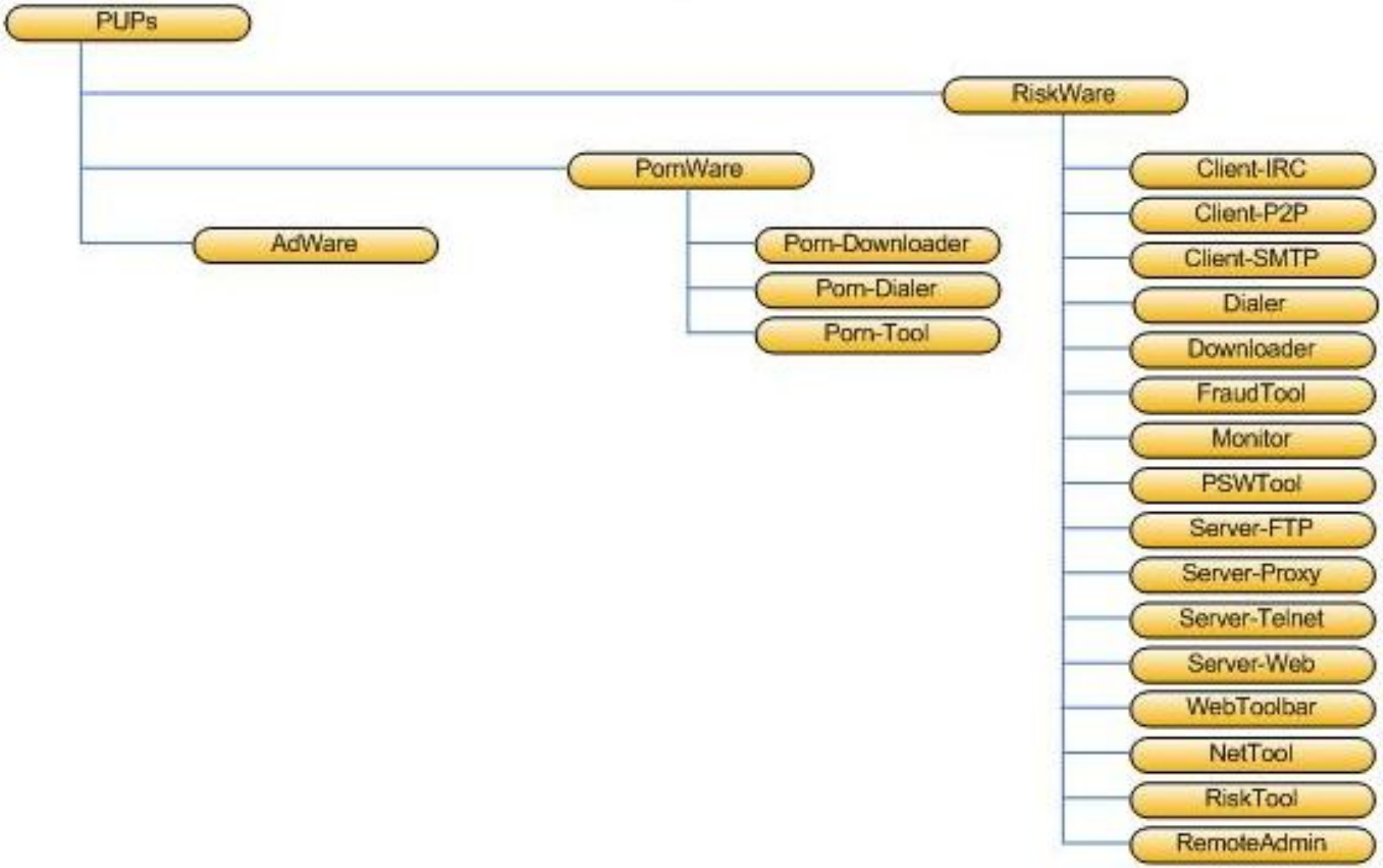
# Классификация троянских программ

| | |
|---|---|
| **Backdoor** | (удаленное администрирование) |
| **Trojan-PSW** | (воровство паролей) |
| **Trojan-Clicker** | (интернет-кликеры) |
| **Trojan-Downloader** | (доставка вредоносных программ) |
| **Trojan-Dropper** | (инсталляторы вредоносных программ) |
| **Trojan-Proxy** | (троянские прокси-серверы) |
| **Trojan-Spy** | (шпионские программы) |
| **Trojan** | (прочие троянские программы) |
| **Rootkit** | (сокрытие присутствия в ОС) |
| **ArcBomb** | («бомбы» в архивах) |
| **Trojan-Notifier** | (оповещение об успешной атаке) |

# Условно опасные программы

PUPs – Potentially Unwanted Programs

# Дерево классификации детектируемых объектов

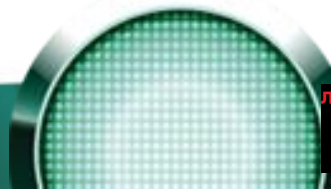


# Условно опасные программы (PUPs)

- Разрабатываются и распространяются легальными компаниями
- Могут использоваться в повседневной работе
  - утилиты удаленного администрирования и т.п.
- Обладают набором функций, которые могут причинить вред пользователю только при выполнении ряда условий
- Могут быть опасны в руках злоумышленника

# Хакерские утилиты и прочие вредоносные программы

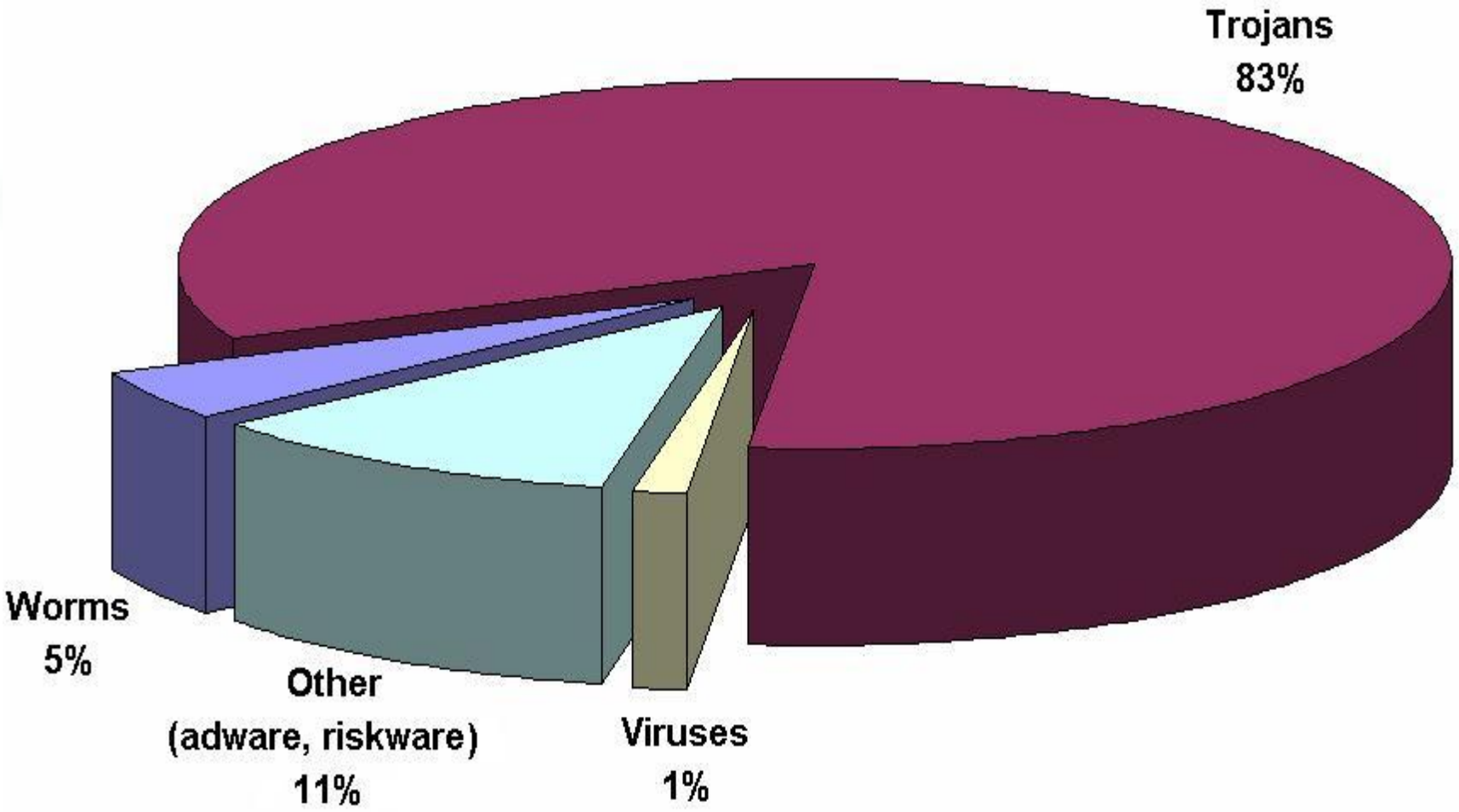




# Хакерские утилиты и прочие вредоносные программы

- Сетевые атаки
- Взломщики удаленных компьютеров
- «Замусоривание» сети
- Конструкторы вирусов и троянских программ
- Злые шутки, введение пользователя в заблуждение
- Фатальные сетевые атаки
- Сокрытие от антивирусных программ
- Полиморфные генераторы
- Средства написания, изучения вирусов

# Состав вредоносных программ за 2006-2007



# Методы борьбы с вредоносными программами

# Задачи антивируса

- Противодействие проникновению вредоносных программ в систему
- Обнаружение в системе уже имеющихся вредоносных программ
- Минимизация ущерба от действий вредоносных программ
- Удаление вредоносных программ без нанесения ущерба остальным объектам системы

# Методы антивирусной защиты

- Сигнатурное детектирование
- Проактивная защита
  - эвристическое детектирование
  - поведенческие блокираторы

# Оценка эффективности антивирусных решений

# Предмет исследования

- Функционал
- Скорость работы
- Частота обновления антивирусных баз
- Качество работы отдельных компонентов

---

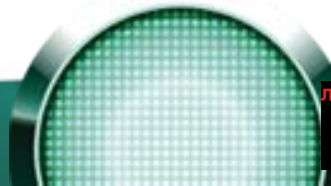
- Основа любого решения – ядро антивируса («антивирусный движок»)

# Критерии оценки антивирусного ядра

- Качество детектирования
- Диапазон детектирования
- Скорость проверки на вирусы
- Поддержка архивированных файлов
- и т.д.

# Антивирус Касперского 6.0 для Windows Workstations





# Назначение Антивируса Касперского

- Защита персонального компьютера от:
  - вредоносных программ
  - сетевых атак
  - интернет-мошенничества
  - нежелательной интернет-рекламы
  - спама

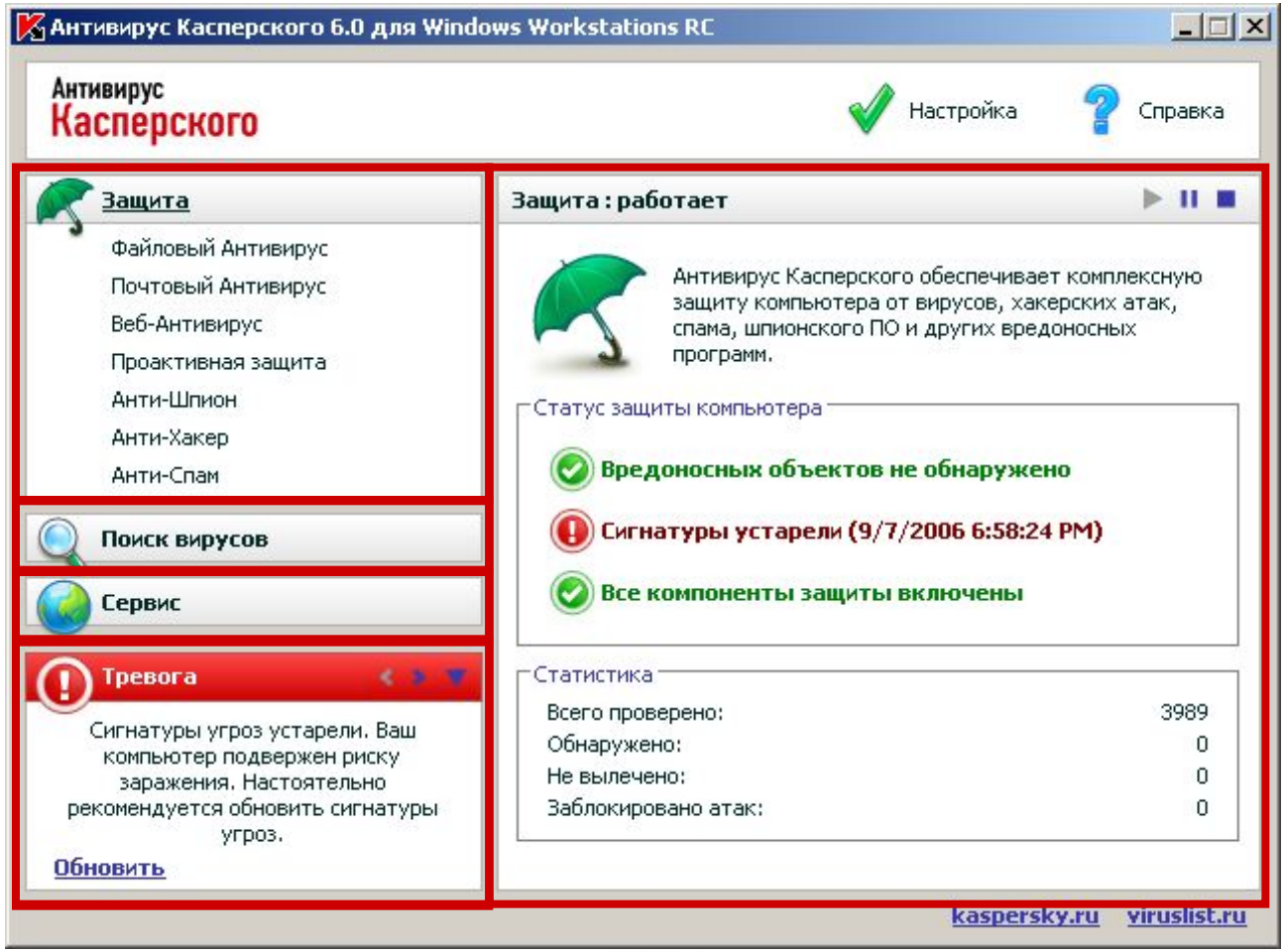
# Компоненты защиты

- Файловый антивирус
- Почтовый антивирус
- Веб-Антивирус
- Проактивная защита
- Анти-Шпион
- Анти-Хакер
- Анти-Спам
- Мастер создания диска аварийного восстановления

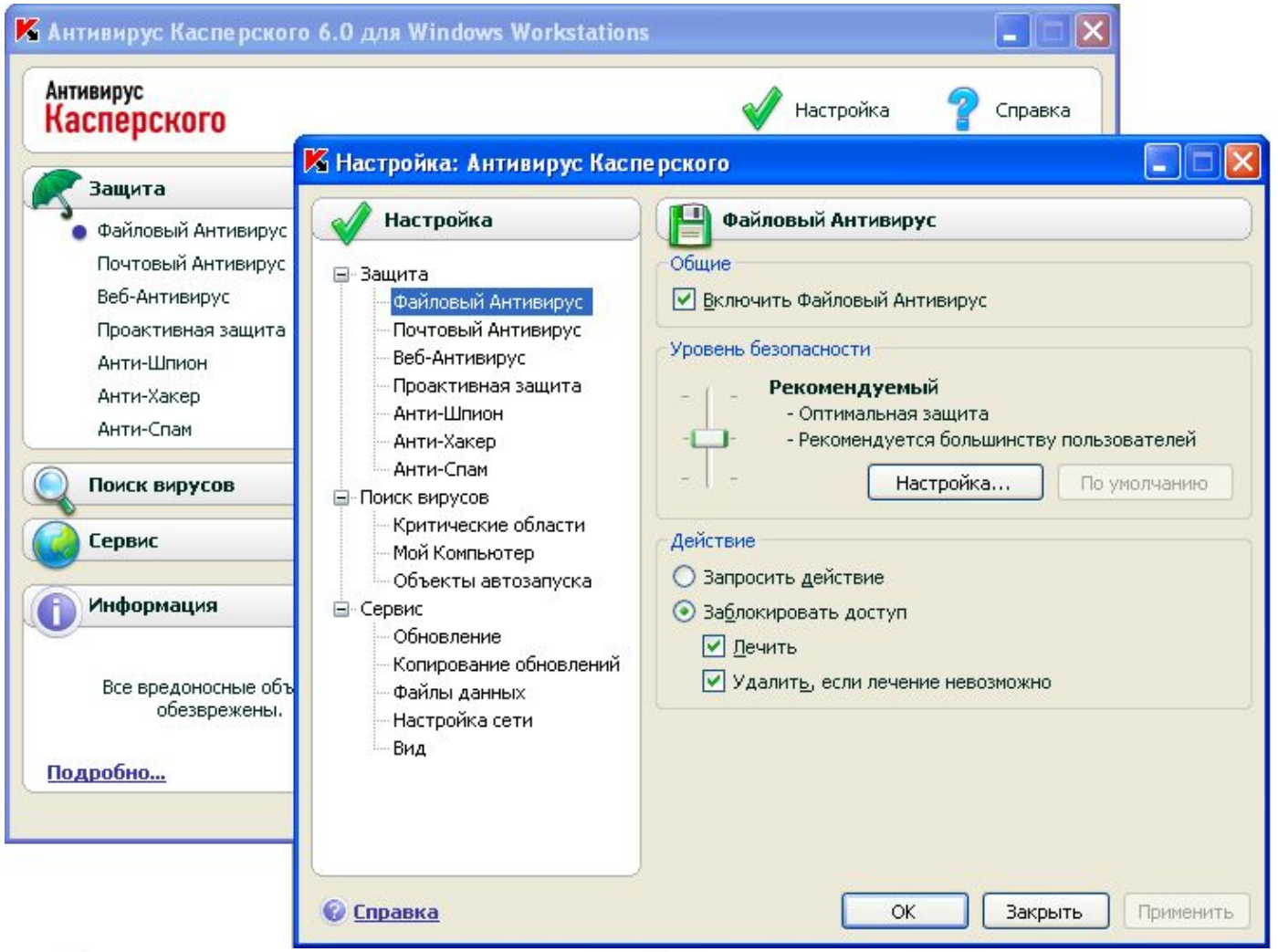
# Распределение функций компонентов защиты

| Информационный поток | Компоненты |
|---|---|
| Съемные носители | • Файловый Антивирус |
| Сетевые ресурсы | • Файловый Антивирус<br>• Анти-Хакер |
| Электронная почта | • Почтовый Антивирус<br>• Анти-Спам |
| Интернет | • Файловый Антивирус<br>• Веб-Антивирус<br>• Анти-Шпион<br>• Анти-Хакер |

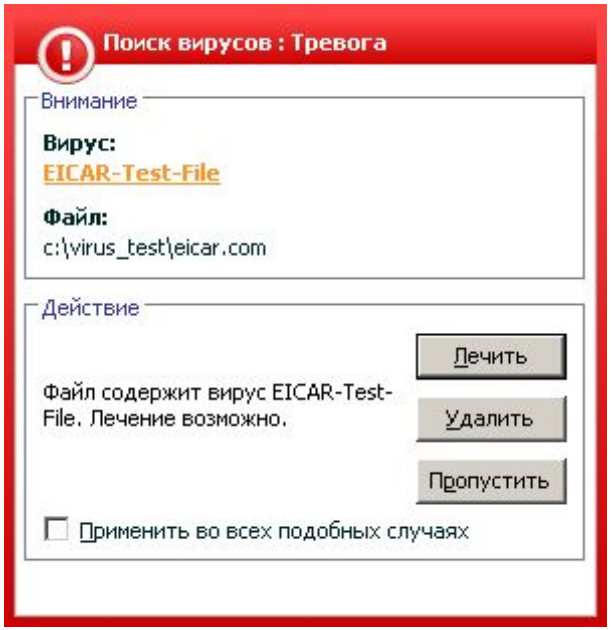
# Пользовательский интерфейс (главное окно)

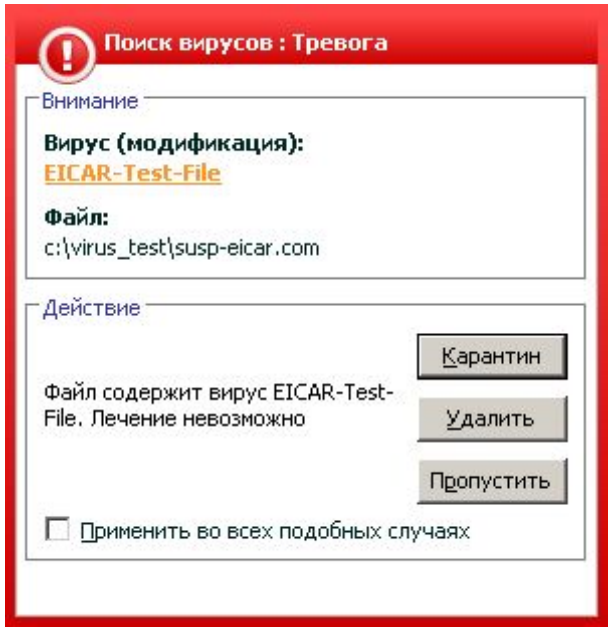


# Пользовательский интерфейс (окно настройки)

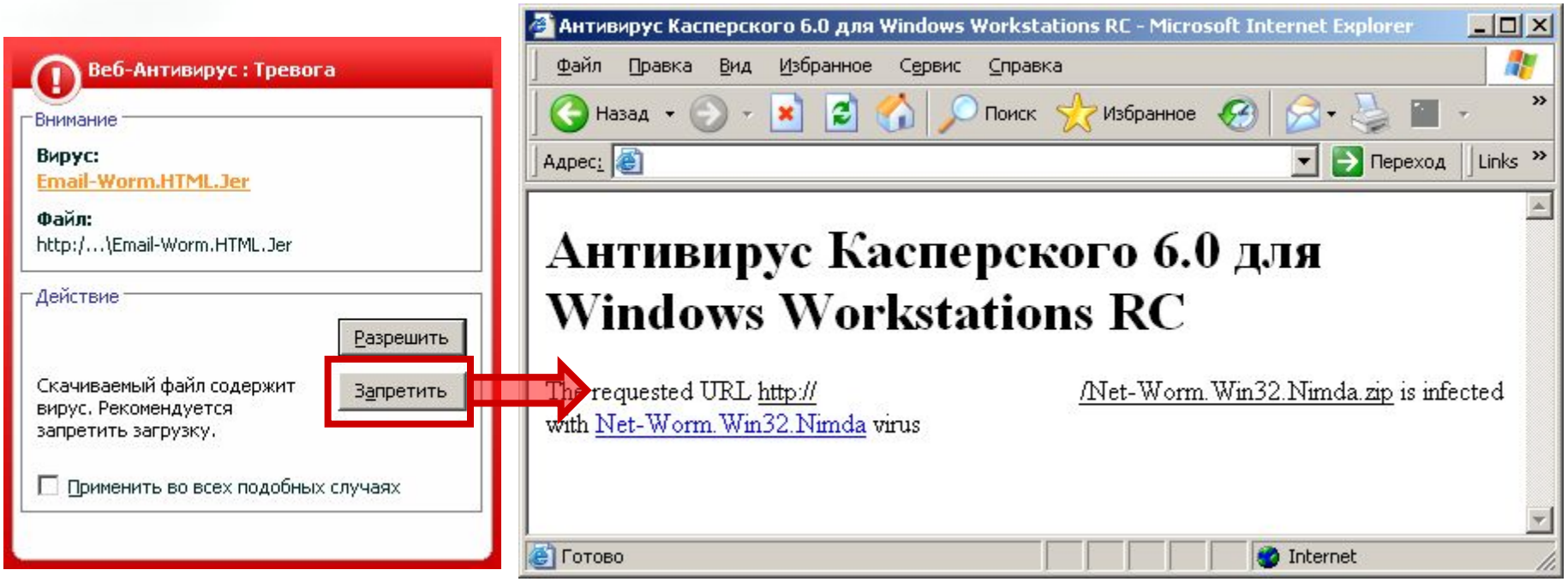


# Обнаружение опасного объекта на локальном или сетевом ресурсе



# Обнаружение опасного объекта на Web-странице



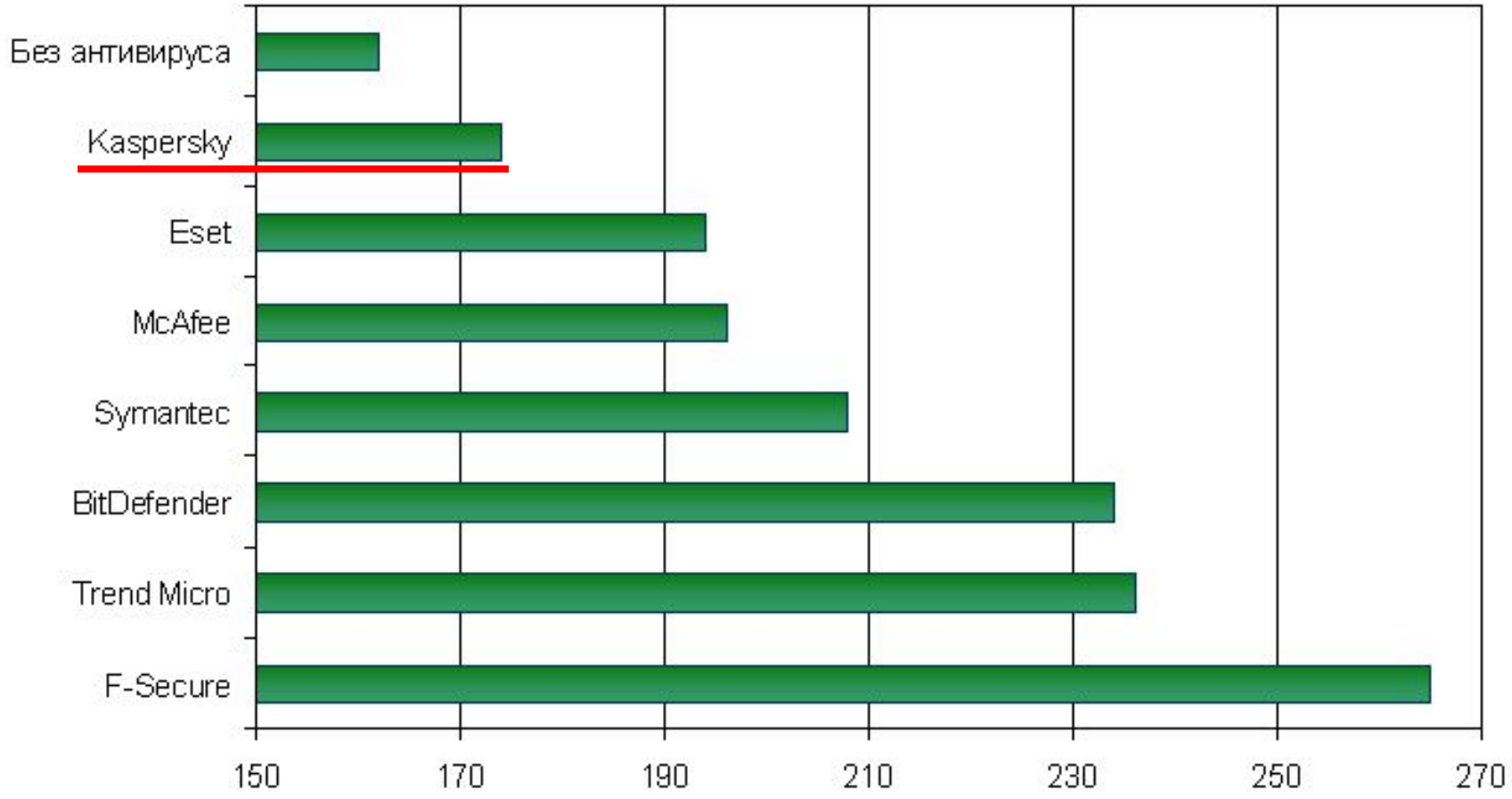
# Качество детектирования

- Сигнатурные методы
  - постоянно обновляемые сигнатуры угроз
- Проактивная защита
  - контроль опасной активности в системе
  - мониторинг системного реестра
  - проверка VBA-макросов
  - обнаружение скрытых процессов (rootkits)
  - откат вредоносных изменений
  - предотвращение вирусных эпидемий

# Скорость работы

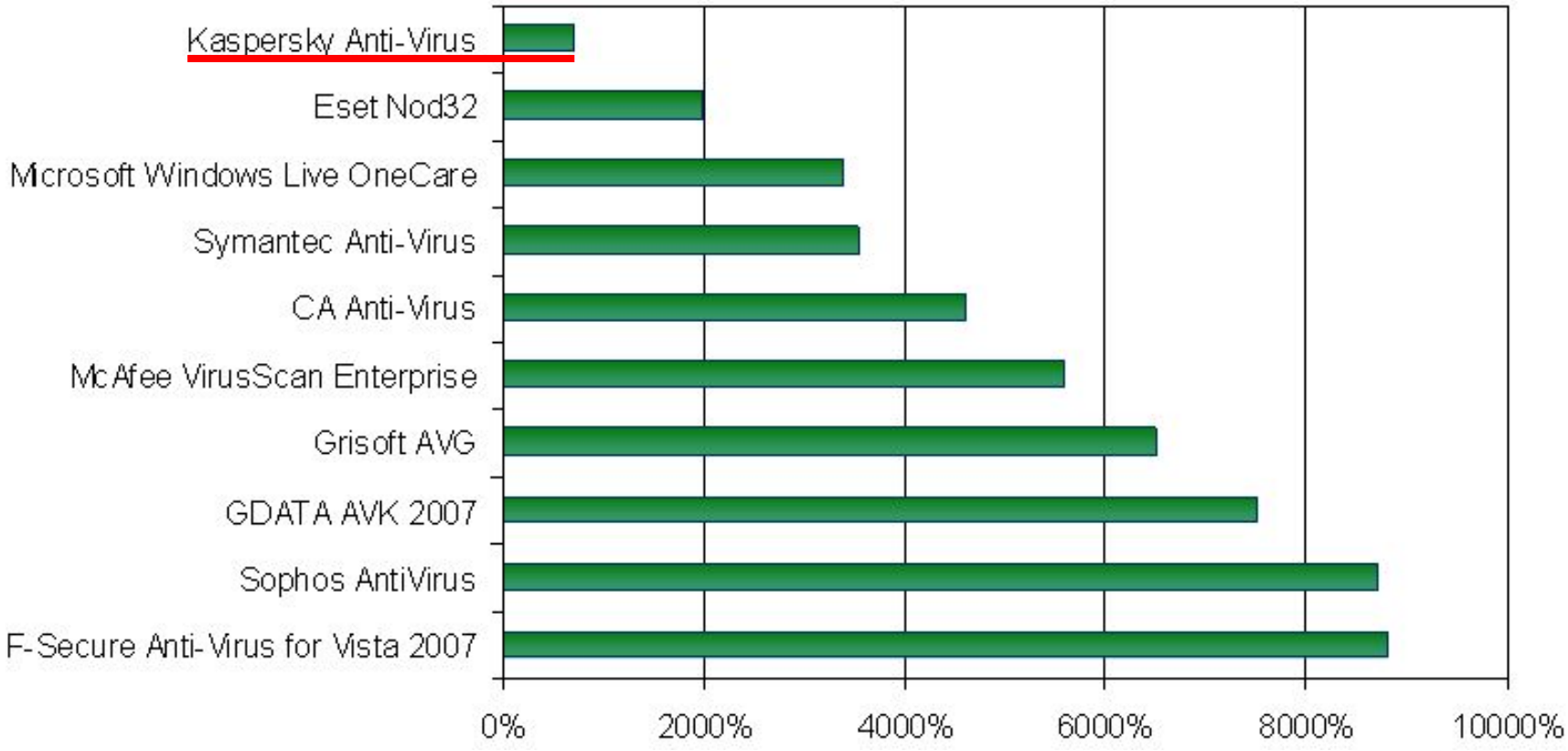
- Технологии iSwift и iChecker
- Возможность приостановки антивирусной проверки
- Распределение ресурсов системы при работе пользовательских приложений
- Адаптация для мобильных ПК
- Доверенные процессы/приложения
- Компактные обновления
- Настройка скорости работы в сети

# Скорость выполнения обычных действий пользователя при проведении проверки по требованию



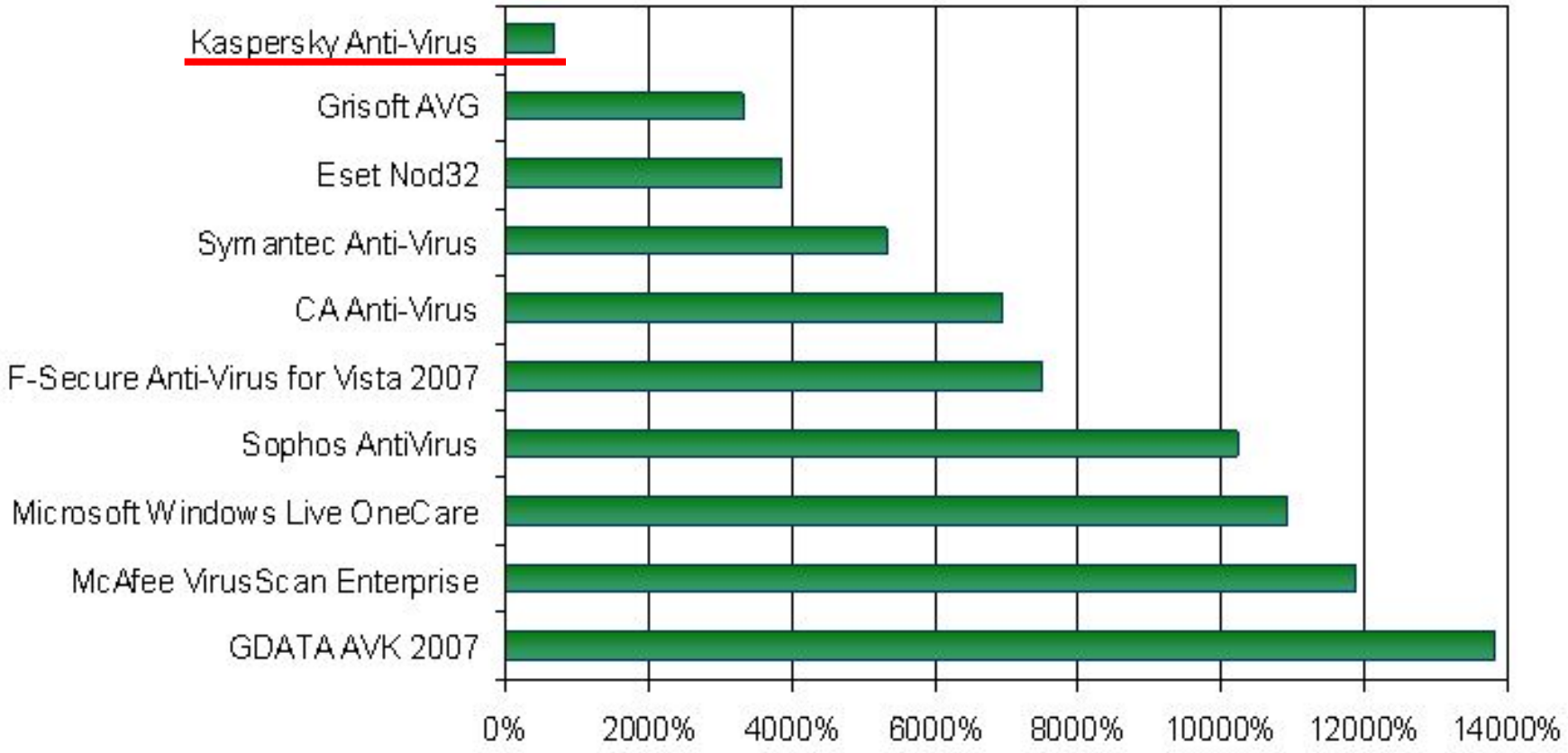

Источник: CNET Labs

# Замедление работы на исполняемых и системных файлах при включенном антивирусном мониторе



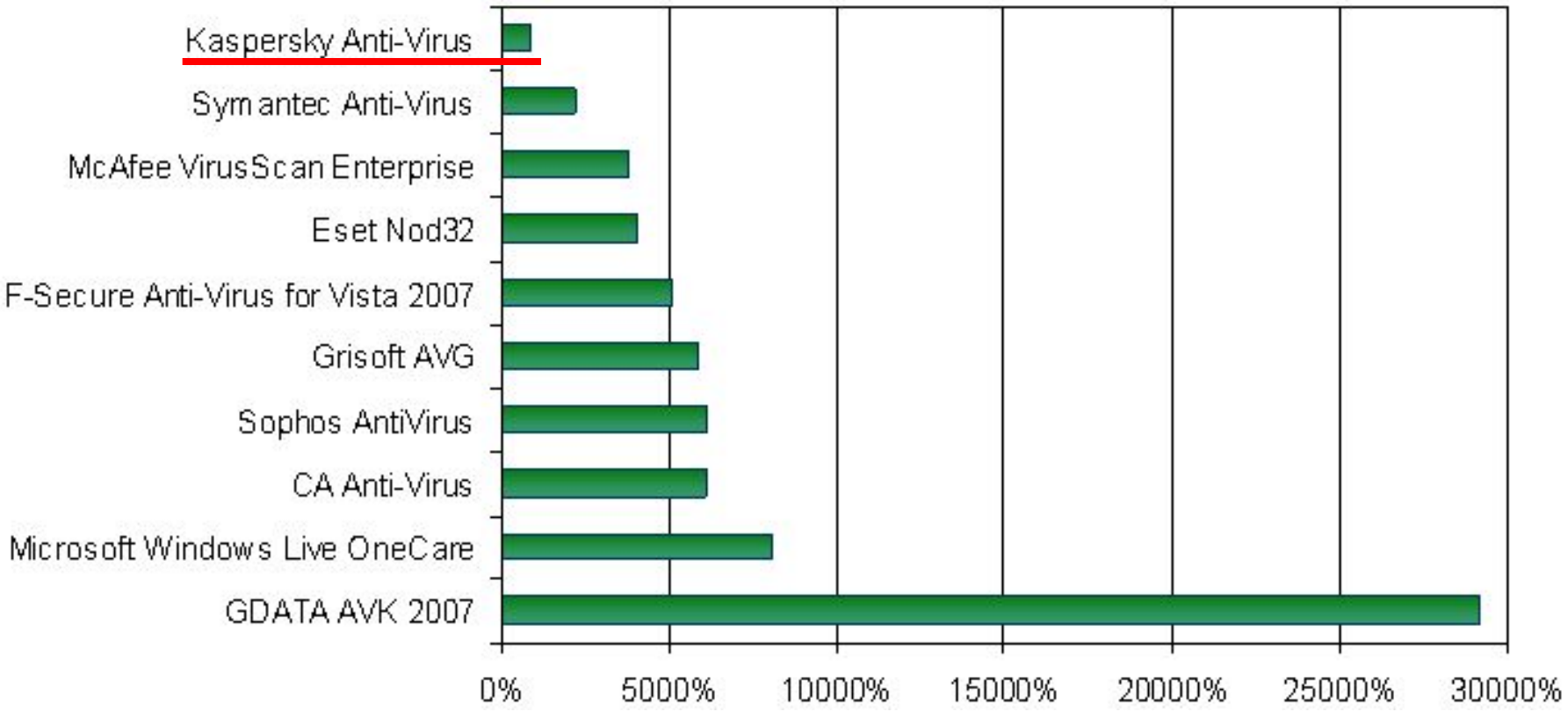

% замедления относительно системы без антивируса
Источник: Virus Bulletin

# Замедление работы на архивах при включенном мониторе




% замедления относительно системы без антивируса
Источник: Virus Bulletin

# Замедление работы на медиафайлах и документах при включенном антивирусном мониторе




% замедления относительно системы без антивируса
Источник: Virus Bulletin

# Возможности Антивируса Касперского для Windows Workstations (версии 5.0 и 6.0)

| Компоненты защиты | 5.0 | 6.0 |
|---|---|---|
| Файловый антивирус | ■ | ■ |
| Почтовый антивирус | ■ | ■ |
| Веб-Антивирус | | ■ |
| Проактивная защита | | ■ |
| Анти-Хакер | | ■ |
| Анти-Шпион | | ■ |
| Анти-Спам | | ■ |

# Тенденции развития вредоносного ПО

# Вредоносное ПО сегодня

- Похищение конфиденциальной информации
- Зомби-сети: рассылка спама, DDoS-атаки, троянские прокси-сервера, ботнеты
- Шифрование пользовательской информации с требованием выкупа
- Атаки на антивирусные продукты

**Криминализация Интернета!**

**Вирусописателями движет выгода!**

# Похищение информации

- Финансовая информация (онлайн-банки и системы Интернет-платежей, Интернет-аукционы)
  - Фишинг
  - Кража логинов, паролей и т.д. (троянские программы, клавиатурные шпионы)
- Пароли-логины Instant Messengers (ICQ и др.), e-mail
- Сбор электронных адресов для последующей рассылки спама
- Пароли к онлайн-играм, кража виртуальной собственности

# Фишинг в Росии

- фишинговая атака на пользователей электронной платежной системы Яндекс.Деньги

  "Уважаемый пользователь,

  Согласно пункту 4.6.2.5. Соглашения об использовании Системы "Яндекс.Деньги", Ваш счет заблокирован. Необходима реактивация счета в системе. Для реактивации проследуйте по линку: (ссылка на yanclex.ru) Либо свяжитесь с одним из наших операторов«.

# Атаки на антивирусные компании

## Противодействие антивирусным технологиям:

- Остановка антивирусного продукта или апдейтера
- Изменение настроек антивирусного продукта
- Авто-нажимание на клавишу “Skip”
- Средства, скрывающие присутствие вредоносных программ – руткиты (Rootkits)
- Шифровка и/или паковка исполняемых файлов-троянцев
- Генерация многочисленных троянцев за короткий промежуток времени

# Шокирующие факты

- Интернет - основной канал распространения вредоносного кода

  *до 4000 вредоносов в неделю, 5000 вредоносных URL в день*

- Среднее время от момента появления компьютера в Интернете до начала атаки на него – 10 минут
- До 90% сообщений, доставляемых по электронной почте, являются спамом или вредоносным кодом
- Воровство частной информации и электронных денег достигло апогея
- Более чем на 90% компьютеров в Интернете установлены программы-шпионы

Спасибо!
Вопросы?
Ваше мнение.