Мнение специалистов

Слухи о гибели Интернета

21 октября 2002 года 13 корневых серверов Интернета были атакованы неизвестными злоумышленниками. Спустя всего 3 месяца, в ночь с 24 на 25 января 2003 года, целые сегменты Сети перестали функционировать в результате эпидемии червя Helkern. И наконец, по одной из первых версий, гибель шатла «Колумбия» 1 февраля 2003 года могла быть связана с проводившимся на борту космического челнока экспериментом по установке интернет-соединения с Землей.

Хотя эксперты почти на 100% исключают связь аварии «Колумбии» с Интернетом, возникновение подобной гипотезы весьма симптоматично. Сегодня Интернет все чаще воспринимается многими специалистами как источник угрозы — вполне осязаемой и реальной.

А оценки дальнейшего развития ситуации, особенно после недавних вирусных эпидемий, серьезно нарушивших работоспособность Сети, колеблются от сдержанного оптимизма до весьма пессимистических прогнозов.

Поскольку данная тема вызывает большой интерес у наших читателей, мы провели опрос среди известных деятелей российского Интернета, задав им несколько вопросов, касающихся сетевой безопасности и перспектив развития Глобальной сети. Нашими собеседниками стали Максим Мошков, Евгений Касперский, Иван Пашкевич, Денис Калинин и Иван Засурский. »

преувеличены

Мы имеем дело с анархией

Chip: Какова, на ваш взгляд, ситуация с глобальной сетевой безопасностью и как она может измениться в среднесрочной перспективе?

Евгений Касперский: То, что сейчас происходит в Интернете, вообще с трудом можно назвать безопасностью. Сегодня мы имеем дело с анархией и полной безнаказанностью: анонимно получить доступ в Сеть и совершить киберпреступление — задача тривиальная даже для школьника. А все меры безопасности, предпринимаемые пользователями, — это исправление последствий, а не причины. Если посмотреть на Интернет как на живой организм, который проходит определенные стадии развития от рождения до смерти, то сейчас Всемирная сеть уже находится на этапе больничной койки. В мире сотни миллионов пользователей и полное отсутствие системы раннего предупреждения и предотвращения вредоносных действий. Как следствие — несколько глобальных эпидемий и десятки тысяч успешных хакерских атак каждый месяц, причем наблюдается явно выраженная тенденция к увеличению их объема. Так что даже краткосрочная перспектива видится мне далеко не в розовых тонах: количество бесполезной и откровенно опасной информации превзойдет объем полезной, и Интернет постепенно превратится в место, где приличному человеку будет стыдно появиться.

Максим Мошков: Ситуация средней тяжести. То есть заметная часть локальных сетей (больше половины) вполне терпимо прикрыта. Перспектива довольно прозрачна: конторы и фирмы, подключенные к Интернету, будут в среднем повышать свою защищенность от сетевых атак (нарастание опыта, софт с меньшим количеством ошибок, разумный расчет на то, что безопасность стоит своих денег), а с другой стороны — будет расти количество обычных домашних пользователей и домовых сетей, в которых преобладают «чайники» и кривые руки. Так что — где-то как-то так. С одной стороны — улучшится, с другой — ухудшится. Неприятность заключается в том, что «дырявые» локалки — идеальная среда для обитания хакеров, которые получают возможность задействовать ресурсы взломанных сетей для своих действий и затрудняют отслеживание источника атак.

Иван Пашкевич: В сегодняшнем положении взрывного развития Интернета ситуация с сетевой безопасностью крайне неровная, и ее невозможно оценить одним показателем, поскольку он будет напоминать «среднюю температуру по больнице», если принимать во внимание степень развития разных предприятий, отраслей, го-

Кто есть кто

Евгений Касперский — руководитель антивирусных исследований «Лаборатории Касперского»

Иван Пашкевич — менеджер по продаже решений корпорации Microsoft

Иван Засурский — заместитель генерального директора ОАО «Рамблер Интернет Холдинг»

Максим Мошков — создатель самой популярной библиотеки Рунета Lib.ru, программист-разработчик газеты Lenta.ru

Денис Калинин — генеральный директор «Rambler Телеком»

» сударств. Одни компании уделяют этой проблеме достаточное внимание, другие, и их большинство, еще не осознали степень своей ответственности при увеличении степени использования IT и подключении к Интернету. Между тем в век информационного общества, когда стоимость информации возрастает многократно, а стоимость ее передачи, наоборот, стремится к нулю, безопасность данных приобретает особенное значение. Безопасность информации всегда обеспечивается комплексом организационных и технических мер, и по мере развития информационных технологий роль технических мер возрастает быстрее, хотя, на мой взгляд, она остается еще сравнительно небольшой. Если компания, государство или конкретный человек видят в участии в информационном обмене выгоду и хотят ее извлекать, для них роль защиты информации будет возрастать и далее. Будут повышаться риски за использование IT и прозрачность бизнес-процессов, но будет повышаться и рисковая премия; сейчас мы видим, что премия за риск растет быстрее.

Атаки были, есть и будут

Chip: Как вы считаете, какова вероятность повторения массированных атак на инфраструктуру Интернета в ближайшем будущем?

М. М.: Атаки были, есть и будут. Это вопрос статистический. Некоторое количество желающих атаковать всегда найдут некоторое количество серверов, поддающихся атакам.

Е. К.: Действительно, это становится обычным явлением. В дальнейшем все будет происходить по накатанной схеме: изобретается способ атаки, реализуется, после чего внедряется адекватная защита. А через некоторое время все повторяется заново.

И. П.: До тех пор, пока это кому-нибудь нужно, попытки атак на любые серверы будут продолжаться. Их можно минимизировать только в том случае, если государства и их правовые органы договорятся о принципах и механизмах отслеживания этих атак. Но это сделать очень сложно из-за разных правовых баз в разных государствах и значительной вероятности того, что всегда найдутся страны, которые не поддержат эту инициативу.

Chip: Атаки на корневые серверы Интернета, очевидно, требуют серьезной подготовки. Какие материальные, финансовые и организационные ресурсы могут понадобиться для таких атак? Кому это может быть выгодно?

Е. К.: Все, естественно, зависит от квалификации атакующего. Для настоящего профессионала достаточно будет хорошо подумать, написать и отладить сетевого червя. Тот, в свою очередь, сделает все сам. Что касается вопроса, кому это выгодно, то я склоняюсь к ответу, что, скорее всего, это киберхулиганы, работающие на грани кибертерроризма. «Завал» интернетовского хребта вряд ли принесет кому-то реальную материальную выгоду, поэтому такими вещами будут заниматься «свободные художники», которые это делают, что называется, прикола ради.

М. М.: Главный ресурс для подобных действий — мозги. Если они есть (а у мозгов — избыток свободного времени) — то этого будет достаточно. Проблемы с каналами и оборудованием не возникнет — атаки обычно не требуют больших материальных вложений. Выгоды от атак не бывает никому. Кроме сомнительной славы, достающейся организаторам атаки (ведь не каждый рискнет пойти получить причитающийся ему «Приз-За-Лучший-Взлом-Года»).

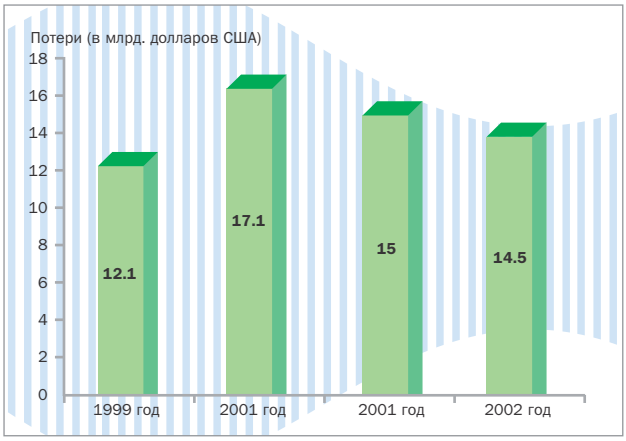
И. П.: Массовые атаки могут быть выгодны по целому ряду причин — идеологических, политических, культурных. А вообще, судя по статистике раскрытых преступлений, большинство сетевых правонарушений совершается из-за денег.

Chip: Как вы оцениваете реальные потери мировой экономики от действий хакеров, вирусов и других вредоносных программ? Кто и по каким методикам подсчитывает ущерб?

Е. К.: По нашим оценкам, предварительный ущерб мировой экономики от вредоносных программ в 2002 году составил $14,5 млрд. Этот результат основан на данных американских научно-исследовательских центров Computer Security Institute и Computer Economics, а также информации аналитического центра «Лаборатории Касперского».

М. М.: Приблизительный ущерб можно оценить самостоятельно. Посчитайте, сколько стоит ваше рабочее время, прикиньте, какая его доля уходит на работу с почтой и какую часть этого времени вы тратите на разгребание спама (у меня 2/3 всей почты — спамерские письма). Положим, 3-5%. В среднем один-два раза в год любая средняя контора встает на уши из-за очередного словленного вируса — выкинем из расписания два рабочих дня в году. Хакерские атаки? С этим сложнее. Наверное, их тоже можно посчитать, но мелкие конторы не часто становятся объектами хакерского вандализма. В общем, очень-очень приблизительно, я готов оценить хакерско/спамерско/вирусные потери как 0,5-5% от оборота пострадавших компаний. »

И. П.: Боюсь, что публикуемые сведения о потерях могут быть очень недостоверными, поскольку одни могут такие данные скрывать (пряча от начальства свою собственную некомпетентность), а другие — сознательно раздувать с целью увеличения ассигнований на собственную деятельность.



Потери мировой экономики от действий вредоносных программ

Не будет горестного плача

Chip: Предположим, что количество и сила атак достигнут некоторой критической величины. Как, на ваш взгляд, может выглядеть конец Всемирной паутины?

Денис Калинин: Чтобы задавать такие вопросы, необходимо быть уверенным в том, что Интернет помрет, но у нас нет оснований верить в это. С тем же успехом можно было бы спросить о судьбе человечества и о том, когда появится новая раса на смену людям — как они будут выглядеть? Это не значит, что постановка таких вопросов невозможна, просто гадать не хочется.

Е. К.: Я не думаю, что конец Всемирной паутины — это будет некое неожиданное, внезапное событие, сопровождаемое горестным плачем и торжественными похоронами. Скорее всего, будет создана параллельная, защищенная сеть, к которой постепенно присоединятся все бизнес-ориентированные компании. Создание новой сети не подорвет мировую экономику, скорее, наоборот — это позволит компаниям значительно сократить расходы на компьютерную защиту и перенаправить их в более продуктивные области. И в этом заинтересована любая компания, любой человек, которому надоело бесконечно выуживать из своего ящика безумные объемы вирусов и спама и тратить все больше денег на установку систем защиты от них. Интернет же станет развлекательно-увеселительной сетью, чем-то вроде Fido, только наполненной вирусами, спамом и непрекращающимися хакерскими атаками. До тех пор, пока нет новой сети, Интернет будут поддерживать и регулярно латать, какие бы конвульсии его не лихорадили. А после этого Интернет просто изменит свою идеологию и станет, как я уже сказал, развлекательно-увеселительной сетью, но никак не основным средством бизнес-коммуникаций.

М. М.: Не вижу ни одной причины, почему бы глобальному Интернету развалиться. Сеть ждет эволюционный путь развития до полного состояния насыщения, которое уже наблюдается в некоторых развитых странах. Штаты уже достигли примерно 60% интернетизации — и Интернет там не развалился. А вырасти

Из истории компьютерных вирусов

Бесконечная история

История компьютерных вирусов неразрывно связана с эволюцией развития электронной вычислительной техники. Еще в 1951 году, на заре компьютеростроения, Джон фон Нейман описал идею самовоспроизводящихся программ. Забегая немного вперед, отметим, что сам термин «вирус» применительно к подобным программам был впервые употреблен только в 1972 году — в статье, посвященной игре «Дарвин» (участниками игры являются специальные программы, борющиеся друг с другом за системные ресурсы).

Распространение первых настоящих («диких») вирусов было затруднено малым количеством совместимых между собой ЭВМ, поэтому одна из первых свободно путешествующих программ — CREEPER — распространялась с 1970 года в сети APRAnet (военном прародителе Интернета). Таким образом, сетевые вирусы появились еще до официального начала вирусной эры. Авторы первых вирусоподобных программ в большинстве случаев не имели никаких злых намерений, а неконтролируемое распространение их питомцев происходило из-за ошибок в алгоритмах. Идея целенаправленных вирусных атак появилась сначала в научно-фантастических произведениях. Например, в романе Томаса Риана «The Adolescence of P-1» (1977 год) был описан вирус, занимающийся сбором информации. Спустя четверть века идея информационных войн, к слову, из научно-фантастического сюжета превратилась в предмет головной боли военных ведомств. Фантасты, кроме того, подарили миру идеи сетевых червей и логических бомб в поставляемом потенциальному противнику оборудовании.

И все же настоящий расцвет вирусописательства наступил с изобретением персональных компьютеров. В 1977 году появился легендарный Apple II, распроданный впоследствии в количестве более 3 млн экземпляров. Наличие дисковода и привычка пользователей обмениваться между собой программами стимулировало развитие первых по-настоящему массовых вирусов. Параллельно шел бурный рост компьютерных сетей на основе телефонных линий. И с появлением публичных досок объявлений (BBS) появился новый вид компьютерного хулиганства — распространение троянских программ.

К настоящему времени известно более 80 тысяч потенциально опасных вирусов, и их количество постоянно растет, гарантируя высокую занятость разработчикам антивирусного софта.

Название	Доля в общем числе вирусных инцидентов, %
I-Worm.Klez	16,65
I-Worm.Lentin	8,75
I-Worm.Sobig	6,57
I-Worm.Avron	6,55
Macro.Word97.Thus	5,17
I-Worm.Hybris	3,13
I-Worm.Roron	2,46
I-Worm.Tanatos	1,92
Backdoor.NetDevil	1,25
Macro.Word97.Saver	1,17
I-Worm.Magistr	0,95
Macro.Word97.Marker	0,95
Worm.Win32.Opasoft	0,79
I-Worm.KakWorm	0,76
Win95.CIH	0,72
Trojan.Spy.SCKeyLog	0,71
Backdoor.Death	0,67
VBS.Redlof	0,66
Win32.Elkern	0,66
Win32.FunLove	0,65
Другие вредоносные программы	38,87

В хит-парад вредоносных программ не включен печально знаменитый Helkern, поскольку собрать более или менее точные данные о нем на момент написания материала не представлялось возможным. По наиболее пессимистичным оценкам жертвами его деятельности стали примерно 80 тысяч компьютеров по всему миру. Специалисты «Лаборатории Касперского» считают, что на долю Helkern приходится около 50% всех заражений в январе 2003 года

▲ Двадцатка наиболее вредоносных программ по данным «Лаборатории Касперского»

» ему количественно более чем в два раза не светит. То есть мы уже имеем пример того, каким будет Интернет везде через обозримое время. Однако некоторые пользовательские протоколы действительно обречены. Вот им — да, светит смерть и забвение. Но именно только некоторым прикладным протоколам, а не самой Глобальной сети. Примеры? Вымерли и выкорчеваны из-за своей врожденной дырявости или слабости против взлома: rlogin, finger, telnet. Устарели и не используются: gopher, WAIS. Вы никогда не слышали таких названий? Не мудрено — они ведь скончались еще до того, как вы впервые в жизни услышали слова Интернет, www, электронная почта. Named (DNS) version 4 повсеместно сменяется на version 8. Кандидаты в покойники (и на замену) в обозримом (но не совсем ближайшем) времени: SMTP — из-за невозможности защитить пользователей от растущих потоков спама, FTP — по причине врожденной кривизны и предрасположенности к дырявости, ICQ — по аналогичной причине. Нет особых сомнений, что выживут и продолжат свое существование HTTP и SSH. И грядет революционное развитие p2p-файлообменных сетей (пользователи не захотят отдавать позиции, завоеванные форматом MP3, а не за горами взрывной рост потребителей DivX).

И. П.: Я думаю, что конец Всемирной паутины в том виде, как она существует сейчас, наступит только вследствие ее технической ограниченности. А скорее всего, при нормальном развитии событий этого не произойдет никогда. Сеть будет эволюционировать. Уверен, что все эти хакерские атаки, неорганизованность информации, быстрая смена бизнес-моделей — лишь болезнь роста, но мы уже прошли ее пик (в мире, но не в России!). С течением времени будут выработаны методики защиты, обкатаны механизмы более рационального поиска и использования информации любого типа. Революционное развитие событий, на мой взгляд, возможно, только если социальное устройство в наиболее экономически развитых странах вдруг изменится. Интернет — это не столько техническое, сколько экономическое и культурное явление. Человечество уже осознало пользу и вкусило преимущества его использования. Поэтому, если вдруг Всемирная паутина в нынешнем виде исчезнет, это значит, что она будет заменена качественно новой инфраструктурой.

Контроль пользователей не получается...

Chip: Разумеется, Интернет давно уже перестал быть чисто компьютерной сетью. Сегодня это и канал для приема и передачи экономической информации, и поле для бизнеса, и серьезный культурный слой. Насколько может измениться ситуация в мире, если Интернет уступит место другой сети, с принципиально новыми стандартами и условиями доступа?

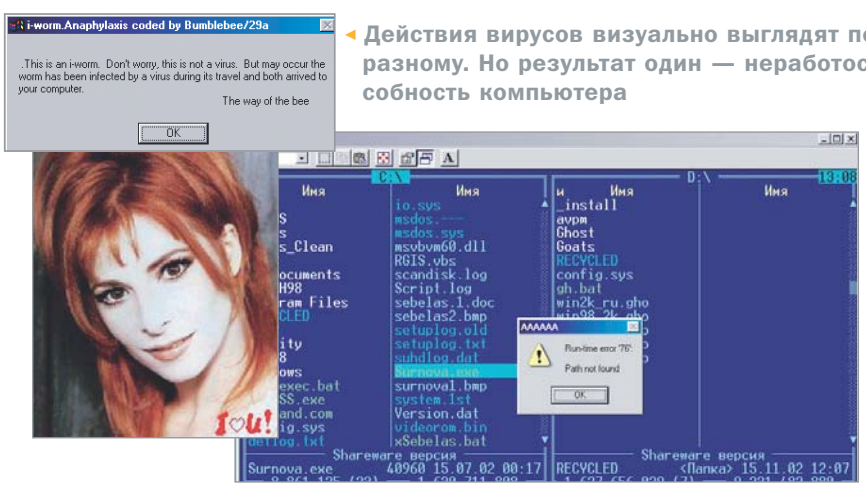
Е. К.: В этом случае при устройстве на работу наряду со знанием текстовых процессоров и Windows люди будут добавлять умение работать в новой сети и Интернете. Мне кажется, что люди будут решать все бизнес-задачи в новой сети, а Интернет оставят для развлечений и общения.

И. П.: Смена стандартов или условий доступа к Сети вряд ли приведет к значительному изменению политической ситуации. Это возможно в отдельно взятой стране: сравните условия работы в Интернете в Китае и, например, Ирландии — но в глобальном масштабе вряд ли что-нибудь существенно изменится.

М. М.: И я не вижу оснований для существенных изменений, так как смены стандарта все равно не предвидится. Все тихо переползут на IPv6, но Интернет при этом останется Интернетом, а TCP/IP — TCP/IP.

Chip: Вполне возможно, что новая сеть будет требовать обязательной паспортизации и предоставления реальных сведений о пользователе. Кто в этом случае возьмет на себя задачу выдачи «паспортов»? Как могут отреагировать на создание такой всемирной базы данных правительства разных стран?

Иван Засурский: На мой взгляд, паспортизация пользователей сети невозможна, хотя степень disclosure, то есть осведомленности, будет расти по мере роста e-commerce и сектора услуг за деньги. Реально контролировать пользователей не получается даже в Китае. »



◂ Действия вирусов визуально выглядят по-разному. Но результат один — неработоспособность компьютера

» **Е. К.:** Это действительно очень сложный вопрос, решение которого потребует серьезных усилий. Мне трудно сказать, как в действительности это будет решено, но я могу определить, что должно в итоге получиться, чтобы система была действительно надежной: «сетевые паспорта» должны выдаваться централизованно — иначе будет невозможно внедрить действительно эффективную систему предотвращения вредоносных действий. Поскольку в данном случае это практически нереализуемо (попробуйте посадить за один стол представителей Индии и Пакистана или Израиля и Палестины), поэтому более вероятен так называемый «тоталитарный» вариант развития событий. Однажды «локомотивы» всемирной индустрии (прежде всего IT-индустрии) заявят, что ограничивают использование Интернета и переходят на новый сетевой стандарт. Так что все остальные компании будут вынуждены постепенно «переползать» в новую сеть.

И. П.: Во-первых, смена механизма регулирования Сети может быть выгодна преимущественно тем, кто планирует извлечь из этого какие-либо дивиденды. Во-вторых, в силу трансграничности Интернета, регулирующей организацией должен стать некий международный орган. Думаю, что он еще не создан. Вряд ли для этих целей можно использовать ООН, поскольку она строилась после Второй мировой войны на совершенно других принципах, ее участниками являются государства. Вряд ли это может быть и какая-то организация при нынешних комитетах по стандартизации типа W3C, поскольку они решают чисто технические вопросы. На мой взгляд, этот орган может когда-нибудь возникнуть только на основе волеизъявления всех (или хотя бы большинства пользователей Сети). Хотя, с другой стороны, а зачем это нужно?

Любая защита является относительной

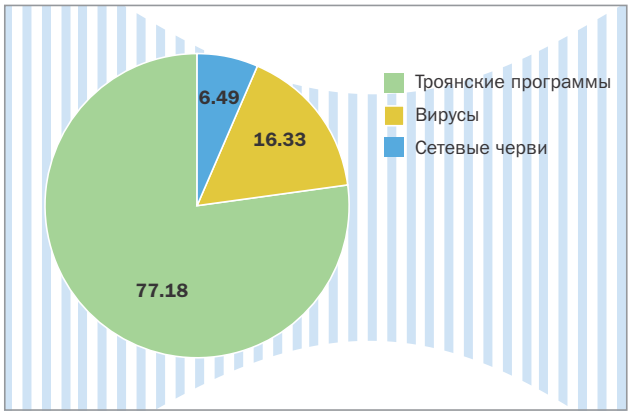
Как несложно заметить, позиции собеседников Chip довольно тесно, хотя и своеобразно кореллируют с родом их занятий. Так, представитель компании Microsoft, неоднократно обвиненной в монополизме и покушении на приватность пользователей, осторожно рассуждает о необходимости международного регулирования Интернета, обходя тему сетевой паспортизации. Евгений Касперский последовательно отстаивает необходимость создания отдельной защищенной сети. Руководители отечественных интернет-холдингов преисполнены оптимизма и считают, что все идет по плану... Боюсь, что нас могут обвинить в необъективности, но рискнем и мы дать собственный прогноз развития ситуации.

Во-первых — и это главное, — второй глобальной сети в обозримом будущем не возникнет. Возможность создания отдельных хорошо защищенных специализированных сетей вовсе не исключается. Но при нынешнем разнообразии телекоммуникационных каналов (телефонные линии, оптоволокно, мобильная телефония и т. д.) с разной пропускной способностью создание чего-то действительно глобального «с чистого листа» будет требовать колоссальных инвестиций.

Во-вторых, любая защита является относительной, и потому сетевые нарушители никогда не будут истреблены полностью. Проблема заключается в том, что необходимые для сетевой атаки или другого акта злой воли ресурсы очень и очень незначительны по сравнению с потенциальным ущербом и затратами на безопасность. Изменение принципов работы Сети ни в коем случае не сделает ее абсолютно защищенной. В конце концов, если, например, кража номеров кредитных карт стала обыденным явлением, то что помешает хакерам воровать сетевые паспорта? В любой сложной системе остаются слабые звенья. И таким слабым звеном, в частности, всегда будут пользователи и их компьютеры.

Одним словом, повысить уровень собственной безопасности можно, только изменив отношение к проблеме. Гораздо надежнее не хранить критически важную информацию на подключенных к Интернету компьютерах, чем уповать на эвристические алгоритмы антивирусов и надеяться на создание новой сети.

Дмитрий Вальяно,
Максим Макаренков



Хотя мы привыкли называть вредоносные программы обобщенным понятием «вирусы», среди них есть свои рекордсмены: сейчас это троянские программы

Вирусные рекорды

Печальные достижения

Наиболее разрушительным сетевым вирусом можно считать безымянный экземпляр, поразивший в 1980 году APRANet. Конечно, количество зараженных тогда машин не шло ни в какое сравнение с числом пострадавших серверов во время январской эпидемии Helkern. Но если последнему удалось «всего-навсего» отключить от Интернета Южную Корею и замедлить работу в Сети в среднем на 25%, то вирус в APRANet «уложил» главную на тот момент сеть на три дня!

Наиболее массовым вирусом пока можно считать легендарного «троянца» Love Bug. Жертвами многообещающей фразы «ILOVEYOU» стали владельцы почти 40 млн компьютеров.

Дороже всех миру обошлись уже упомянутые Helkern и Love Bug (примерно по $10 млрд каждый). Общий ежегодный ущерб от всех вирусов достигает $15 млрд, и нынешний год может поставить новый печальный рекорд.