

Реальная опасность вирусных угроз и возможные меры противодействия

21-23 июня 2005

Андрей Зеренков

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

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:

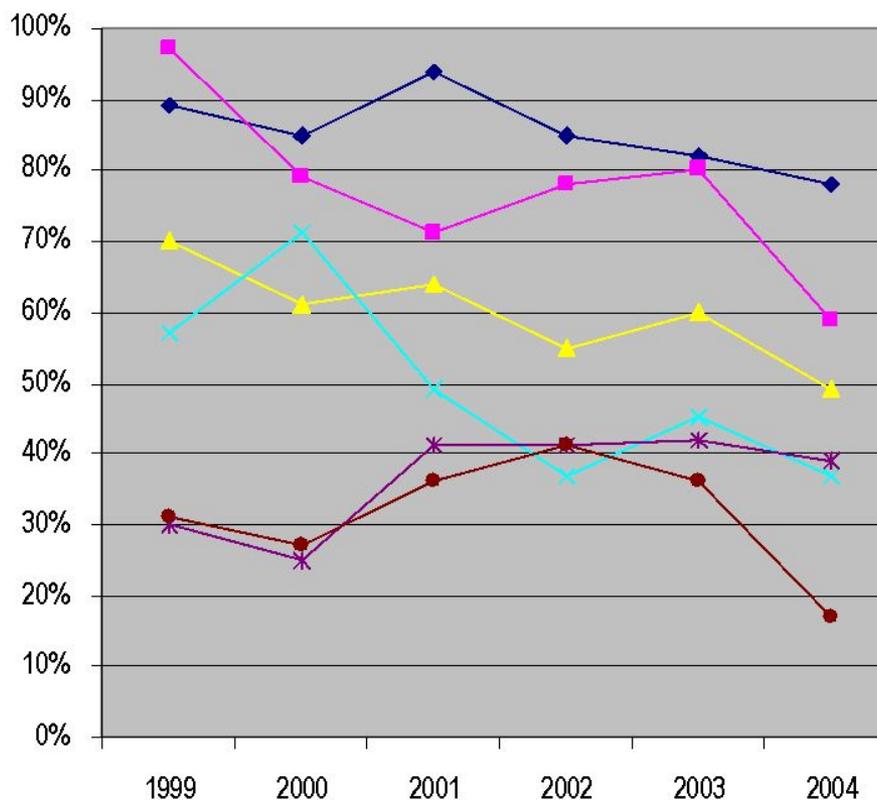
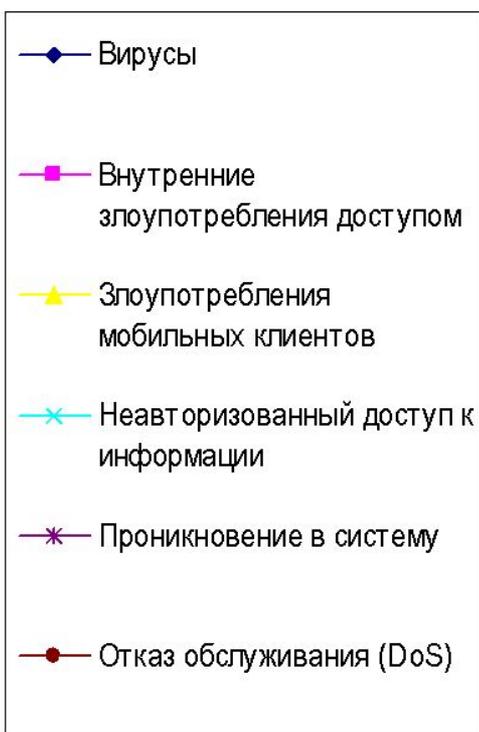
- О том, почему мы всем этим занимаемся, то есть
- Какова текущая ситуация и, следовательно, требования, и
- Какова миссия и цель нашей компании

Нарастание угроз ИТ-безопасности



Источник: [CERT Statistics, 2005](#)

Актуальность различных видов угроз

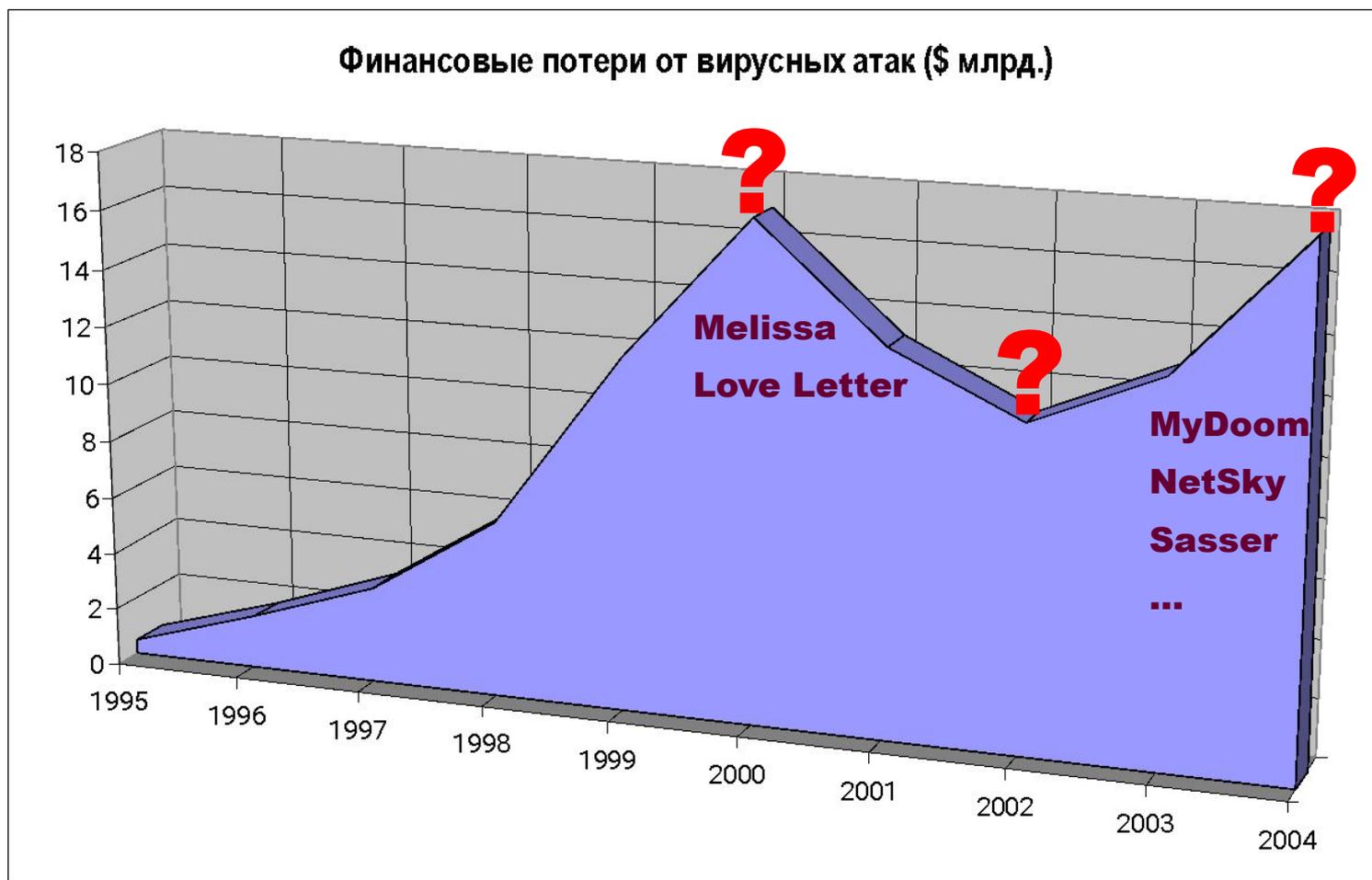


История развития

- ❖ 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



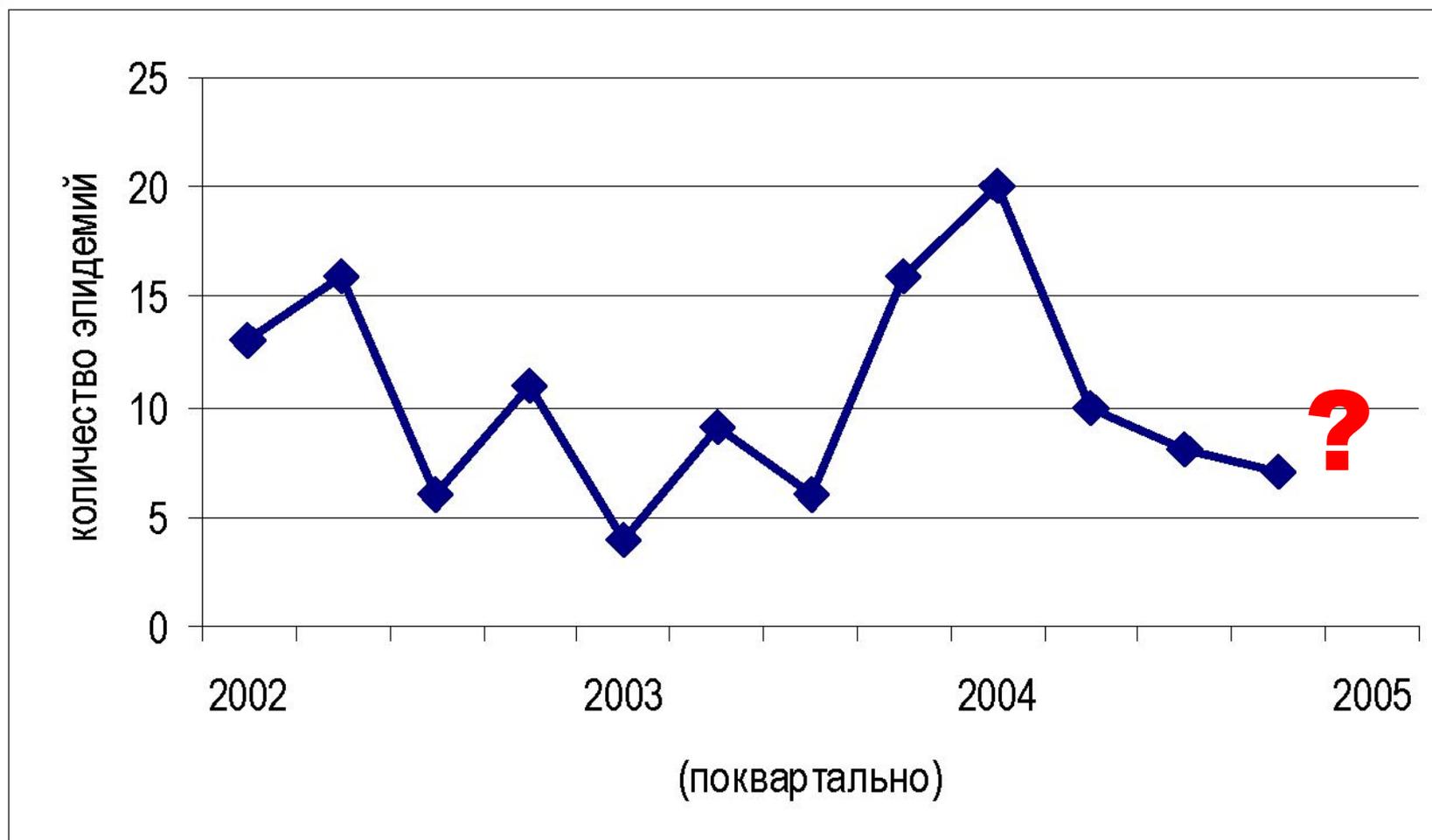
Динамика экономических потерь



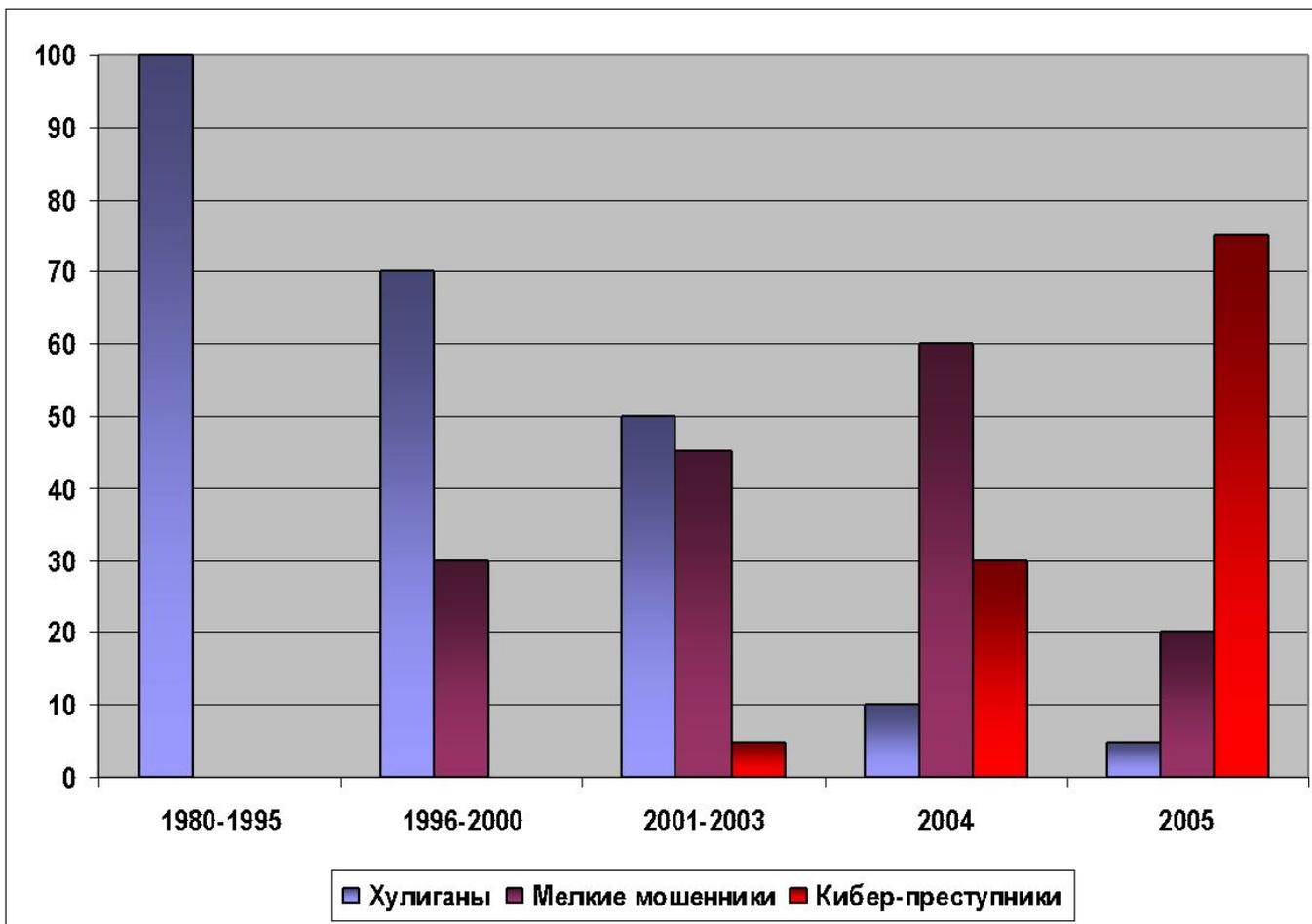
Мрачная реальность'2004

- ❖ 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 мобильных 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 привлекавший Linux-пользователей
 - **Opener** – первый реальный зловаред (скрипт) для Apple Macintosh OS X
- ❖ Ноябрь:
 - **Bofra** – минимальное время от объявления уязвимости до её использования (5 дней)
 - **Sober.I** – наибольший «успех» среди зловаредов второй половины 2004 года
 - **Skulls** – первый троян для мобильных телефонов

Громкие вирусные эпидемии



Сетевая криминализация



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

Kaspersky Lab - antivirus protection - protect your cyberspace - Microsoft Internet Explorer

Address: <http://www.kaspersky.com/cebit2005>

КАСПЕРСКИЙ 14:49:53

LATEST VIRUSES	Detection time (your system time)
28 March 2005	
Virus.Win32.HLLW.Rolog.f	14:48
Trojan-Downloader.Win32.Small.abc	14:47
Backdoor.Win32.VB.acf	14:43
Trojan-Downloader.Win32.Small.aph	14:40
Trojan-PSW.Win32.Delf.ah	14:38
Trojan-Proxy.Win32.Small.bm	14:34
Trojan-Dropper.Win32.Agent.cf	14:34
not-a-virus:Porn-Dialer.Win32.IVADial.a	14:32

Done Internet

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!