Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения

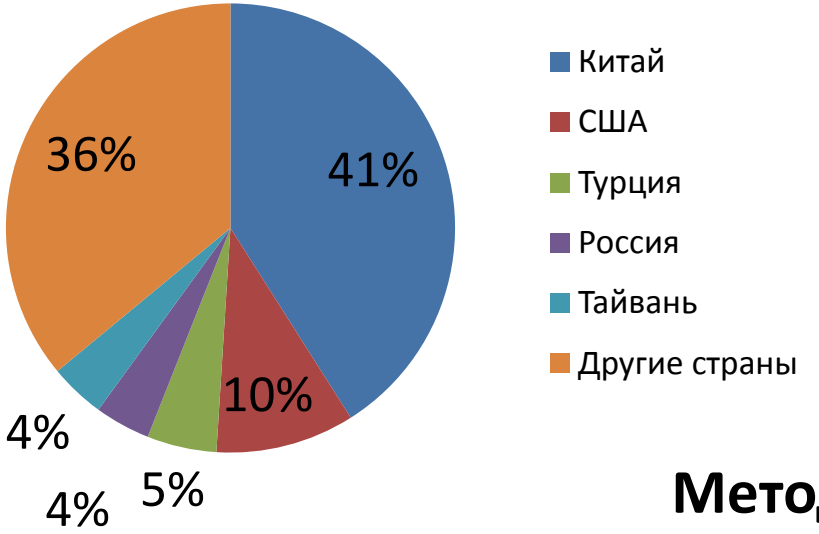
Федорченко А.В.
«Опытное конструкторское бюро «КАРАТ»

Чечулин А.А., Котенко И.В.
Лаборатория проблем компьютерной безопасности
Санкт-Петербургского Института Информатики и Автоматизации РАН

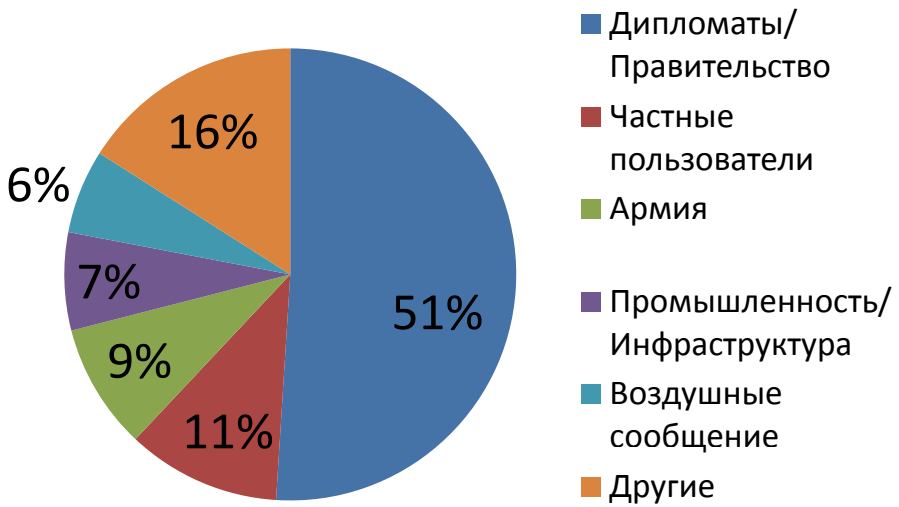
Санкт-Петербург, Россия

РусКрипто`14
25 — 28 марта 2014 г.

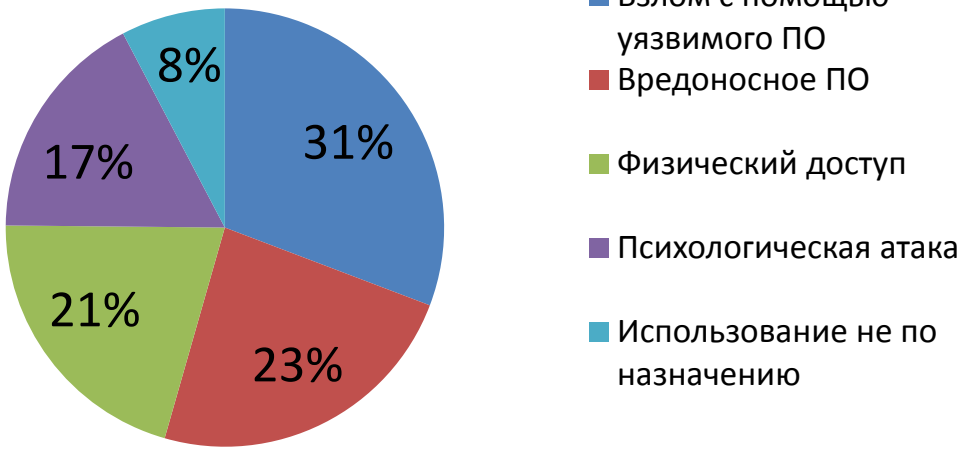
Мировые лидеры киберпреступности



Цели кибершпионажа



Методы кибератак



Базы данных уязвимостей

Common Vulnerabilities & Exposures
(Общие уязвимости и воздействия)

National Vulnerabilities Database
(Национальная база данных уязвимостей США)

Open Source Vulnerabilities Data Base
(Открытая база данных уязвимостей)

Vulnerability Notes Database
(База данных записей уязвимостей)

BugTraq
(Поддерживается открытым сообществом)

Secunia
(Коммерческая база данных уязвимостей)

Задачи

1. Анализ структур открытых баз уязвимостей
2. Анализ обнаруженных уязвимостей программно-аппаратного обеспечения крупнейших мировых производителей
3. Прогноз обнаружения уязвимостей наиболее используемых продуктов в будущем

Сравнительный анализ баз уязвимостей CVE, NVD и OSVDB

База данных уязвимостей	Ссылки на сторонние базы данных уязвимостей	Ссылки на уязвимое программно-аппаратное обеспечение	Унифицированный формат записей программно-аппаратного обеспечение	Зависимости программно-аппаратного обеспечения	Показатели, характери-зующие уязвимости	Прямая загрузка
CVE	+	-	-	-	-	+
NVD	±	+	+	+	+	+
OSVDB	+	+	-	-	-	-

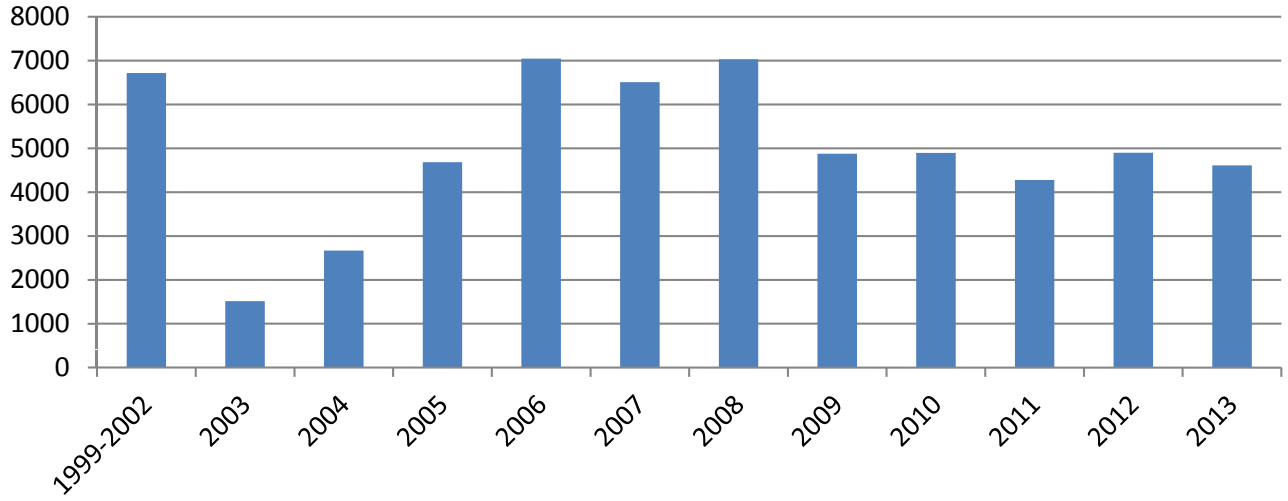
\+ наличие
± условное наличие
\- отсутствие

cve.mitre.org

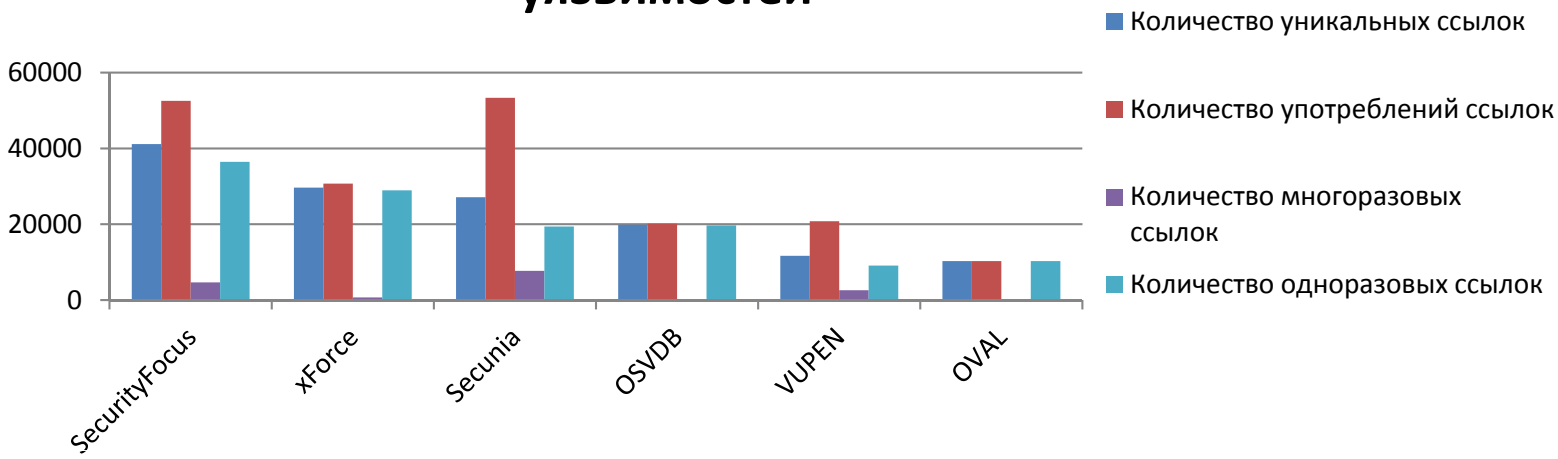
National Vulnerability Database nvd.nist.gov

Базы данных уязвимостей CVE и NVD

Распределение уязвимостей по годам



Ссылки на сторонние источники описания уязвимостей



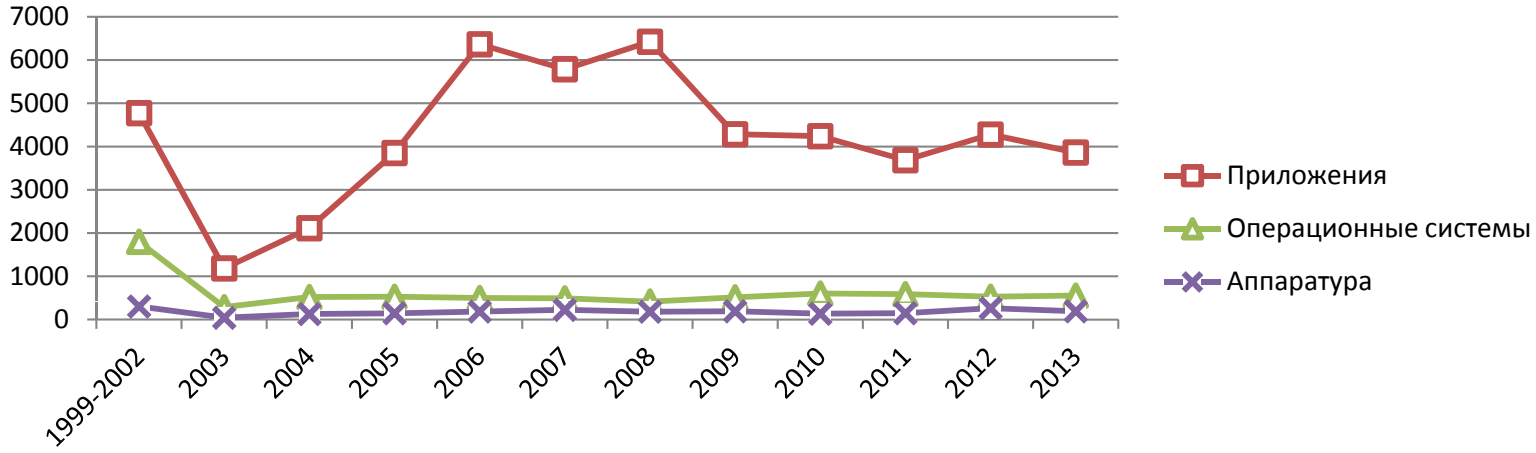
Анализ баз уязвимостей (3/4)

cve.mitre.org

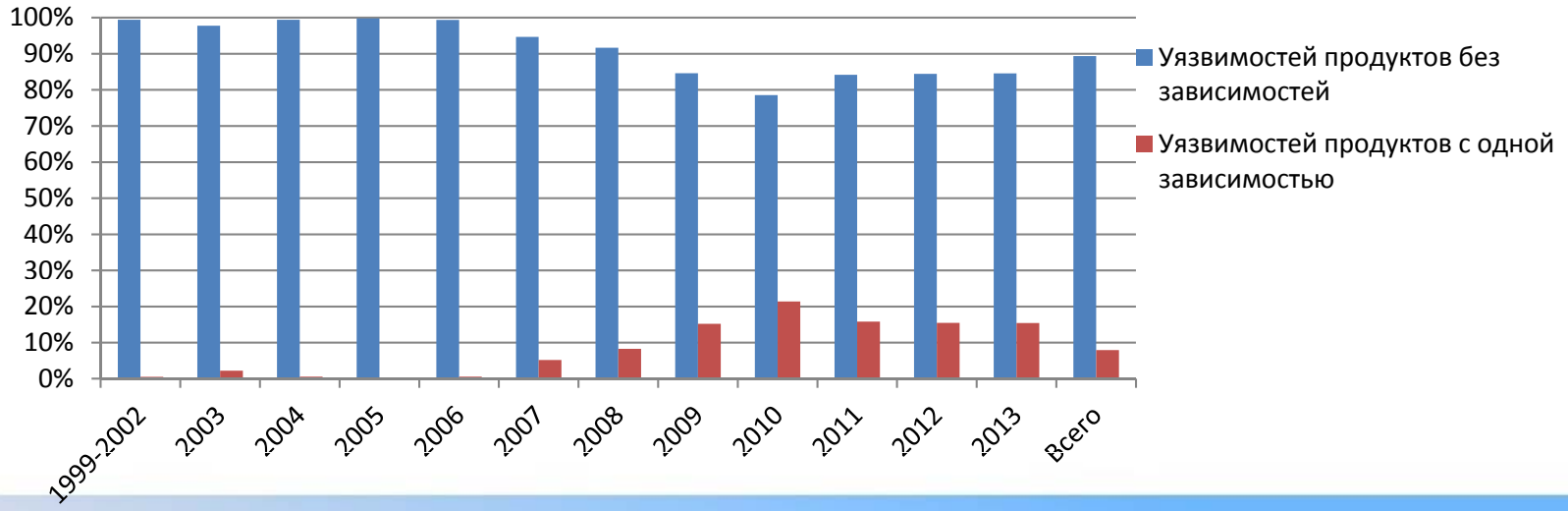
National Vulnerability Database nvd.nist.gov

Базы данных уязвимостей CVE и NVD

Распределение уязвимостей в типизированных продуктах

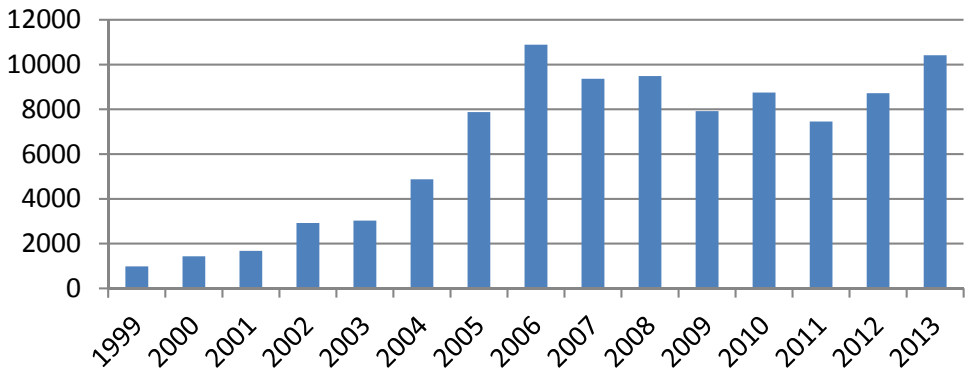


Статистика уязвимостей с зависимостями

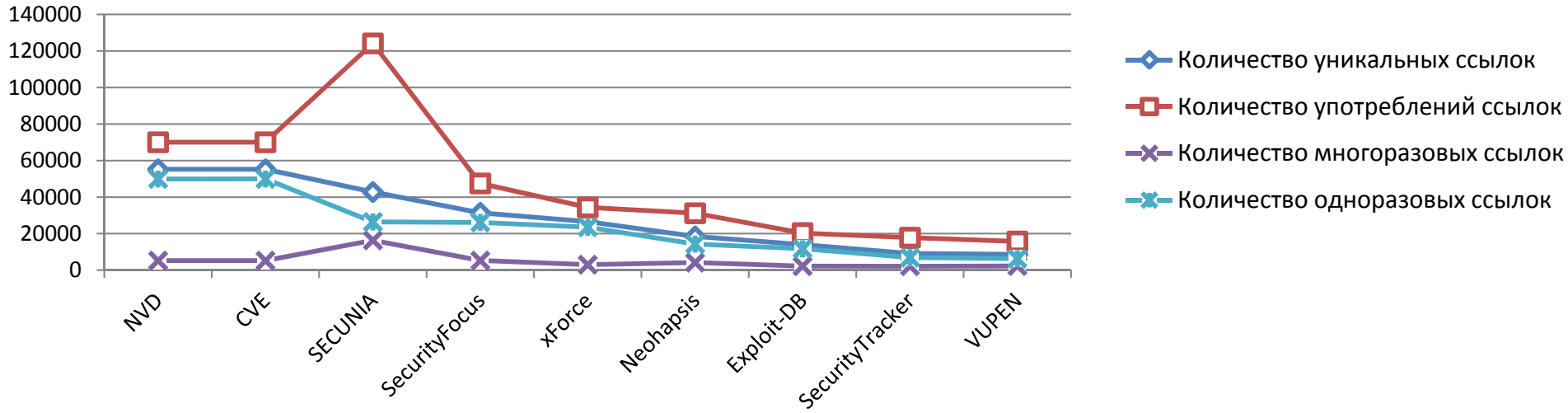


Открытая база данных уязвимостей OSVDB

Распределение уязвимостей по годам



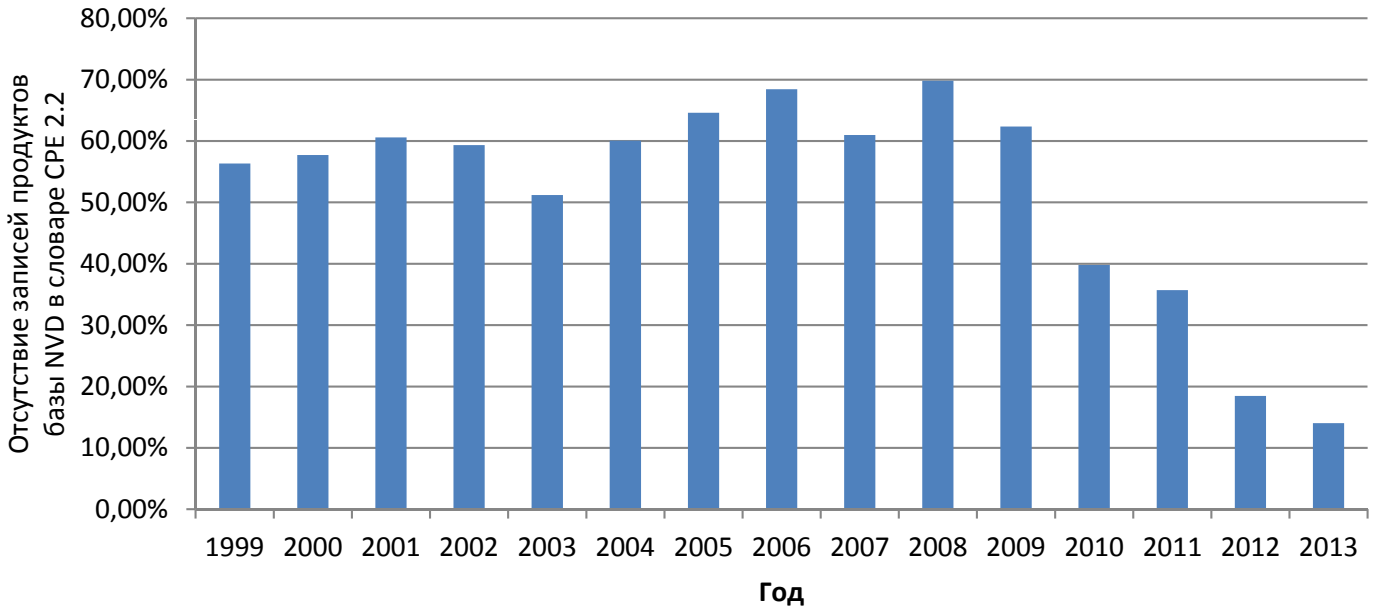
Ссылки на сторонние источники описания уязвимостей



Словарь продуктов

Common platform enumeration
(Общее перечисление платформ)

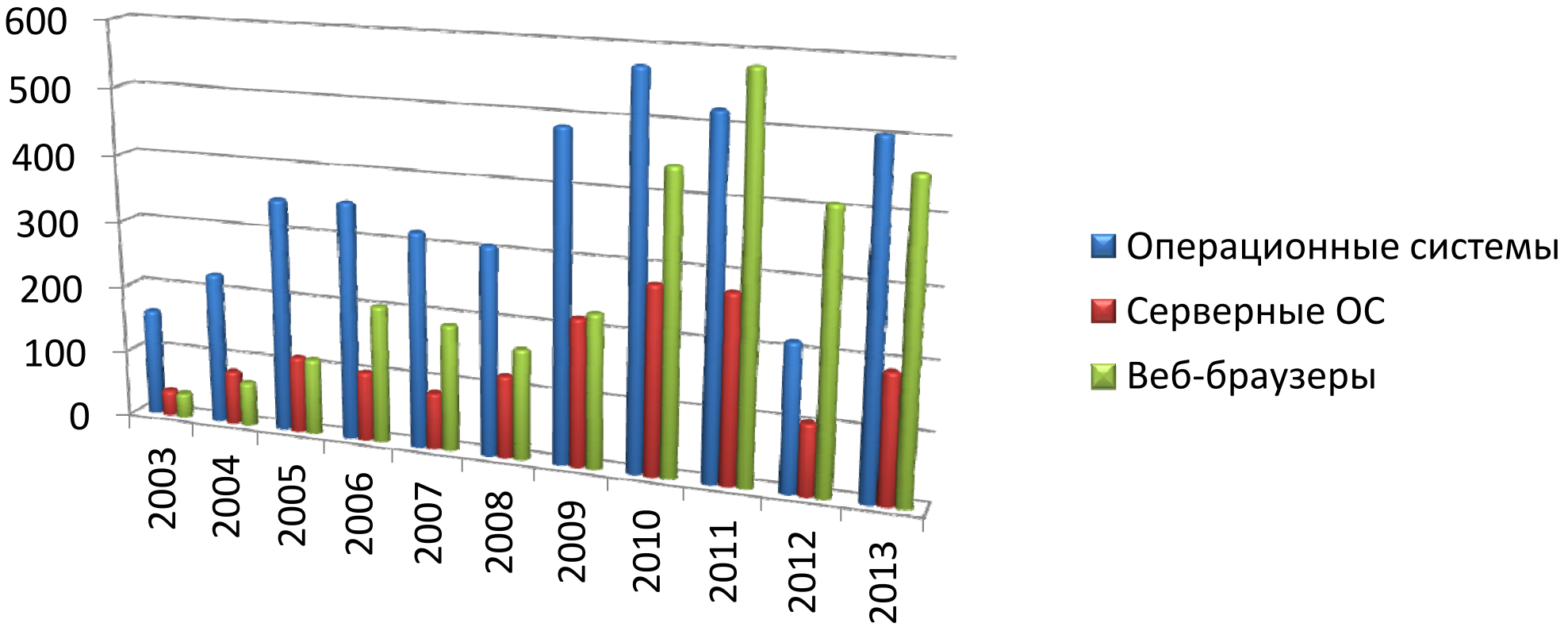
Использование словаря CPE базой NVD



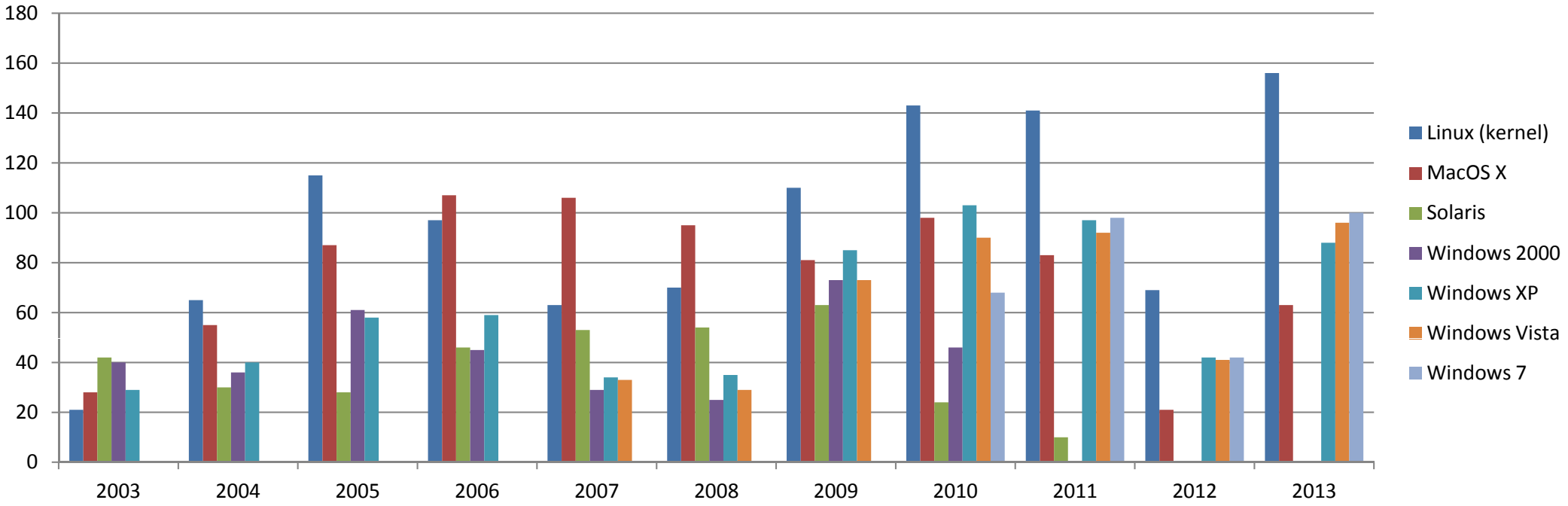
Всего записей – 82987
Продуктов – 10593
Производителей – 2614

Виды продуктов

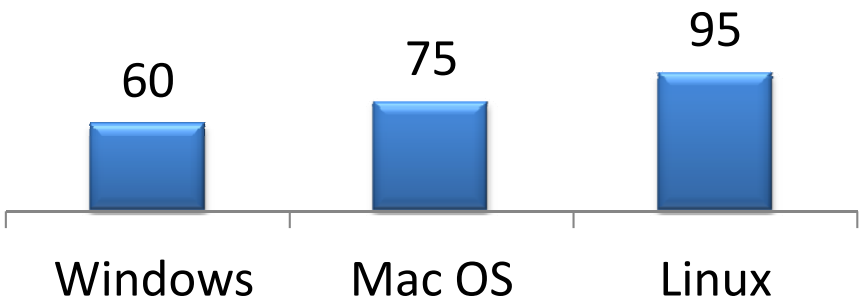
Распределение уязвимостей однотипных продуктов



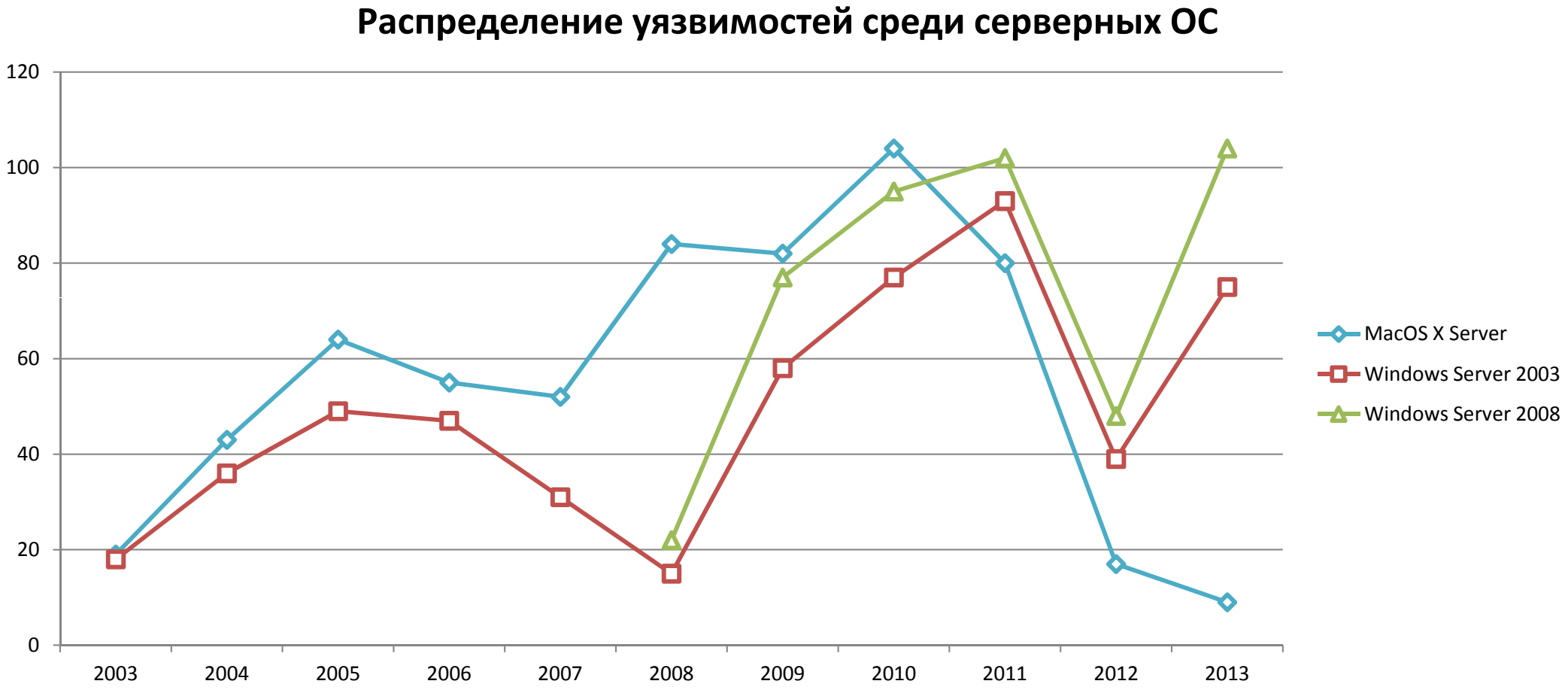
Распределение уязвимостей среди операционных систем



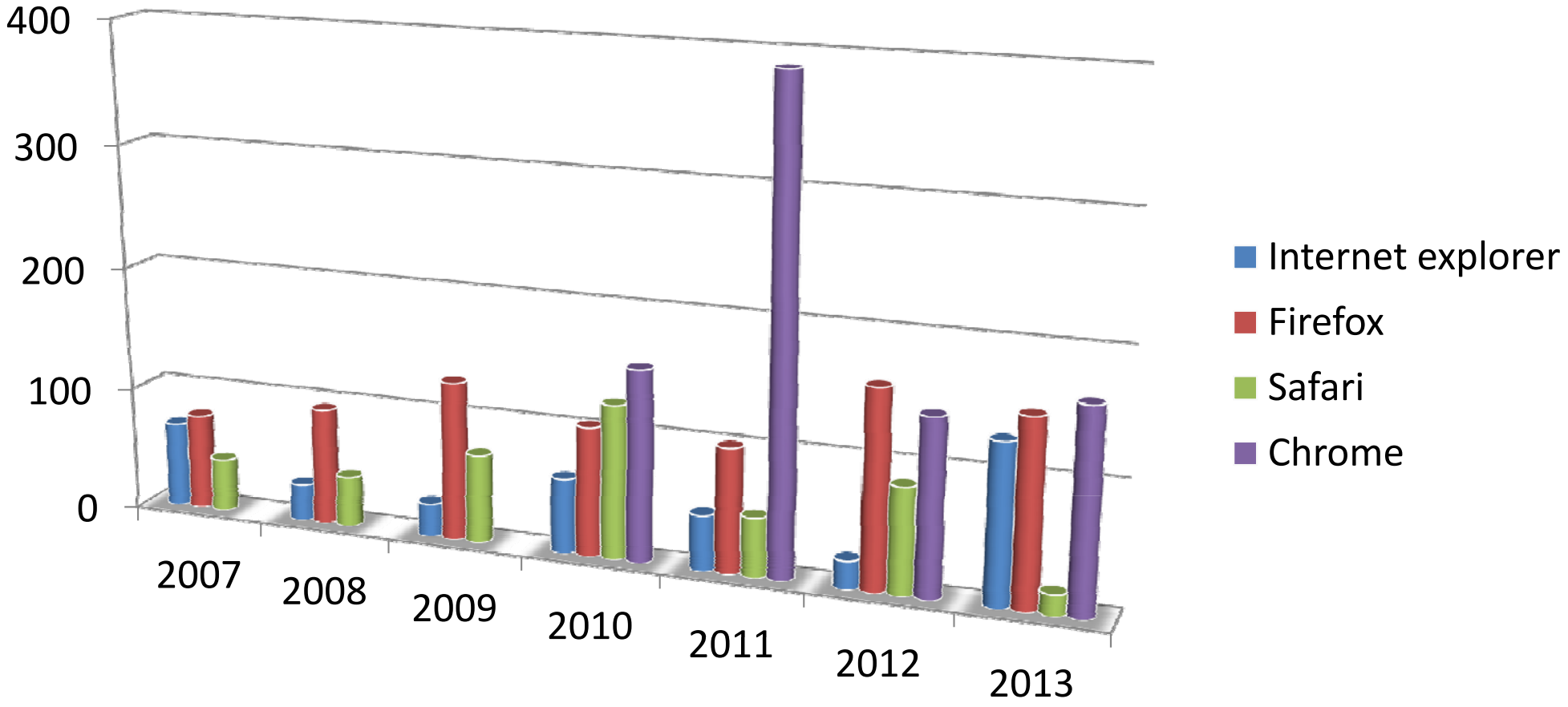
Среднее количество уязвимостей в год



Серверные ОС

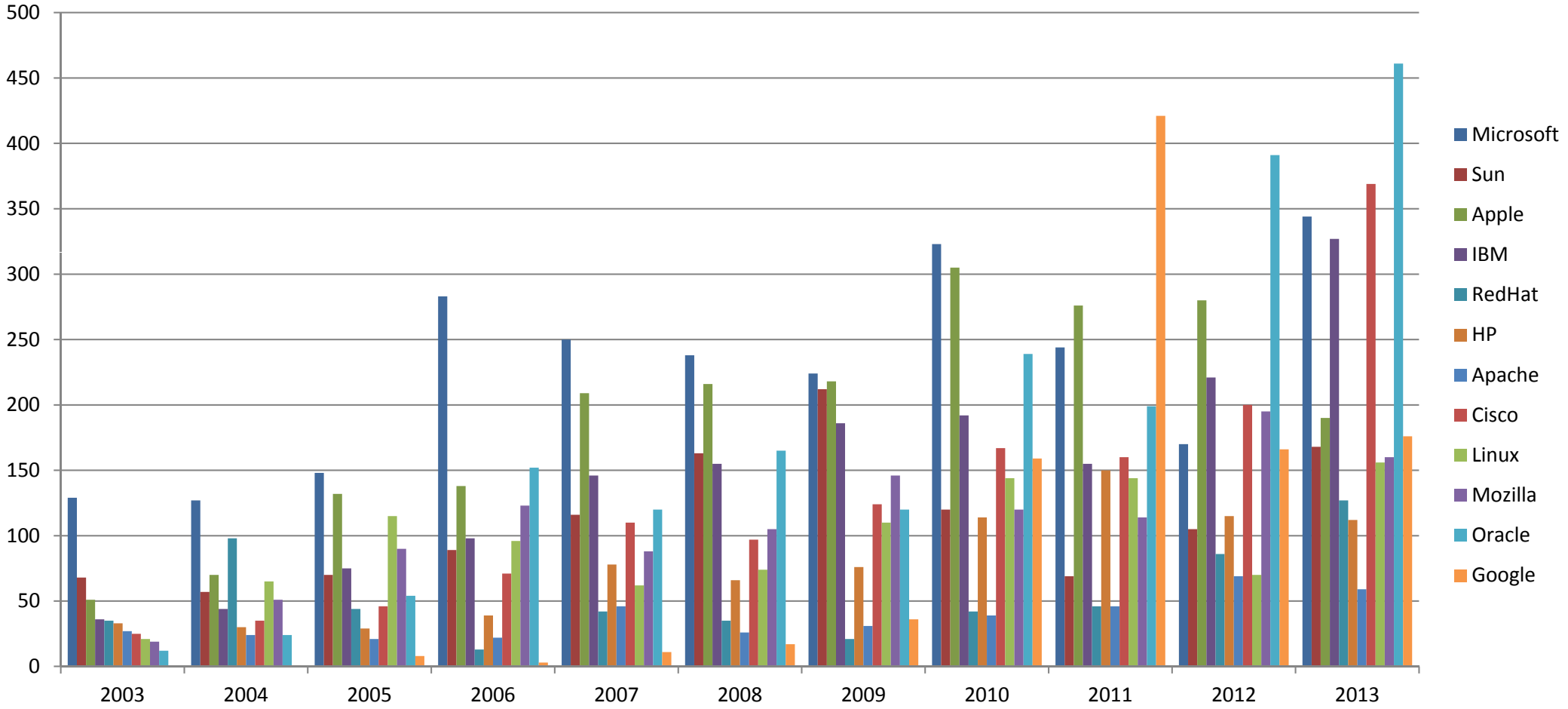


Распределение уязвимостей среди веб-браузеров



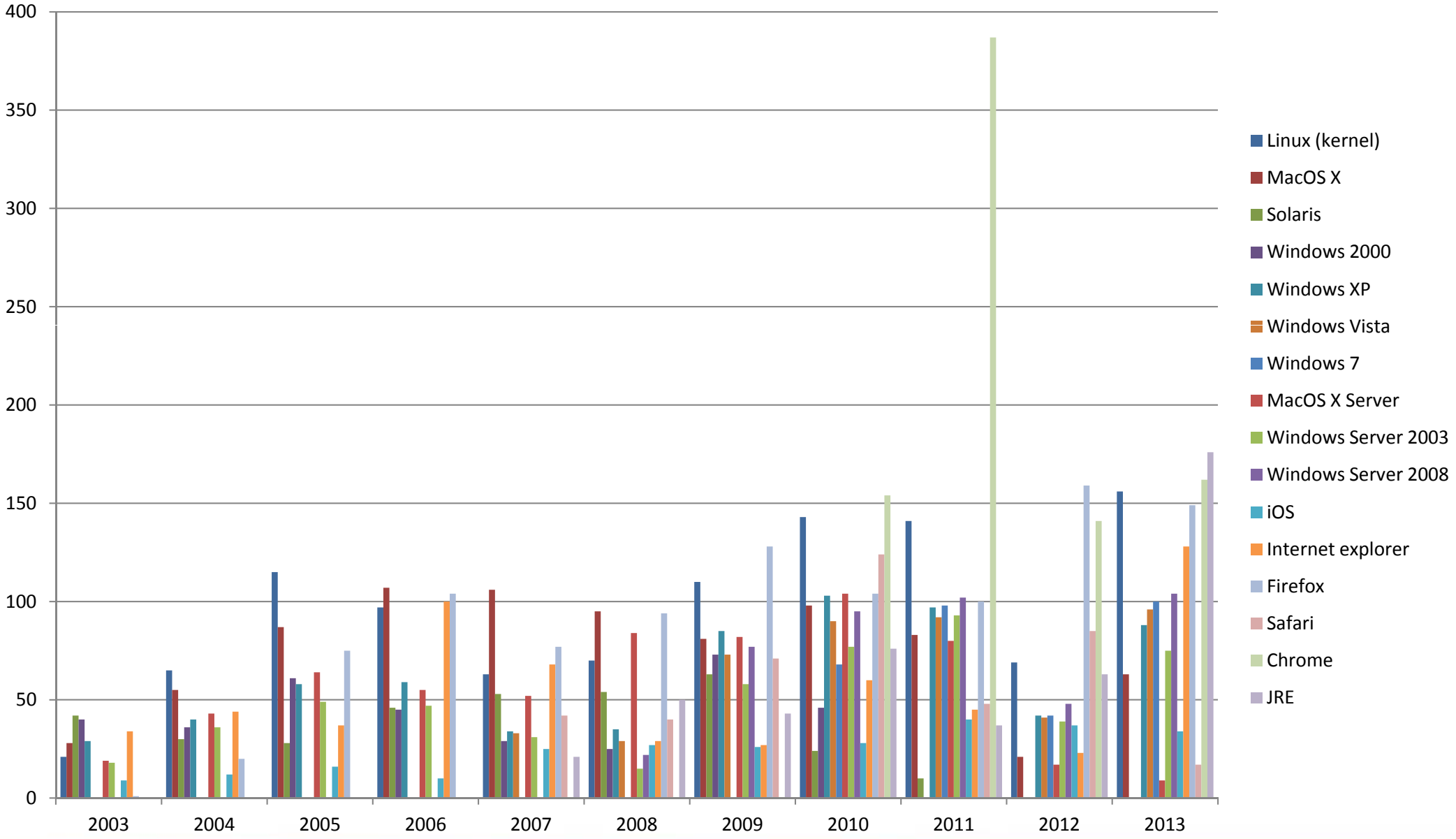
Производители

Распределение уязвимостей крупнейших производителей программно-аппаратного обеспечения



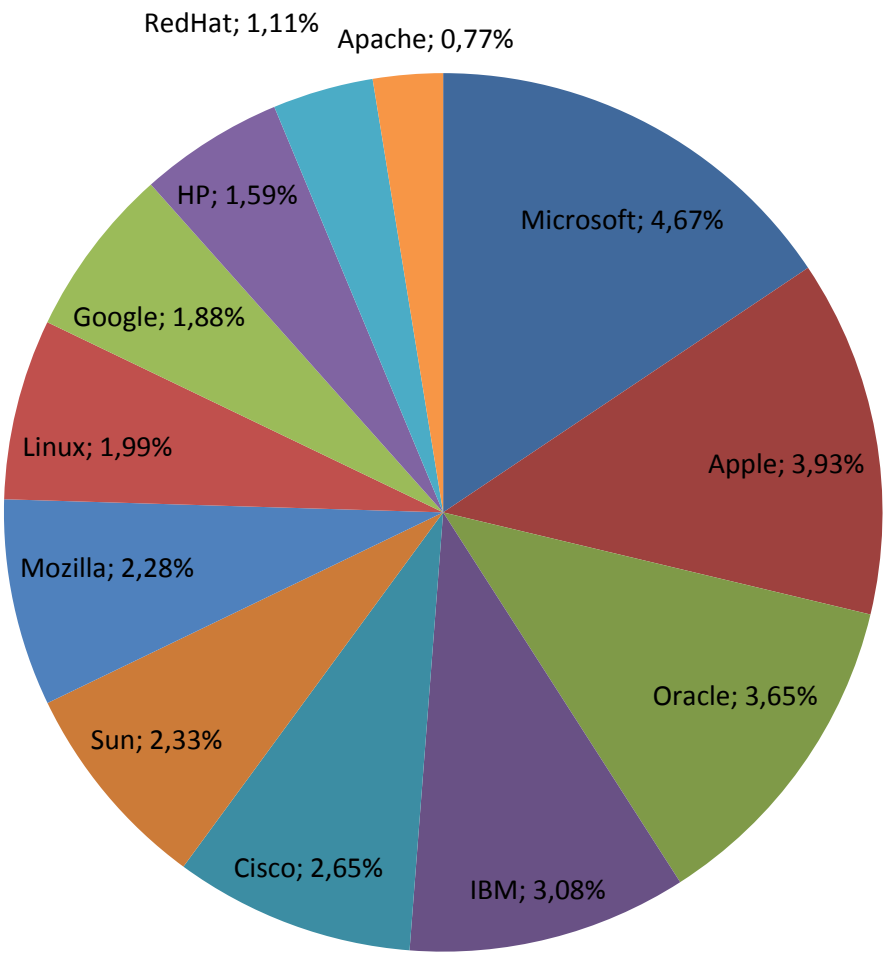
Популярные продукты

Распределение уязвимостей среди наиболее популярных продуктов

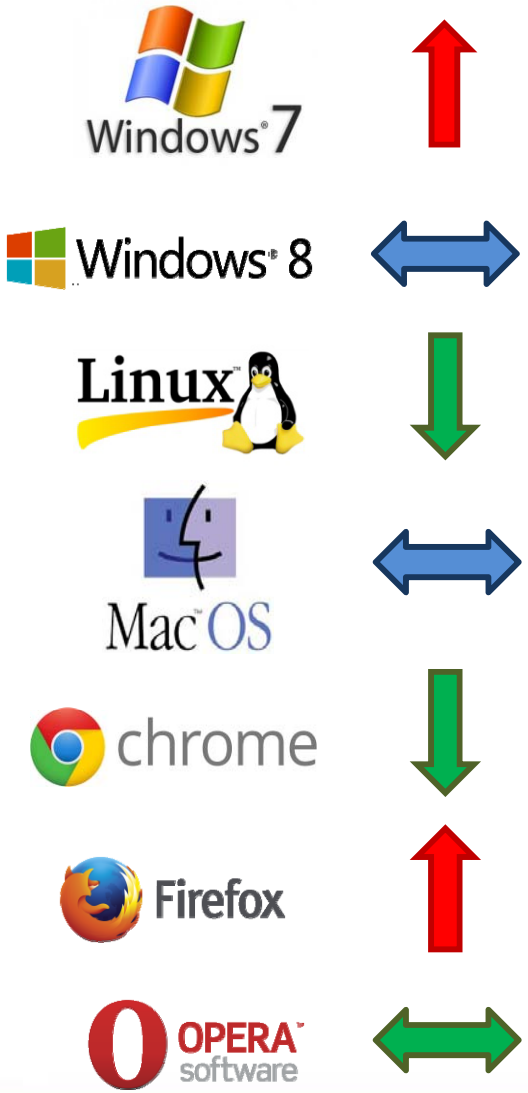


Заключение

Производители-лидеры по числу обнаруженных уязвимостей разрабатываемого программно-аппаратного обеспечения в период 2003-2013гг.



Прогноз количества обнаруживаемых уязвимостей в продуктах в 2014 году



СПАСИБО ЗА ВНИМАНИЕ!

Федорченко Андрей Владимирович
fedorchenkoandrei28@rambler.ru

Чечулин Андрей Алексеевич
chechulin@comsec.spb.ru
http://comsec.spb.ru/chechulin

Котенко Игорь Витальевич
ivkote@comsec.spb.ru
http://comsec.spb.ru/kotenko