Безопасность национальных ИТ-систем. Как это делается?

Бешков Андрей
Руководитель программы информационной безопасности
ООО «Майкрософт Рус»
abeshkov@microsoft.com
блог: http://beshkov.ru

Microsoft в стратегических системах

- Подводный лодки «Вэнгард» Великобритании
- Противоракетные системы Израиля
- Воздушный флот США 500 тысяч машин
- Пентагон США -1,5 миллиона машин
- Применение продуктов Microsoft в стратегических системах более 60 стран

Уязвимости! Каждый месяц!

Уязвимости за 5 лет топ 20 производителей

#	Vendor	History 2006-11	2011 CVEs	Risk	Trend 5yr		1yr	
1	Novell		1,113		+81%	▲	+32%	▲
2	Red Hat		982		+45%	▲	-5%	▼
3	Canonical		625		+48%	▲	+9%	▲
4	Debian		563		+15%	▲	+33%	▲
5	Gentoo		523		+28%	▲	+154%	▲
6	Oracle		497		+27%	▲	+34%	▲
7	Apple		360		+12%	▲	-17%	▼
8	Google		324		+800%	▲	+116%	▲
9	Microsoft		231		+17%	▲	-20%	▼
10	VMware		205		+193%	▲	+63%	▲
11	IBM		192		+21%	▲	-19%	▼
12	Adobe		179		+106%	▲	-16%	▼
13	HP		175		+9%	▲	-34%	▼
14	Cisco		135		+41%	▲	+7%	▲
15	Mozilla		117		+26%	▲	+2%	▲
16	Kernel		81		+8%	▲	-21%	▼
17	Apache		45		+88%	▲	+18%	▲
18	Xerox		43		+330%	▲	+2050%	▲
19	Attachmate		41		+583%	▲	+273%	▲
20	Opera		41		+116%	▲	+28%	▲

Источник Secunia 2011 yearly report

Уязвимости на 5 апреля 2013

Sun Solaris 10	1437
Red Hat Enterprise Linux Server v.5	2119
FreeBSD 6.x	86
Microsoft Windows Server 2008	410
Microsoft Windows Server 2012	87
Apple Mac OS X –	1838
Red Hat Enterprise Linux Client v.5	2349
Ubuntu Linux 8.04 (выпуск 2008 год)	1667
Windows XP (выпуск 2001 год)	599
Windows 7	276
Windows 8	84
Oracle Database 11.x	354
IBM DB2 9.x	121
MySQL 5.x	145
Microsoft SQL Server 2008	4
Microsoft SQL Server 2012	1
Cisco ASA 7.x	89
Microsoft ISA Server 2006	7
Microsoft Forefront TMG	2

В ядре Linux 2.6 — 634 уязвимостей . Столько же сколько в целой Windows XP

источник: **http://secunia.com**

Открытый значит безопасный?

Майкрософт предоставляет исходные коды

- 2002 – Россия стала первой страной в мире с которой Microsoft подписала соглашение Government Security Program о доступе к исходным кодам своих программ (подписано с НТЦ «Атлас» и ФСБ).
  - Соглашение ежегодно продлевается.
  - На территории НТЦ «Атлас» с 2003 организована лаборатория по исследованию исходных кодов продуктов Microsoft – она работает ПОСТОЯННО
- Сейчас в программе GSP участвует более 60 стран

Microsoft SDL

Открытость кода не гарантия безопасности. Методология раннего предупреждения дефектов кода помогает снизить количество и критичность уязвимостей.

Так же применяется в CISCO, Adobe и многих других компаниях.

Сертификация?

Сертифицированные продукты *Microsoft* -1

- **Все продукты *Microsoft* сертифицированы во ФСТЭК «как есть», без изменений, и могут быть использованы для построения автоматизированных систем уровня защищенности 1Г**:
  - **Windows XP Professional** русская версия
  - **Windows Vista** русская версия
  - **Windows Server 2003** и **R2 (Standard и Enterprise)** русские версии
  - **SQL Server 2005 (Standard и Enterprise**) русские версии
  - **Office 2003 и 2007 Standard, Professional, Plus** русские версии
  - **ISA Server 2006 (Standard)** русская версия
  - Антивирусные продукты **Forefront** (**Client**, для **Exchange** и для **SharePoint)** – русские версии
  - **Exchange Server 2007 ****
  - **BizTalk Server 2006 R2 ****
  - **SharePoint Server 2007 ****

  ** получены летом 2009 и на сайте ФСТЭК помечены, как соответствующие Закону о ПД (до 2 класса включительно)

Сертифицированные продукты *Microsoft* - 2

- **Все продукты *Microsoft* сертифицированы «как есть», без изменений, и могут быть использованы для построения автоматизированных систем уровня защищенности 1Г**:
  - **Windows Server 2008 (Standard, Enterprise, Datacenter)** ***
  - **SQL Server 2008 (Standard, Enterprise)** ***
  - **System Center Operation Manager 2007*****
  - **System Center Configuration Manager 2007 R2****
  - **System Center Data Protection Manager 2007*****
  - **System Center Virtual Machine Manager 2008*****
  - **Dynamics CRM 4.0** **
  - **Dynamics AX 2009** **
  - **Dynamics AX 4.0** **
  - **Dynamics NAV 5.0** **
  - **Windows 7 (Профессиональная, Корпоративная, Максимальная)** **
  - **Windows Server 2008 R2 (Standard, Enterprise, Datacenter)** **
  - **BizTalk server 2009** **

*** соответствуют Закону о ПД (до 3 класса включительно)

** соответствуют Закону о ПД (до 2 класса включительно)

Новые сертификаты ФСТЭК - на 1Г и на соответствие ФЗ 152

- **Exchange Server 2010 SP1** – сертифицирован на 1Г и К2
- **System Center Service Manager 2010 SP1** – сертифицирован на 1Г и К2
- **Dynamics CRM 2011** – сертифицирован на 1Г и К2
- **Office 2010 Professional Plus** – сертифицирован на 1Г и К2
- **Forefront Endpoint Protection** – сертифицирован на 1Г и К2
- **SharePoint 2010** – сертифицирован на 1Г и К2
- **Lync 2010** – сертифицирован на 1Г и К2

Работы и планы по сертификации во ФСТЭК

- **Windows 7** – **сертификация на НДВ завершена, идет экспертиза результатов**
- **Windows Server 2008 R2** – **сертификация на НДВ завершена, идет экспертиза результатов**

- **Windows 8 (на Intel и на ARM)**
- **Windows Server 2012**
- **System Center 2012**
- **SQL Server 2012**
- **Office 2013**
- **Exchange 2013**
- **SharePoint 2013**
- **Lync 2013**

Сертификация в ФСБ

- **Сертифицированы:**
  - **Windows XP Professional**
  - **Windows Server 2003 Enterprise**
  - **SharePoint Server 2007**
  - **SQL Server 2008**
  - **Windows 7 – получено положительное заключение**
  - **Windows Server 2008 R2 – получено положительное заключение**
  - **Exchange Server 2010 – получено положительное заключение**

  Каждый сертифицированный продукт включает в себя, кроме продукта Майкрософт, соответствующий продукту «Secure Pack Rus»
- **Работы и планы:**
  - **Windows 8 – сертификация идет**

Отношение к обновлениям

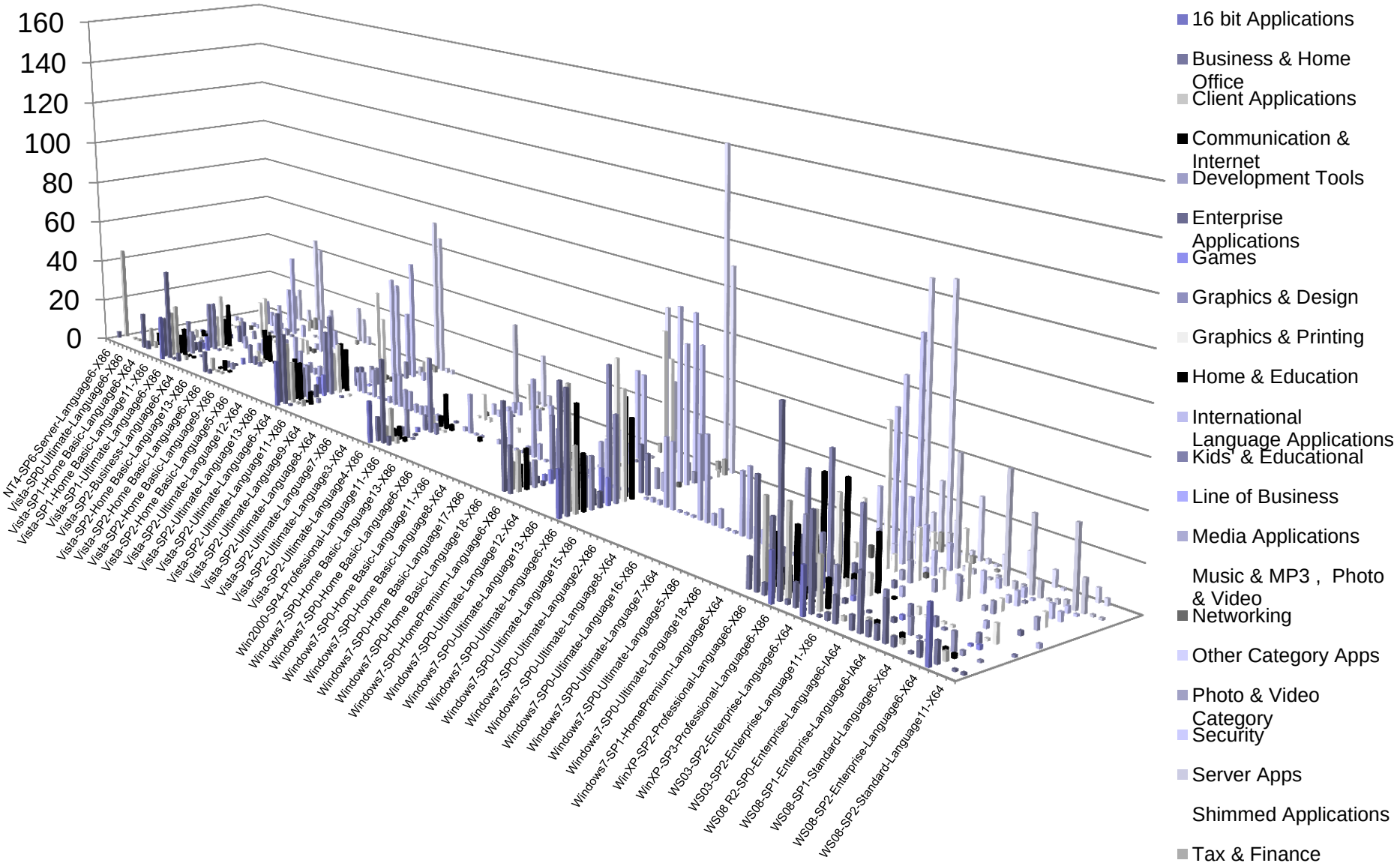
Тестирование на совместимость

- Минимизация проблем с совместимостью приложений требует тестирования огромного количества приложений. Матрица тестирования разрастается очень быстро.
- Обновления безопасности Windows тестируются на:
  - Всех версиях подверженных уязвимости ОС
    - Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2
  - Разных SKU Windows
    - Home Basic, Home Premium, Business, Ultimate, и.тд.
  - Разных сервис паках Windows и уровнях (QFEs)
  - Разных языковых локализациях Windows
  - Разных процессорных архитектурах
    - x86, x64 и Itanium

- И более того тестируются ~3000 распространенных семейств приложений…

Тестирование на совместимость

Группы приложений X версии ОС X SKU



Тестирование на совместимость

- Security Update Validation Program (SUVP) запущена в 2005 году
- Перед выпуском обновления даются группе клиентов под соглашение о неразглашении (NDA)
- Позволяет протестировать на широком наборе сред и конфигураций
- Участники сообщают о найденных проблемах
- Данные об исправляемых уязвимостях и способах эксплуатации не раскрываются

http://blogs.technet.com/b/msrc/archive/2005/03/15/403612.aspx

Что еще делают?

- Система обнаружения атак
  Центры экстренного реагирования
  Анализ инцидентов
- Профилактика потенциальных угроз в национальном киберпространстве (борьба с ботнетами и т.п.).
- Борьба за национальный DNS
- Внедрение национальных систем Deep Packet Inspection

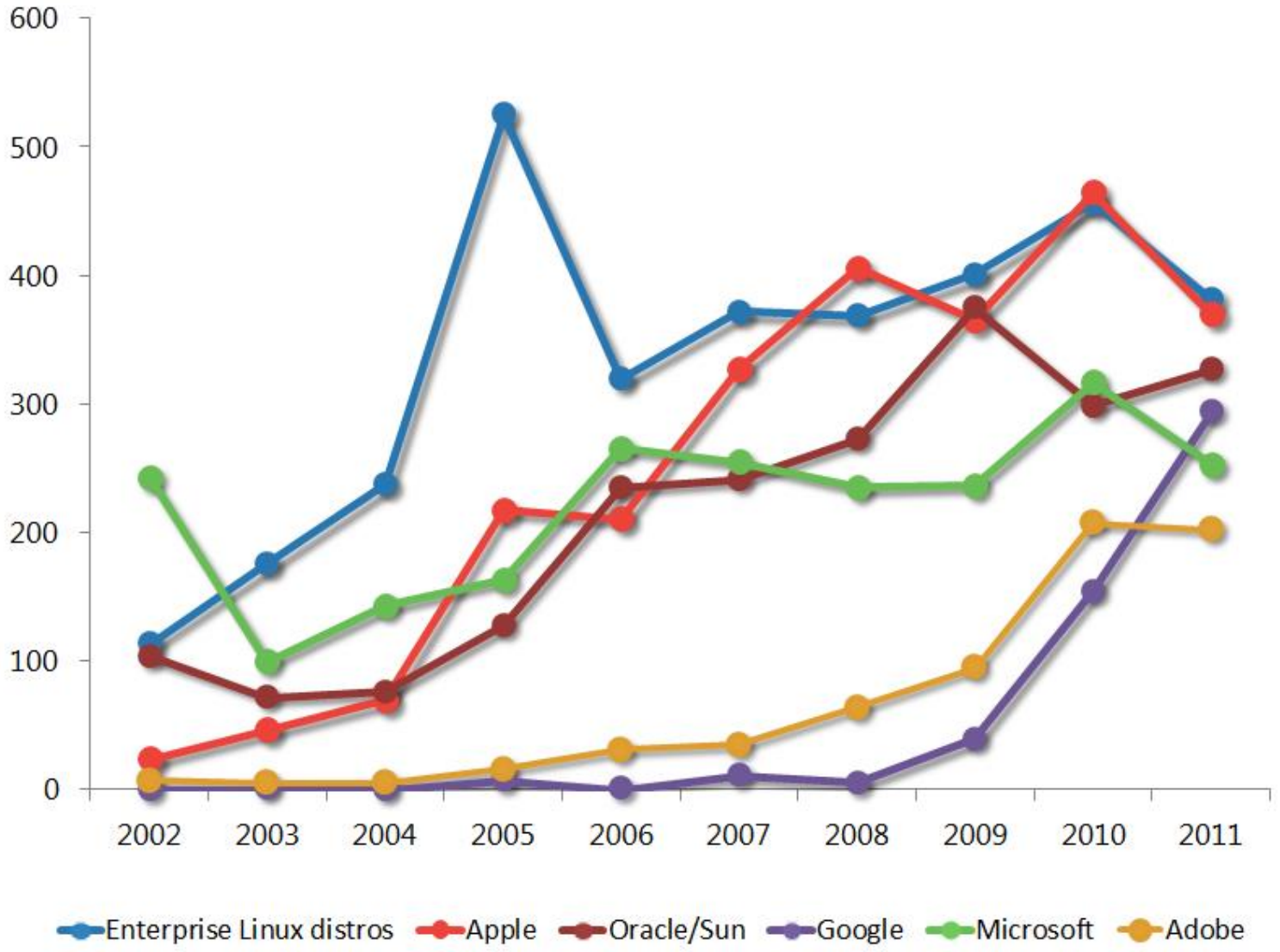
Вопросы?

- **Бешков Андрей**
- **Руководитель программы информационной безопасности**
- **E-mail: abeshkov@microsoft.com**
- **Twitter: @abeshkov**

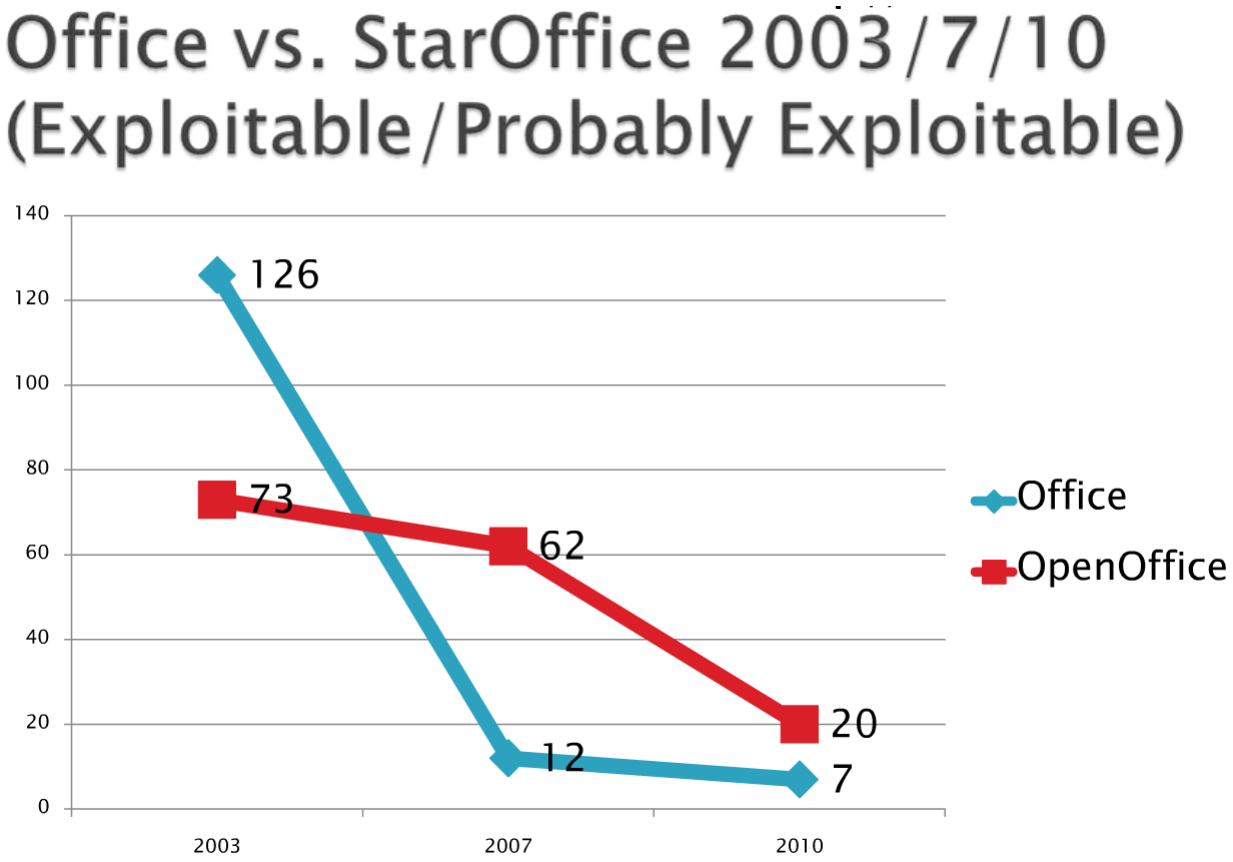
Дополнительные ресурсы

- О сертификации
- Управление уязвимостями в Microsoft
- SDL - разработка безопасного ПО
- Security Intelligence Report
- Microsoft Security Update Guide
- Microsoft Security Response Center
- Microsoft Malware Protection Center
- Trustworthy Computing blogs

Уязвимости за 9 лет



Миф о безопасности ПО с открытым кодом?



http://www.h-online.com/security/news/item/Vulnerabilities-in-Microsoft-Office-and-OpenOffice-compared-1230956.html