



**Появление и эволюция
вредоносных программ.**

Основные направления развития.

Методы противодействия.



Введение

По данным **Computer Economics** в **2000** году ущерб мировой экономике от действий вирусов составил огромную сумму — около **17,5 млрд долларов**. Большинство бизнес-компаний тогда пострадало от целой серии скриптовых вирусов и печально знаменитых «любовных» писем (LoveLetter). Чтобы не допустить подобного в будущем, многие представители бизнеса увеличили свои ИТ-бюджеты, в частности ту часть, которая приходилась на информационную безопасность. Это принесло существенные плоды — ущерб снизился до **13,2 млрд долларов**.

В **2001** году весь мир был потрясен ужасным террористическим актом в США, многие компании снова вложили свои средства в информационную безопасность и, как результат, ущерб снизился еще до **11,1 млрд долларов** — это ниже чем в 1999 году.

Как часто бывает, у пользователей возникло ложное ощущение безопасности. Многие представители бизнеса, будучи полностью удовлетворенными эффективностью своих вложений в последние два года, урезали бюджеты на ИТ-безопасность. В результате ущерб от вирусов за **2003** год составил порядка **13 млрд долларов**, что значительно больше, чем в 2001-2002 годах.



Кто и почему создает вредоносные программы?

- студенты и школьники – которые только что изучили язык программирования, хотят попробовать свои силы, но не смогли найти для себя какое-либо применение
- молодые люди (чаще – студенты) которые еще не полностью овладели искусством программирования, но с большим желанием похулиганить
- профессиональные виросописатели
- «исследователи»

- *Ради шутки*
- *Мелкое воровство*
- *Криминальный бизнес*



История возникновения

Доподлинно **известно**: на машине Чарльза Бэббиджа, считающегося изобретателем **1-го** компьютера, **ВИРУСОВ не было**.

Появление глобальных сетей стало началом для

Отправной точкой можно считать труды Джона фон Неймана по изучению разделения вредоносных программ самовоспроизводящихся математических автоматов.

13 ноября 1987г. – первая в истории крупная вирусная эпидемия. Вирус **Jerusalem** поразил компании, правительственные и научные учреждения по всему миру.

Во времена эпидемии **Jerusalem** компьютеры связывались между собой в основном посредством локальных сетей, а файлы переносились между компьютерами при помощи дискет. Чтобы достигнуть большой распространенности вирусам требовалось внушительное время.

Основные классы вредоносных программ по их функционалам:

- ✓ **способные к саморазмножению** – способны выполнять различные функции. Наиболее известной стала та, которая удаляет с компьютера все запускаемые в пятницу, 13-го числа, программы. Поскольку совпадение пятницы с 13-м числом месяца случается не так уж часто, то большинство времени **Jerusalem** распространялся незаметно, без какого-либо вмешательства в действия пользователя.
- ✓ **не способные к саморазмножению**
- ✓ **прочие**

Вредоносные программы способные к саморазмножению



Классические компьютерные вирусы. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера.

Вирусы не используют сетевых сервисов для проникновения на другие компьютеры.

Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.



Сетевые черви. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: *электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.*

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: **социальный инжиниринг** (например, текст электронного письма, призывающий открыть вложенный файл), **недочеты в конфигурации сети** (например, копирование на диск, открытый на полный доступ), **ошибки в службах безопасности операционных систем и приложений.**

Основные признаки сетевых червей

Вредоносные программы Неспособные к саморазмножению

Прочее вредоносное программное обеспечение

Программы скрыто предоставляющие доступ к компьютеру

Вымогательство в среде Internet

Основные способы заражения

Чем опасна социальная инженерия

Перспективы развития вредоносных программ

Методы борьбы со зловредами

О чем следует помнить при выборе защиты

