Реальная опасность вирусных угроз и возможные меры противодействия

Андрей Зеренков
Руководитель службы консалтинга
Лаборатория Касперского, Россия, страны СНГ и Балтии

21-23 июня 2005

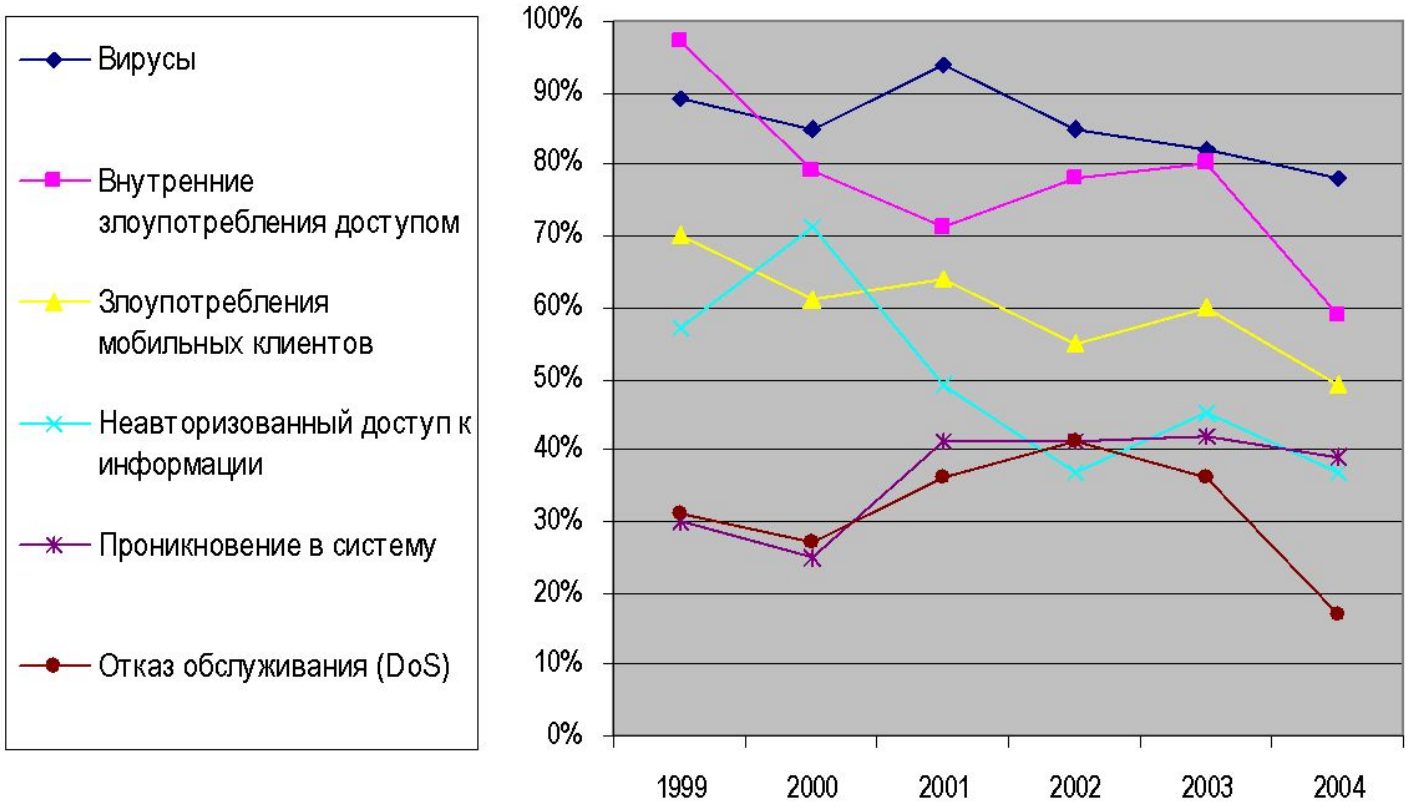
О чём я...

- **...говорить не буду:**
  - Версия 5.0 MP2 существенно отличается не только от версий 4.x, но и от 5.0 по производительности, ресурсоёмкости, функционалу
  - Средства администрирования развиваются семимильными шагами и уже включают, например, поддержку иерархических систем
  - Активно совершенствуются существующие продукты и начата разработка новых на основе наших передовых технологий
- **...собираюсь рассказать:**
  - О том, почему мы всем этим занимаемся, то есть
  - Какова текущая ситуация и, следовательно, требования, и
  - Какова миссия и цель нашей компании

Нарастание угроз ИТ-безопасности

Источник: *CERT Statistics, 2005*

Актуальность различных видов угроз



Источник: *CSI/FBI Computer Crime and Security Survey 2004*

История развития

- Финансовое мошенничество:
  - 1996 – мелкое воровство
  - 1998 – удалённый контроль, шпионаж
  - 2002 – Интернет-мошенничество (е-деньги)
  - 2003 – финансовое мошенничество (банковские операции)
  - 2004 – массовые атаки на Интернет-банки
- Нежелательная реклама:
  - 1994 – появление электронного спама
  - 1999 – навязчивая реклама платных Web-ресурсов
  - 2001 – троянские прокси-серверы (спам)
  - 2002 – троянские рекламные системы
- Шантаж и вымогательство (2002 – 2004):
  - Нелегальный захват Web-ресурсов
  - Хищения конфиденциальной информации
  - DoS-атаки, рэкет

Динамика экономических потерь

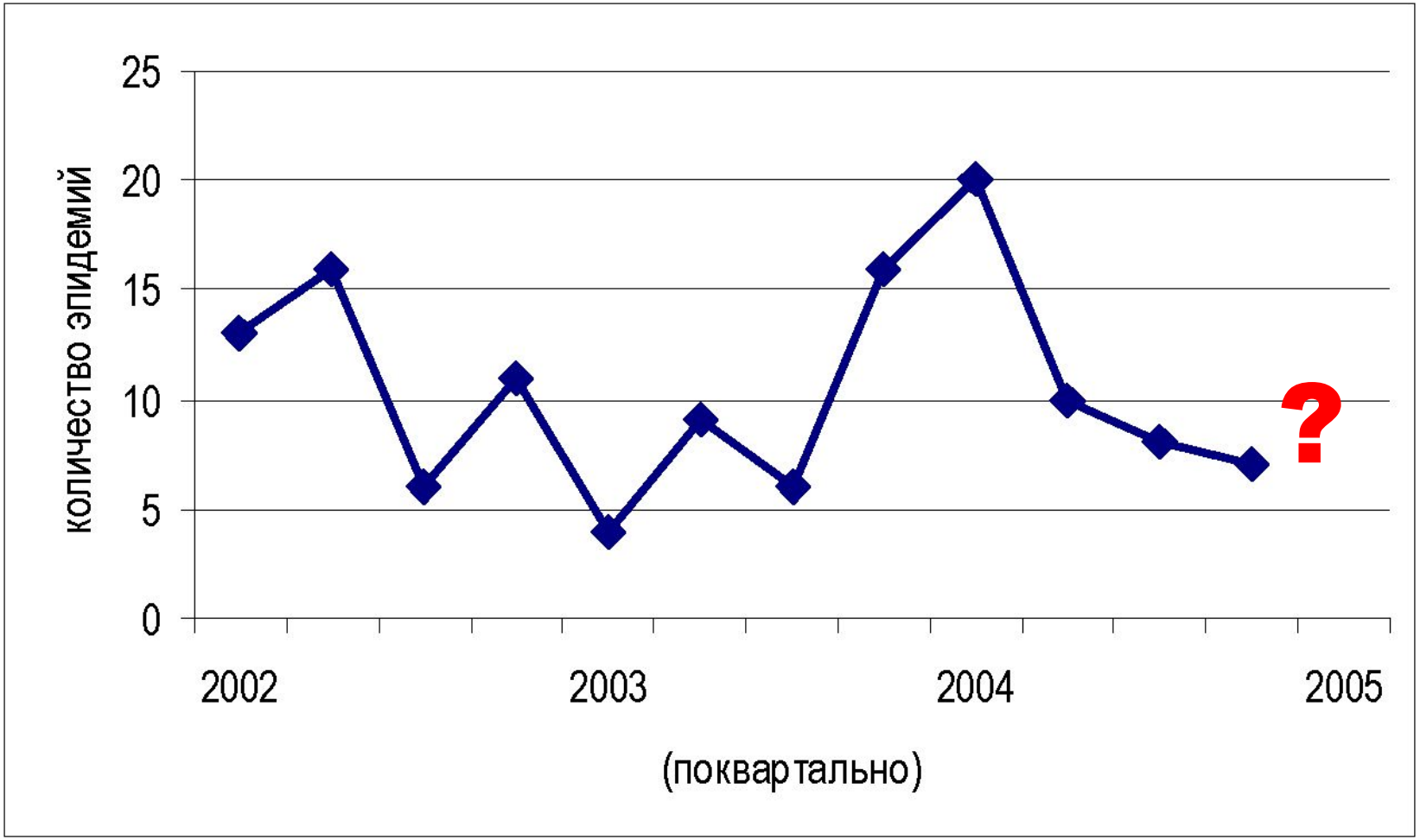
Источник: *Computer Economics, 2005*

Мрачная реальность'2004

- *С февраля по май* экономические потери от нескольких вариантов **MyDoom**, **NetSky**, **Bagle** и **Sasser** превысили **$11 млрд**.
  - Эта рекордная величина достигнута всего за 4 месяца
  - В пиковый период (29 января) **MyDoom** заражал **в час до 12 000** компьютеров
  - Вирусом **Sasser** заражены менее, чем за неделю сотни тысяч компьютеров
- *Июнь:* **Cabir** – первый реальный вирус для мобильный телефонов (OS Symbian + Bluetooth)
- *Июль:* **Duts** – первый реальный вирус для PocketPC-телефонов и КПК
- *Август:* **Brador** – первый троян для PocketPC-устройств
- *Сентябрь:* Очень много шума по проблеме уязвимости обработки файлов **JPEG**
- *Октябрь:*
  - Фиктивный домен ***fedora-redhat.com***, активно завлекавший Linux-пользователей
  - **Opener** – первый реальный зловред (скрипт) для Apple Macintosh OS X
- *Ноябрь:*
  - **Bofra** – минимальное время от объявления уязвимости до её использования (5 дней)
  - **Sober.I** – наибольший «успех» среди зловредов второй половины 2004 года
  - **Skulls** – первый троян для мобильных телефонов

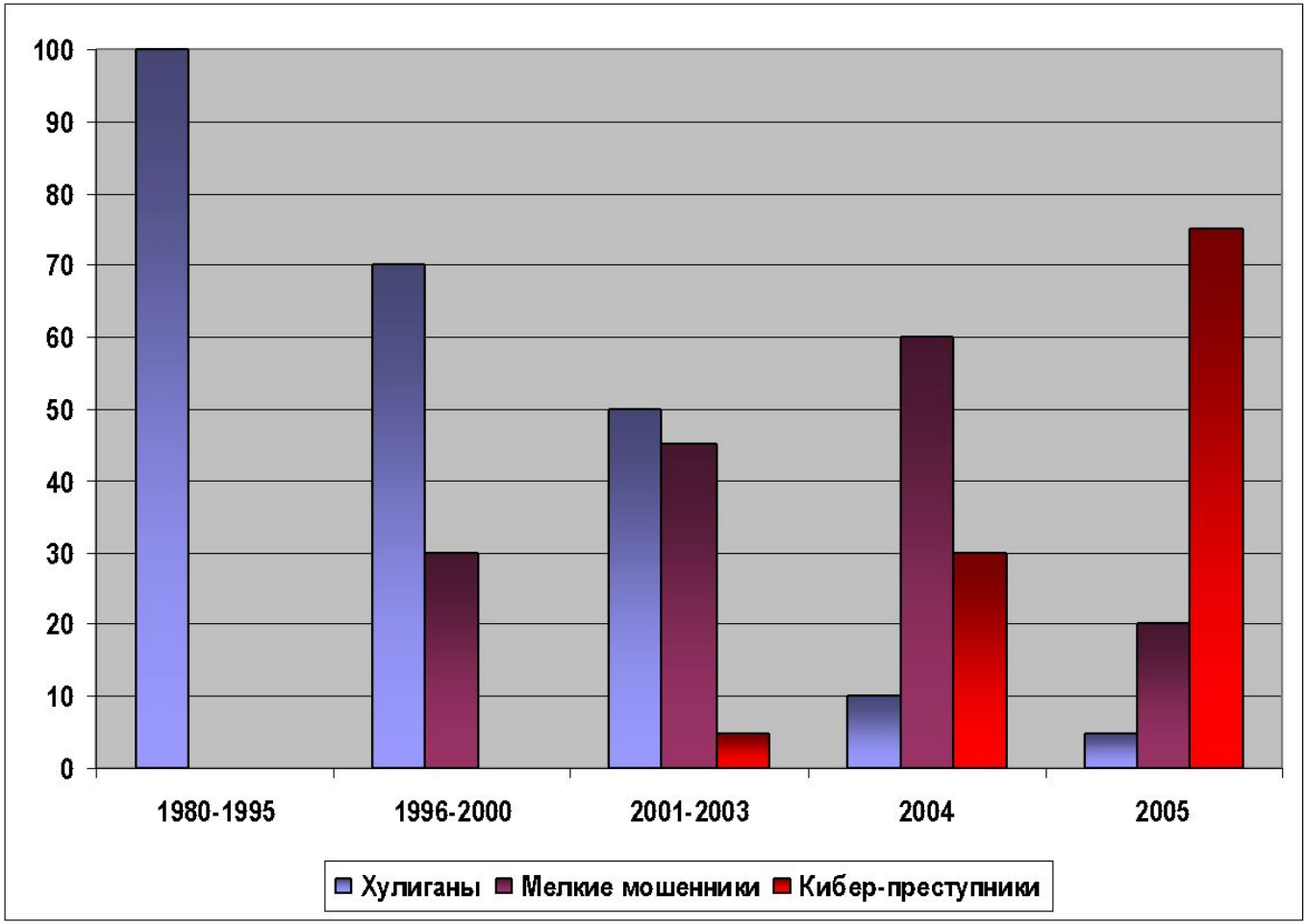
Источник: *Computer Economics, 2005*

Громкие вирусные эпидемии



Источник: *данные «Лаборатории Касперского»*

Сетевая криминализация



Источник: *данные «Лаборатории Касперского»*

Тактика вирусописателей

- Локальные вирусные эпидемии: 1000 x 1000 x 1000…
- Комбинация технологий заражения: E-mail + Web
- Кооперация вирусописателей – структуризация криминала в Интернете
- Конкуренция (войны вирусописателей)
- Противодействие антивирусным компаниям

Противодействие злоумышленникам

Кто виноват?

- Операционные системы и сети небезопасны по своей архитектуре

Что делать?

- Создавать комплексную систему антивирусной защиты (КСАЗ), охватывающую все информационные узлы вашей ИТ-инфраструктуры
  - Рабочие станции и ноутбуки
  - Файловые серверы и серверы внутренних приложений
  - Почтовые серверы
  - Интернет-серверы и серверы «внешних» приложений
  - КПК и смартфоны
- Использовать наиболее передовые и совершенные средства защиты, и своевременно их обновлять

Лаборатория Касперского сегодня

- **380** человек в **12** странах:
  - *Беларусь, Великобритания, Германия, Казахстан, Китай, Нидерланды, Польша, Россия, США, Украина, Франция, Япония*
- Оборот за 2004 г. – **$27 млн.,** прирост – **76%**
  - Россия – **35**%, OEM – **30**%, за рубежом – **35**%
- **Более 200** международных наград

...

- **Сертификаты**


ФСБ

ГТК

West Coast Labs

ICSA

Вопросы?

Спасибо за внимание!