Руслан Богатырев

Антивирусы Касперского: разящий меч революций

Основные проблемы антивирусных программ

Компьютерные вирусы и другие вредоносные программы давно уже стали бичом современных компьютеров и ежегодно наносят огромный ущерб сотням миллионов пользователей. Если раньше авторы создавали вредоносные программы в основном ради самовыражения, то в последнее время они уже поставлены на службу теневому бизнесу и военно-промышленному комплексу ведущих стран мира.

В подобной ситуации резко возрастает роль антивирусных компаний, производящих всевозможные "противоядия" — средства обнаружения (диагностики), устранения, лечения и профилактики несанкционированного вторжения в компьютерный организм. За четверть века на этом рынке уже определились основные игроки, поделившие между собой сферы влияния: Network Associates (McAfee) и Symantec — Америка, Trend Micro — Азия, Panda — Европа. В России все последние годы практически безраздельно господствует компания "Лаборатория Касперского".

К сожалению, жесткая конкуренция привела к тому, что антивирусные компании, преследуя свои коммерческие интересы, породили немало проблем на потребительском рынке, решение которых еще ждет своего часа (корпоративный рынок — предмет отдельного обсуждения).

Перечислим наиболее важные из них.

1. Различия в трактовке понятия "компьютерный вирус".

Термин "компьютерный вирус" укоренился в общественном сознании как *очень опасный* инородный "микроб" ("микроорганизм"), неизбежно приводящий к тяжелому поражению компьютерной системы, а нередко и к "летальному" исходу. При этом сами антивирусные компании частенько обозначают данным термином *любой* внешний "микроорганизм", чье происхождение и поведение может рассматриваться *ими* как потенциальная угроза информационной безопасности. С недавних пор стал активно применяться термин malware (происходит от malicious software — вредоносные программы), объединяющий такие группы, как черви (worms), трояны (Trojans), вирусы (viruses) и потенциально опасные программы (spyware, adware и др.). Подобной классификации придерживается авторитетный британский журнал Virus Bulletin (http://www.virusbtn.com). Удивительно, что нередко подход к терминологии различается даже внутри одной компании! Налицо явный и опасный разрыв в восприятии ключевого термина производителями и потребителями антивирусных программ.

2. Расхождения в определении степени опасности заражения.

Антивирусные компании по-разному трактуют степень угрозы со стороны "микробов". Как и в биологии, в мире компьютеров "микробы" могут быть не только болезнетворными (патогенными). Известно, что определенные виды бактерий продуцируют антибиотики, аминокислоты, витамины. В программном обеспечении нередко приходится использовать механизмы для дистанционного одно- или двустороннего обмена информацией с внешним компьютером. Практически любое подобное взаимодействие (независимо от того, что это — то ли обновление программ или информации, то ли передача новостей, рекламы и т.п.) может рассматриваться как потенциальная угроза. Причем если одни компании дают одному и тому же компьютерному "микробу" минимальный уровень опасности, то другие — максимальный.

3. Отсутствие единой международной классификации компьютерной инфекции.

Каждая компания присваивает инфекции свои названия, причем даже специалистам очень трудно понять, какой "микроб" имеется в виду. Есть, конечно, весьма уважаемое издание Virus Bulletin со своей классификацией, но и она расходится с реальностью для многих компаний. Существует WildList Organization (http://www.wildlist.org), ежемесячно собирающая отчеты различных экспертов-вирусологов о вирусной опасности. Ее тестовыми наборами пользуется Virus Bulletin для сертификации продуктов на соответствие критериям VB 100%. Имеется и так называемая "Организация антивирусных исследований" (CARO, Computer Antivirus Research Organization, http://www.caro.org), но при ближайшем рассмотрении выясняется, что это всего лишь неформальный клуб, объединяющий два десятка авторитетных экспертов. За годы своей публичной деятельности CARO ограничилась тем, что выдала некоторые рекомендации, касающихся именования "микробов". Но их все же нельзя назвать единым реестром. Чтобы как-то разрешить наболевшую проблему, Айан Уолли (Ian Whalley) создал программу VGrep, постоянно обновляющую свою базу кросс-ссылок (словарь "синонимов") для самых известных антивирусных продуктов. Такая база строится путем "натравливания" разных антивирусов на эталонный набор зараженных файлов и выявления диагностики их инфицирования (сейчас ее сопровождает Дмитрий Грязнов из департамента Advanced Security Research исследовательской лаборатории McAfee Security).

4. Технологическая исключительность.
Антивирусы не терпят наличия конкурирующих программ на одном и том же ПК.

Если пользователь поставил на свой компьютер антивирус одной компании, то почти наверняка ему не удастся полноценно задействовать конкурирующую программу. Это обусловлено особенностями реализации антивирусного контроля, и прежде всего тем, что помимо статического сканирования памяти и файлов ("препарирование" каждого файла) антивирусные программы выполняют еще и динамический мониторинг всей системы (расставляют "камеры наблюдения") для выявления фактов потенциального или реального инфицирования. Поскольку такие компании не являются производителями ни процессоров, ни соответствующих операционных систем, им приходится вместо работы на уровне ядра компьютерной системы (где как раз-таки и необходимо возводить фундамент защиты) довольствоваться дальними рубежами операционного окружения. Другая причина — конкурентная борьба. Антивирусные компании не только не заинтересованы в обеспечении полноценной работы своих конкурентов, но нередко намеренно чинят им всяческие препятствия. В результате страдают пользователи, ибо, не имея возможности сопоставлять и анализировать результаты проверок на наличие вирусов и угроз, они вынуждены передоверяться конкретной компании.

5. Информационное отчуждение. Антивирусные компании практически не сотрудничают друг с другом в области оперативного информирования о появлении новых микробов.

Показательный пример такого рыночного “эгоизма” (в связке Symantec — “Лаборатория Касперского” — “ДиалогНаука”) см. в статье “Трояны и Adware” (“Мир ПК-диск”).

Если проводить параллели с медициной времен дореволюционной России, то можно сказать, что больному, то бишь пользователю, приходится довольствоваться услугами местного уездного лекаря, хотя тот путает болезни, применяет непроверенные методы врачевания и никем не контролируется, — выбирать, увы, не приходится.

Из медицинских энциклопедий

Вирусы (от лат. virus — яд) — внутриклеточные паразиты, способные размножаться только внутри живых клеток. Возбудители многих опасных заболеваний. Вирусы (вирус табачной мозаики) открыты русским ботаником Дмитрием Ивановским в 1892 г.

Бактерии (от греч. bakterion — палочка) — одноклеточные микроорганизмы, лишенные клеточного ядра. Являются возбудителями многих опасных заболеваний человека (туберкулез, дизентерия, дифтерия и др.). Но при этом участвуют в круговороте элементов (азота, углерода, серы, фосфора), способствуют повышению плодородия почвы.

Риккетсии (Rickettsiae) — бактерии, похожие по строению на крупные вирусы. Размножаются в клетках живых организмов. Открыты американским ученым Ховардом Риккетсом, погибшим от тифа.

Чтобы глубже разобраться в причинах и следствиях приведенных проблем, рассмотрим их на примере самой известной отечественной фирмы, занимающейся антивирусной защитой, — "Лаборатории Касперского".

Мифы "Лаборатории Касперского"

Данная компания сумела выстроить в умах наших пользователей образ беспощадного палача любой компьютерной заразы — палача, от которого не может спрятаться ни один мало-мальски вредоносный микроорганизм. Если посмотреть на результаты трех последних лет в ежегодном читательском опросе "Лучший продукт года", проводимом журналом "Мир ПК", то выяснится, что первую строку в соответствующей номинации неизменно занимает именно "Лаборатория Касперского", чья доля в предпочтениях пользователей колеблется в районе 50%. Как показывает сравнение данных опроса "Лучший продукт года" с результатами исследования рынка соответствующими профессиональными агентствами, цифры в ряде номинаций очень близки, так что их априори можно брать за надежный ориентир.

Лаборатория Касперского

Образована 21 июля 1997 г. В нее вошли сотрудники антивирусного отдела компании "КАМИ", возглавлявшегося Натальей Касперской, нынешним генеральным директором "Лаборатории Касперского". В момент создания в компании работало 19 человек, из них 6 были разработчиками. В настоящее время в ее составе свыше 400 человек. Центральный офис расположен в Москве, имеются представительства компании в Великобритании, Китае, Франции, США, Германии, Японии, Нидерландах и Польше. По различным оценкам, она контролирует 60—70% российского рынка антивирусных программ; доля на мировом рынке — около 1% (данные 2002 г.). По результатам 2004 г. корпоративные продукты составили 90% объема продаж, персональные — 10%. Официальный сайт — http://www.kaspersky.ru.

Эта одна причина выбора данной компании в качестве образца для анализа проблем антивирусной безопасности. Другая куда более прозаичная. За последние несколько месяцев мы получили много писем, в которых читатели буквально пригвоздили нас к позорному столбу за то, что наши диски "просто кишат вирусами". Причем в 100% случаев речь шла именно об антивирусах Касперского и применительно как раз-таки к псевдовирусам (потенциальным угрозам).

В представлении большинства пользователей, если такой уважаемый продукт, как "Антивирус Касперского", написал "вирус", то значит, вирус, и точка. Никаких сомнений в "прокаженности" диска. Ложные срабатывания, потенциальные ошибки в программном обеспечении, разная трактовка степени угроз — все это лирика, которая обывателя вообще никого не интересует. На совет перепроверить другими доступными антивирусами например, (онлайновыми сервисами ведущих антивирусных компаний или бесплатными антивирусами) реакция потрясающая: "Зачем? И так все ясно".

Как показала практика, уровень доверия (точнее говоря, невероятной, безграничной доверчивости) отечественных пользователей к антивирусной продукции "Лаборатории Касперского" просто поражает, хотя налицо очевидное расхождение между реальными возможностями продуктовой линейки этой компании и восприятием ее потребителями. Чем вызван подобный феномен? Насколько опасны эти искусственно культивируемые заблуждения пользователей? Какова степень ответственности подобных компаний в наши дни? Попробуем обстоятельно ответить на поставленные вопросы.

Прежде чем погрузиться в анализ затронутых проблем, рассмотрим те ключевые мифы, на которых базируется нынешний образ "Лаборатории Касперского".

Миф 1. Антивирусы Касперского — лучшие в мире

Это далеко не так. Ни с технологической точки зрения, ни тем более с рыночной лидерами они не являются. Рыночная доля измеряется единицами процентов. "На мировом рынке, — пишет Йенс Хартманн (Die Welt, Германия, март 2004 г.), — Касперский пока не крупный

игрок. Главное, ему пока не удалось закрепиться в США. Такие предприятия, как Symantec, Network Associates, Check Point и фирма Trend Micro имеют намного большие доли на мировом рынке".

Рыночная доля в мире измеряется единицами процентов. С точки зрения международной сертификации (VB 100%), в среде Windows XP "Антивирус Касперского" успешно прошел тестирование в 2005 г. (июнь, Kaspersky KAV Personal 5.0.227) и 2004 г. (июнь, Kaspersky Anti-Virus 4.5.0.94). До этого в 2003 г. (Kaspersky Anti-Virus 4.0.5.37), в 2002 г. (Kaspersky Anti-Virus 4.0.50), в 2001 г. (Windows 2000, Kaspersky Lab KAV v3.5.133.0), в 2000 г. (Windows 98/NT, Kaspersky Lab AVP v3.5.133.0) тестирование завершалось неудачей. Если брать неформальную сторону, то по вскрытию угроз (особенно на базе сигнатурного подхода) компания — безусловно, одна из лучших в мире, а вот что касается остального (диагностика, корректная нейтрализация угроз, качество реализации ПО, сервис), то оно еще требует большой и кропотливой работы.

Миф 2. Антивирусы Касперского — самые проницательные, ничто не скроится от их всевидящего ока.

Знаете ли вы, что существуют такие вирусы, которые просто не обнаруживаются антивирусами Касперского? Подавляющее большинство антивирусных компаний (не исключение и "Лаборатория Касперского") использует в качестве основного подход на базе сканирования сигнатур (уникальной последовательности программного кода). В качестве правил верификации применяются знания об алгоритмах полиморфизма (видоизменения) сигнатур. Причем требуется постоянно проводить через Интернет "вакцинацию", т.е. обновлять базу сигнатур (по состоянию на июль 2005 г. в "Антивирусе Касперского" насчитывается свыше 125 тыс. сигнатур). Механизмы прогнозного эвристического анализа (попытки найти вирусную угрозу без прямого использования базы сигнатур) могут лишь слегка подсластить горькую пилюлю. Что касается мониторинга угроз антивирусом, то это не только сильно загружает компьютер, создает проблемы с установленным ПО, но и при этом еще не дает серьезных гарантий ограждения от неприятностей со стороны вредоносных программ. Куда более надежным подходом являются особые поведенческие технологии, в частности имитация выполнения сомнительного кода, контролирующая и блокирующая опасные операции (принцип саркофага), чего антивирусы Касперского, к сожалению, пока не делают.

Небольшой пример. В НПФ "Стокона" (http://www.stocona.ru) уже довольно давно разработана технология интеллектуального антивирусного сканирования, построенная на принципиально ином подходе — анализе функций программ без их выполнения. Для класса потенциально вредоносного ПО на основе интерпретируемых программных модулей, таких как макровирусы (VBA в документах Microsoft Office) и скрипт-вирусы (JavaScript в браузерах), задача успешно решена (сравнительный анализ с ведущими антивирусными программами мира см. http://www.stocona.ru/products/antivirus/comparison.html).

Другой штрих. Подавляющее большинство пользователей применяет в антивирусах только механизм статического сканирования файлов (без мониторинга операций). Если авторы вредоносных программ используют методы криптографии, то невозможно обнаружить опасные участки кода.

Программы из зоны риска.
Мнения ведущих экспертов "Лаборатории Касперского"

Дэвид Эмм,
старший технический консультант
английского отделения "Лаборатории Касперского"

"Я считаю, что шпионские (spyware) и рекламные (adware) коды представляют реальную угрозу для информационной безопасности. Тем не менее, это не новая угроза. Разобраться в ситуации мешает путаница с терминологией. Если следовать большинству определений шпионских кодов (spyware), то придется причислить к ним еще и троянские программы… Многие разработчики и аналитики относят к шпионским кодам еще и рекламные (adware). Последние же показывают рекламу на зараженном ПК и подменяют результаты поиска. Рекламные коды очень похожи на спам, но не распространяются по электронной почте. Мы в «Лаборатории Касперского» называем все эти программы riskware ("программы из зоны риска", "потенциально опасные программы"). Во многих случаях эти приложения являются легальными, но могут быть

использованы в противозаконных целях в руках преступника… Продукты «Лаборатория Касперского» предлагают защиту от riskware, но в виде отдельной дополнительной опции.

Костин Раю,
глава отдела исследований и разработки
румынского отделения «Лаборатории Касперского»

"Я считаю, что не все антивирусы достаточно хорошо детектируют потенциально вредоносный код (riskware). Другими словами, такие программы могут очень долго жить на компьютере пользователя, пока тот не заподозрит что-то неладное. В некоторых случаях, удалить компоненты рекламного кода (adware) очень сложно. К тому же они могут снова попасть на компьютер из Интернета. В итоге, детектирование adware-программ представляется очень деликатной задачей, особенно в странах с довольно либеральными законами. Например, известны случаи, когда разработчики антивирусной программы, добавившие детектирование определенного нежелательного кода в свой продукт, были привлечены к суду и, как следствие, были вынуждены пойти на уступки."

Евгений Касперский,
глава антивирусных исследований «Лаборатории Касперского»

Я считаю, что шпионские программы (spyware) представляют собой очень серьезную угрозу. Они могут привести к краже конфиденциальной информации, включая банковские реквизиты пользователя. Рекламные коды (adware) не так опасны. Они не причастны к утечке важных данных, но воздействуют на посещаемые веб-страницы и поисковые запросы. Вдобавок представители класса adware могут конфликтовать с установленным программным обеспечением (что часто и происходит), а это чревато неприятными последствиями. По степени опасности между шпионскими и рекламными кодами я бы разместил другие потенциально опасные программы (riskware). Хакеры достаточно часто при атаках используют легальные сетевые программы и различные утилиты мониторинга клавиатуры, экрана и т.д. Если говорить о средствах борьбы со всеми вышеперечисленными категориями вредителей, то антивирусные программы всегда детектировали и удаляли шпионские коды, а антирекламная функциональность была добавлена лишь в последние годы. Таким образом, рекламные программы успели действительно «достать всех и вся» (этим объясняется такое повышенное внимание к ним со стороны прессы)…"

Миф 3. Антивирусы Касперского — самые лучшие диагносты.

Известно ли вам, что далеко не все, что выявляется как вирусы с помощью антивирусов Касперского, таковым является? Это, пожалуй, одно из самых уязвимых мест в антивирусной продукции компании. Если раньше все потенциально опасные коды без разбора обозначались убийственным словом "вирус", то в последнее время в "Лаборатории Касперского" после долгих и настойчивых обращений (в том числе и с нашей стороны) снизошли до просьб пользователей и стали применять понятие riskware ("программы из зоны риска"). Показательно, что глубоко в недрах отчетов самых известных продуктов компании — Антивируса Касперского Personal 5.0 и Антивируса Касперского Personal Pro 5.0 — рядом с файлами сомнительной опасности фигурирует надпись на английском языке "not-a-virus" (т.е. "не вирус"), тогда как в итоговой статистике в самом начале отчета на понятном русском языке без тени сомнения эти же файлы включены в число вирусов.

Мифотворчество — хорошо известное оружие маркетинговых войн, сыгравшее немалую роль в формировании нынешнего образа "Лаборатории Касперского". Разумеется, используются и другие эффективные приемы. Но в контексте данной статьи нет смысла касаться тонких материй закулисной конкурентной борьбы, вполне достаточно ограничиться взглядом рядового потребителя.

Кто виноват и что делать?

Кто виноват в подобном хаосе и что же делать обычному пользователю? Куда податься и на кого ориентироваться? Очевидно, хаос возник вследствие ожесточенной рыночной борьбы антивирусных продуктов, роль которых при постоянном нарастании и нагнетании информационных угроз становится все более и более значимой. Как известно, у человека

иммунитет бывает врожденный и приобретенный, а у компьютерных систем — пока только приобретенный. Врожденный же должен устанавливаться на уровне грамотно продуманной интеграции ключевых аппаратных средств (процессоров) и ядра соответствующей операционной системы. Работы в этом направлении уже ведутся, но весьма неспешно. На протяжении двух последних десятилетий антивирусные компании желают закрыть образовавшуюся брешь и сделать на этом свой бизнес. Каждая из них проводит *собственный* поиск новых "микробов", пополняет *свою* базу сигнатур и ведет *свой* реестр "микроорганизмов". Для многих, думаю, будет откровением узнать, что названия, которые дают в этой бесконечной ежедневной гонке, через какое-то время могут изменяться даже внутри одной и той же компании (тут не поможет никакой VGrep)!

При прочих равных условиях отдельные антивирусные компании (в том числе и "Лаборатория Касперского") не ограничиваются поиском конкурентного преимущества в одних только технологиях, а планомерно ведут агрессивную политику, намеренно (либо по недосмотру) замалчивая степень угрозы тех или иных программных кодов. Как вы думаете, если одна программа на тестовом наборе не найдет ни одного вируса, а другая — сразу три (причем неважно, что это всего лишь условно опасные коды), какую из них предпочтет использовать у себя обычный пользователь, не имеющий ни времени, ни желания погружаться в хитросплетения антивирусной индустрии?

Что такое потенциально опасные программы (riskware, spyware, adware)? Это не черное (blackware) и не белое (whiteware), это пограничный слой (greyware), порождающий проблему грамотного управления подобными рисками. Если обратиться к бытовой ситуации, то это подобно наличию ножа. Но разве тот, кто его держит в руках, — обязательно преступник? В подавляющем большинстве случаев, конечно же, нет.

С теми программами, которые наносят очевидный урон, все ясно. А вот в отношении потенциально опасных программ налицо диктат производителей антивирусных средств, единолично определяющих, какие программы плохие, какие — хорошие. Собственными ушами слышал, как на очередной пресс-конференции Евгений Касперский с Максимом Поташевым поясняли, какие параметры функционирования программ (некоторые скрытые и/или недекларированные действия) они считают "плохими", что автоматически заносит в черный список создающие их компании. Может быть, эти критерии утверждены какой-либо ассоциацией или на худой конец закреплены в публичном официальном документе "Лаборатории Касперского"? Если разобраться, то любая программа, осуществляющая явным или скрытым образом недекларированные действия (хотя бы из-за неточностей в документации), автоматически попадает в разряд потенциально опасных. Доказать умысел скрытого поведения или недекларированности возможностей очень сложно. Многое зависит от того, что это за функции и возможности.

Таким образом, антивирусные компании, видимо, сами того не желая, взвалили на свои плечи обязанности не только полицейского (как любит говорить Евгений Касперский), но также законодателя, судьи и даже палача, немедленно приводящего приговор в исполнение. Каким образом могут "отмыться" мелкие компании-производители, попавшие ни с того ни с сего в подобный черный список? На Западе приходится добиваться восстановления попранных прав путем судебной тяжбы. Это подтверждает и Костин Раю, глава отдела исследований и разработки румынского отделения "Лаборатории Касперского" (см. врезку выше). У нас же в стране такие прецеденты неизвестны. Возможно, пока...

Нередко в прессе можно встретить обвинения, направленные в сторону антивирусных компаний, в якобы намеренном сокрытии информации о начале вирусных эпидемий или даже о том, что они организовали собственное подпольное производство некоторых вредоносных программ. В основном подобные обвинения наверняка надуманны. Но ведь сама антивирусная индустрия дает все основания так полагать. Де-факто статус полицейского, законодателя, судьи и палача одновременно не только предоставляет поистине безграничную власть, но и плодит у бесправных потребителей самые фантастические догадки.

Деятельность антивирусных компаний нередко сравнивают с медициной и здравоохранением. В самом деле, параллелей здесь много, однако если спроецировать их продукты и услуги на типичную жизненную ситуацию, получится настоящий театр абсурда. Представьте себе, что вы пришли на прием к врачу (роль которого в нашем воображаемом случае выполняет "Антивирус Касперского"). Он собирает анализы, читает историю болезни, выслушивает жалобы и ставит диагноз — болезнь. Простите, доктор, а как она называется и каким образом ее лечить? Что это — легкое отравление или СПИД? В ответ врач молча пишет на листочке (в вирусном отчете) мудреное название латинскими буквами и говорит: "Следующий". Вы остаетесь в недоумении.

Сначала пытаетесь найти в местном справочнике (у "Лаборатории Касперского" имеется онлайновая вирусная энциклопедия http://www.viruslist.com/ru/, которая, как показал наш опыт, ведется из рук вон плохо). Там с трудом удается отыскать название, но к нему не дается никакого описания, а в других справочниках даже нет таких названий! Мыслимое ли дело, если бы врач назвал заболевание, но найти его описание в справочниках не смог даже специалист, не говоря уже о больном? А в области антивирусного ПО (в большей степени у нас в стране) подобное считается нормой.

Что же делать? Идти на прием к другому врачу? Потом сопоставить диагнозы, чтобы разобраться, в чем суть недомогания, и заняться *самолечением*. Увы, такой воображаемый случай не исключение, а скорее правило.

Рекламные программы — исчадие зла?

Adware-программы (рекламные программы) благодаря активной пропаганде со стороны ряда антивирусных компаний буквально с момента своего появления сразу же стали изгоями. Причина — использование механизма скрытой подкачки рекламы с удаленного сервера, а также возможность сбора и передачи информации в обратную сторону — на сервер поставщика рекламы.

Очевидно, что сам подход, где в качестве оплаты за услуги (программу) потребитель соглашается просматривать рекламные блоки, давно завоевал право на жизнь. Достаточно включить телевизор, чтобы убедиться, сколь эффективно (хотя и излишне назойливо) работает такая бизнес-модель. За все нужно платить. Если у потребителя нет возможности (или желания) приобрести понравившуюся ему программу, то почему его надо лишать права выбора? Одни смотрят спутниковое телевидение и платят, в том числе, за почти полное отсутствие там рекламы. Другие хотят тоже смотреть интересные передачи, но бесплатно (точнее, за рекламу). Каждому — свое.

Неужели поголовно все производители рекламных программ (adware) такие нехорошие, что только и думают о том, как бы доставить неприятности пользователю? У них свой бизнес, где априори нужно стремиться к доверию и расширению числа потребителей, так что не уважать их права в данном случае, мягко говоря, некорректно.

Интересно, кто мешает сертифицировать (в рамках сообщества антивирусных компаний мира) представленный в исходных текстах надежный механизм, в котором угрозы ИТ-безопасности были бы сведены к нулю? Неужели разработчики рекламных программ отказались бы его использовать, раз он функционально решает вопрос доставки на компьютер потребителя рекламных блоков? Ответ простой: никакого организованного сообщества антивирусных компаний (профессиональной ассоциации), к сожалению, не наблюдается. Почти наверняка, если кто-то из adware-компаний попробует предложить нечто подобное антивирусному сообществу, его просто не захотят слушать. Вот и получается, что сами антивирусные компании (разумеется, не все) предпочитают делать себе дешевую рекламу, дискредитируя чужой бизнес.

Простой вопрос: публиковать ли на "Мир ПК-диске" продукты класса adware? С одной стороны, этому вроде бы ничто не мешает. В конце концов, при соответствующей индикации об особом классе ПО (и внимательном прочтении лицензии перед установкой) каждый пользователь сам вправе решать, устанавливать его или нет. С другой — какой интерес в тысячный раз объяснять очередному возмущенному читателю, что это легальные программы, имеющие право на жизнь, и диск ничем не провинился в том, что одна из популярных антивирусных программ считает adware тем злом, которое надо непременно искоренять.

Казалось бы, что может быть проще — проводите предварительный контроль планируемого к размещению adware самыми агрессивными антивирусными программами, и дело с концом. Что пропустят — публикуйте. Если бы все было так просто… В случае потенциальных угроз (а не реальных вирусов) дело обстоит крайне неважно.

У той же "Лаборатории Касперского" на персональном рынке есть два продукта: "Антивирус Касперского Personal 5.0" и "Антивирус Касперского Personal Pro 5.0" (для простоты рассуждений о предыдущих версиях умолчу, поскольку их учет проблемы только усугубляет). Если кто-то думает, что суффикс Pro (Professional) автоматически означает, что детектировать угрозы продукт будет не хуже, чем обычный, он сильно ошибается. Специфика подключения расширенных баз сигнатур (необходимых для выявления riskware), их совместимости с определенными модификациями подверсий этих продуктов и т.п. столь запутанная, что никакой

гарантии такая фильтрация adware не даст. Тем более, что в базу сигнатур информация может попасть и после выхода диска (как было в случае с ситуацией 2003 г., описанной в статье "Трояны и Adware"), когда даже теоретически такую угрозу (не вирус) детектировать было невозможно.

Из-за подобных проблем наши коллеги из журнала PC Magazine RE в мае этого года были вынуждены на страницах издания заявить по сути об отказе от дальнейшего размещения на своих дисках программ класса adware.

Легендарный Касперский

Имя Касперского гремит по всей стране. Трудно найти на российском компьютерном рынке другую персону, которая могла бы сравниться по уровню известности с этим непримиримым революционером, объявившим смертный бой всей вредоносной нечисти.

Евгений Валентинович Касперский

Руководитель антивирусных исследований компании "Лаборатория Касперского". Родился 4 октября 1965 г. в Новороссийске. Имеет польские корни (прапрадедушка в конце XIX в. эмигрировал из Кракова в Россию). В 1982 г. окончил известную физико-математическую школу №18 им. А. Н. Колмогорова (в 1988 г. она вошла в состав Специализированного учебно-научного центра МГУ им. М. В. Ломоносова), а в 1988 г. — Высшую школу КГБ СССР ("Институт криптографии, связи и информатики"). До 1991 г. работал в закрытом секретном учреждении. С 1991 по 1997 г. — в НТЦ "КАМИ", где занимался развитием антивирусного проекта AVP. Один из основателей "Лаборатории Касперского". По настоянию бывшей жены, Натальи Касперской, дал свое имя семейству продуктов и самой компании. В связи с некоей темной, по словам Касперского, историей названия AVP и Antiviral Toolkit Pro были преданы забвению, а флагманский продукт компании стал называться "Антивирус Касперского". В 2001 г. британским журналом Virus Bulletin назван лучшим антивирусным экспертом мира.

Надо отдать должное Евгению Касперскому. В лучших традициях крупных русских промышленников и предпринимателей царской России он дал свое имя той компании, с которой связал жизнь. Это марка, это тот знак качества, которому привыкли доверять. "Действительно, даже из мировой практики я могу вспомнить только Питера Нортона, автора Norton Commander, — признается Евгений Касперский в недавнем интервью журналу "Свой бизнес" (июнь 2005 г., http://is.park.ru/doc.jsp?urn=4873977). Видимо, основатели компаний в этой сфере не хотят связывать свою продукцию с собственным именем, боятся рисковать. Но ведь я тоже не хотел этого, просто судьба так распорядилась".

К сожалению, всякая медаль имеет и оборотную сторону: с именем основателя связывают не только успехи, но и неудачи его компании. Думаю, многие помнят, сколько нареканий с точки зрения быстродействия вызывала "четверка" (Антивирус Касперского Personal 4.0). По правде говоря, до знакомства с "четверкой" я никогда в своей практике не сталкивался с ситуацией, когда ориентированная на массовый рынок авторитетнейшая программа, в чьи функции входит защита информационной безопасности, намертво блокировала новенький импортный ПК с лицензионным ПО: немало времени и усилий потребовалось отнюдь не начинающему пользователю, чтобы вывести из комы Sony Vaio.

В Интернете на этот счет ходила народная байка-легенда, достаточно точно отражавшая проколы с "четверкой". Не удержусь, чтобы не привести ее здесь в некоторой обработке.

Легенда о мастерах Мурамаса и Масамунэ

Мастер Мурамаса делал самурайские мечи, беспощадно разившие врага. *Мастер Масамунэ* ковал мечи как оружие, которому вверяют свою жизнь. Чтобы сравнить лучшие клинки, их вонзили в дно лесного ручья. Осенние листья, что плыли по течению, должны были соприкоснуться с творениями великих мастеров, но, о чудо: те листья, которым выпала судьба дотронуться до меча *мастера Мурамаса*, оказывались рассеченными надвое. Другие же опавшие листья тихо проплывали мимо меча *мастера Масамунэ*, не касаясь его.

Питер Нортон делал антивирусы грозные, как разящий самурайский меч. *Евгений Касперский* делал антивирусы капитальные, как железобетонные сваи. Чтобы сравнить их, к той сети, где постоянно кишели вирусы, подключили два ПК с Windows XP

> Professional и антивирусами *Нортона* и *Касперского*. Все вирусы, что попались антивирусу Нортона, оказались уничтоженными. А машину с антивирусом Касперского вирусы обходили стороной, ведь при 100%-ной загрузке центрального процессора сетевой адаптер просто не успевает общаться с сетью...

Казалось, все позади, вышла пятая версия, где удалось ликвидировать серьезные изъяны в работе. Но тут на плечи компании легли новые заботы. Нельзя не сказать, что проблемы с некорректной трактовкой вирусных угроз (пресловутое adware) затронули не только "Лабораторию Касперского". Их пытается решить каждая мало-мальски значимая на рынке антивирусная компания. У одних что-то получается, у других — не очень. Хочется верить, что время поможет выработать взвешенный подход к решению этих непростых задач.

Это тем более важно, что туманность и двусмысленность формулировок в нашем законодательстве внушает немалое опасение. Ведь если следовать букве закона, то под статью 273 УК РФ можно будет подвести не только вредителей, но и нейтральных, ничего не подозревающих лиц и даже… антивирусные компании. Судите сами…

> **Статья 273 УК РФ.** Создание, использование и распространение вредоносных программ для ЭВМ
>
> 1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, **блокированию** (здесь и далее выделено мной — Р. Б.), модификации либо копированию информации, **нарушению работы ЭВМ**, системы ЭВМ или их сети, а равно **использование** либо **распространение** таких программ или машинных носителей с такими программами — наказываются лишением свободы на срок **до трех лет** со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
>
> 2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет.
>
> Источник: Уголовный кодекс РФ от 13 июня 1996 г. N 63-Ф
> (введен в действие с 1 января 1997 г.)
>
> **Комментарии к данной статье ведущих юристов России**
>
> Под вредоносными программами в смысле комментируемой статьи понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под **нормальным функционированием** понимается выполнение операций, для которых эти программы предназначены, что определено в документации на программу… Уголовная ответственность возникает уже в результате **создания** программы, независимо от того, использовалась эта программа или нет.
>
> Из комментария М. М. Карелиной,
> доцента Российской академии правосудия,
> члена Экспертного совета Комитета по безопасности
> Государственной Думы Федерального Собрания
> (Комментарий к Уголовному кодексу Российской Федерации /
> Отв. ред. Председатель Верховного Суда РФ В. М. Лебедев. — М.: Юрайт-Издат, 2004)
>
> Понятие вредоносной программы шире понятия "вирусная программа", которая кроме вредоносности должна обладать способностью самораспространения… **Несанкционированное блокирование**, модификация и т. д. означает достижение этого результата без разрешения владельца ЭВМ или иного законного полномочия… **Распространение** вредоносной программы означает как распространение ее с помощью средств связи, так и простую передачу ее другому лицу в любой форме (в том числе и виде записи на бумаге).
>
> Из комментария канд. юрид. наук И. А. Клепицкого
> (Комментарий к Уголовному кодексу Российской Федерации /
> отв. ред. проф. А. И. Рарог. — М.: ТК Велби, Изд-во Проспект, 2004.)
>
> Самой распространенной разновидностью вредоносных программ является вирус — компьютерная программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии вируса сохраняют способность дальнейшего распространения (ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов). За

создание вредоносных программ, их использование либо распространение установлена уголовная ответственность ст.273 УК РФ.

В. Погуляев, А. Теренин "эж-ЮРИСТ", 2004 г., январь, № 2.

Именно высокой степенью общественной опасности объясняется то, что уголовный закон преследует **достаточно строго** за сам факт создания программ для ЭВМ или внесения изменений в существующие программы, не оговаривая наступление каких-либо последствий... С субъективной стороны преступление может быть совершено как по неосторожности в виде **легкомыслия**, так и с косвенным умыслом в виде **безразличного отношения** к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил виновный, а когда наступили последствия, к достижению которых он стремился, — и в зависимости от наступивших последствий.

Из комментария проф. С. В. Бородина,
заслуженного юриста РФ,
главного научного сотрудника Института государства и права РАН
(Постатейный Комментарий к Уголовному кодексу РФ 1996 г. /
под ред. проф. А. В. Наумова)

При установлении вреда, причиненного преступлением, следует помнить, что вредоносная программа в виде вируса может практически мгновенно размножиться в большом количестве экземпляров и очень быстро заразить многие компьютерные системы и сети. Это реально, ибо компьютерные вирусы могут:

а) заполнить весь диск или всю свободную память ЭВМ своими копиями;

б) поменять местами файлы, т.е. смешать их так, что отыскать их в компьютере будет практически невозможно;

в) испортить таблицу размещения файлов;

г) отформатировать диск или дискету, уничтожив все ранее записанное на соответствующем носителе;

д) вывести на дисплей то или иное нежелательное сообщение;

е) перезагрузить ЭВМ, т.е. осуществить произвольный перезапуск;

ж) замедлить ее работу;

з) изменить таблицу определения кодов, сделав невозможным пользование клавиатурой;

и) изменить содержание программ и файлов, что повлечет ошибки в сложных расчетах;

к) раскрыть информацию с ограниченным доступом;

л) привести компьютер в полную негодность.

Размер причиненного ущерба устанавливается экспертным путем в рамках судебно-бухгалтерской и судебно-экономической экспертиз, проводимых в комплексе с информационно-технологической и информационно-технической экспертизами.

Полную безопасность компьютерных систем обеспечить чрезвычайно трудно, однако снизить вредные последствия вирусов до определенного уровня можно. Для этого необходимо:

а) применять антивирусные средства;

б) не использовать случайное несертифицированное программное обеспечение, а также нелегальные копии программ для ЭВМ;

в) делать резервные копии программ и системных файлов, а также контролировать доступ к компьютерным системам;

г) проверять каждую приобретенную программу (дискету) на возможную зараженность компьютерным вирусом;

е) регулярно записывать программы, устанавливаемые в компьютерную систему, и др.

Ищенко Е.П., Топорков А.А. Криминалистика: Учебник. Изд. 2-е, испр. и доп./
Под ред. доктора юридических наук, профессора Е.П. Ищенко —
"Инфра-М", 2005 г.

> В диспозиции ст. 273 УК не содержится указания на неосторожность, и, следовательно, в соответствии с ч. 2 ст. 24 УК действия могут совершаться как умышленно, так и по неосторожности. Однако включение в диспозицию признака "заведомости" для виновного вредных последствий исключает неосторожность в качестве формы вины в данном преступлении. Вместе с тем ограничивать субъективную сторону только прямым умыслом тоже, вероятно, не стоит. Возможны случаи, когда лицо не желает, но сознательно допускает наступление последствий или безразлично к ним относится.
>
> Курс уголовного права. Том 4. Особенная часть
> (под ред. доктора юридических наук, профессора Г.Н.Борзенкова
> и доктора юридических наук, профессора В.С.Комиссарова) —
> М.: ИКД "Зерцало-М", 2002

> В данной статье УК РФ речь идет не только о программах, записанных на машинных носителях, но и о записях программ на бумаге. Это обусловлено тем, что процесс создания программы для ЭВМ зачастую начинается написанием ее текста с последующим введением его в память ЭВМ или без такового. С учетом этого наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности по ст. 273 УК РФ… Использование вредоносной программы для ЭВМ для личных нужд (например, для уничтожения собственной компьютерной информации) не наказуемо.
>
> А. Г. Волеводз "Российский судья", 2002, № 9.

В начале 1990-х годов, когда "Лаборатория Касперского" только-только зарождалась, максимально быстрое препарирование вирусов и выработка вакцины были главным, если не решающим аргументом в борьбе за потребителя. В дальнейшем приоритеты (такова жизнь) сместились в сторону качества и надежности соответствующего ПО, а также уровня сервиса. Но революционному духу Касперского явно претили такие нудные задачи повседневного постепенного совершенствования. И, надо сказать, он себе не изменил, продолжая плодотворно работать в том направлении, где заслуженно получил мировое признание.

Вот как описывает Евгений Касперский свой рабочий день (Bugtraq.Ru, 2003): "Ничего особенного. Континенты я не двигаю и судьбами мира не распоряжаюсь. Прихожу, сажусь за компьютер и "долбаю" вирусы. У нас даже есть такой термин для коллег-вирусологов — "дятел". "Дятел" — это тот, кто долбает вирусы. Получается, я главный :) Вообще, это затягивает. Ведь каждый вирус — своего рода задача. Иногда попадаются очень сложные задачи. И нахождение решения — как курение. Начнешь один раз и потом уже не остановиться".

Нет, не правы недоброжелатели, сваливая всю вину за просчеты компании на Евгения Касперского. "Если серьезно, быть брендом не только не очень приятно, но и тяжело. Чем больше известность, тем больше от тебя требуют, тем больше приходится работать…" (из интервью Е. Касперского журналу "Свой бизнес", июнь 2005 г.)

> "Я параноик, это профессиональное заболевание борцов с вирусами".
>
> Из интервью Die Welt (Германия, март 2004 г.)

> "Я совершенно серьезно уверен, что успех "Лаборатории" состоит именно в превосходстве технологий, оперативной реакции на новые угрозы и человеческом отношении к пользователю. В пятой версии антивируса, извините за нескромность, имени меня, будет решена основная проблема существующей версии — скорость работы и требовательность к системным ресурсам. Мы внедрили наши новые технологии ускорения проверки, которые позволяют увеличить производительность в три раза. Учитывая, что сегодня мы идем наравне по этому показателю с крупнейшими конкурентами, "пятерка" будет очень сильным ударом по их рыночным позициям."
>
> Из интервью Bugtraq.Ru (декабрь 2003 г.)

> Говоря про другие антивирусные программы, я могу ошибаться: не надо воспринимать мое мнение как мнение компании — это мое личное мнение антивирусного эксперта, которое может не совпадать с другими мнениями — компаний и других антивирусных экспертов. NOD32 — очень удобная, очень быстрая антивирусная программа, которая очень плохо ловит вирусы. Регулярно получает награды "VB 100%", поскольку "заточена" на получение этих наград. В реальной жизни очень часто пропускает случаи заражения. Пользуется популярностью среди пользователей, которые эффективность антивирусной программы определяют по красоте интерфейса. Не пользуется популярностью среди системных администраторов, которые разбираются, что к чему. Dr.Web — к сожалению, как мне кажется, разработчики Dr.Web не

понимают, что программный продукт отличается от файла на диске. Программа сама по себе является, наверное, пятой частью продукта. Вторая важная отличительная черта Dr.Web — количество ложных срабатываний. Мы тестировали различные антивирусные программы на огромной коллекции чистых файлов, и Dr.Web показал "лучшие" результаты — он определил наибольшее число чистых файлов как зараженных."

Из интервью интернет-изданию "Газета.Ru" (апрель 2004 г.)
http://www.gazeta.ru/avp.shtml

"За рубежом продавать, безусловно, сложнее. Этому есть несколько причин. Во-первых, мы российская компания, а западные заказчики еще не избавились от синдрома "холодной войны". Да, мы для них — бывший "враг номер один". Бывший, но враг. Периодически мы сталкиваемся с мнением, что "Россия — это подозрительно". Естественно, масла в огонь подливают и конкуренты, иногда ведя нечестную борьбу за заказчиков. Приходится пробивать эту стену и доказывать им, что мы не то, что они думают. Во-вторых, в России еще не сформировался класс профессиональных и опытных ИТ-управленцев, способных продвигать программные продукты на Западе. У нас есть талантливые менеджеры, но их явно недостаточно".

Из интервью газете "Ведомости" (март 2002 г.),
Евгений Касперский, Наталья Касперская

Евгений Касперский — настоящий непримиримый революционер, подобный Сен-Жюсту, для которого идея справедливости была превыше всего. Невольно в памяти всплывают слова известного поэта-философа Максимилиана Волошина, много времени посвятившего изучению архивов Великой Французской революции и по сути предсказавшего катаклизмы революции 1917 г., кровавые трагедии гражданской войны и террор 1930-х годов.

"Пароксизм идеи справедливости — это безумие революций, — пишет Максимилиан Волошин. — В гармонии мира страшны не те казни, не те убийства, которые совершаются во имя злобы, во имя личной мести, во имя стихийного звериного чувства, а те, которые совершаются во имя любви к человечеству и человеку. Только пароксизм любви может создать инквизицию, религиозные войны и террор".

Однако справедливость тоже бывает разной, оттого и разные масштабы последствий непримиримой борьбы за эту идею. "Робеспьер справедливость поставил выше божества и этим сделал ее мещанской, — продолжает свою мысль Волошин. — У Марата и у сентябрьских убийц была справедливость самая непоследовательная, так как ее критерием служит личная страсть. Справедливость Дантона — справедливость во имя Родины — справедливость жестокая, но целесообразная… Справедливость жирондистов — справедливость во имя человечества, обманчивая справедливость Руссо… Но самая страшная справедливость — справедливость Сен-Жюста — справедливость во имя справедливости… Сен-Жюст — воплощение абсолютной идеи справедливости, которая в самом звуке его имени отметила свое появление на земле".

Разящий меч революций в руках Касперского — скорее уже символ прошлого. Взвешенный, обстоятельный подход Дмитрия Ивановича Менделеева, считавшего себя "постепеновцем" и в "Заветных мыслях" (1904—1905) изложившего свой план государственного переустройства России, внушает куда больше доверия. Всем нам не стоит забывать мудрые слова Максимилиана Волошина: "У статуи Справедливости в руках меч. У статуи Справедливости глаза всегда завязаны, а одна чаша весов всегда опущена!"

Единый центр — всемирный сейф

Компании-разработчики ПО давно уже приучили пользователей своих продуктов к тому, что принятие лицензионного соглашения автоматически означает отказ от любых претензий к фирме-производителю. Фактически разрешается легально работать с программным продуктом только в том случае, если подписался под словами: "Претензий не имел, не имею и никогда иметь не буду". Обычно с этим диктатом как-то еще удается мириться, но в случае антивирусного ПО острота проблемы стократно возрастает.

Пожалуй, не правы те, кто обвиняет антивирусные компании в стремлении к необузданной наживе и намерении построить свой бизнес непременно на несчастьях других людей. В конечном счете эти фирмы делают благое дело, предлагая "лекарства" страждущим. Плохо то, что каждая из них обязательно хочет выделиться своим "особым" видением вирусных угроз, своими "особыми" подходами к диагностике и лечению, чаще всего заканчивающемуся"ампутацией".

Мировой рынок фармацевтики достиг той стадии зрелости, при которой выпуск новых лекарств находится под государственным контролем и жестко регламентируется. В случае же антивирусных компаний, предлагающих свое компьютерное "зелье" прямо с пылу с жару, ничего подобного не наблюдается.

Луис Герстнер, легендарный глава IBM, поднявший корпорацию буквально с колен после страшного кризиса середины 1990-х годов, был человеком бизнеса, но новичком в ИТ-индустрии. Как Герстнер признается в своих мемуарах, когда он встал у руля Голубого гиганта, его больше всего поразило отсутствие в компьютерной отрасли собственной влиятельной профессиональной ассоциации... А вот антивирусные компании и сейчас продолжают жить, как в период анархического безвластия, никому не подконтрольные и ни за что не отвечающие.

Разумеется, время внесет свои коррективы: на смену хаосу либо придет жесткая централизация в лице яркого лидера (очевидно, Microsoft), либо рынок антивирусных средств станет все больше походить на мировой фармацевтический рынок.

Стив Чанг, основатель и глава антивирусной компании Trend Micro, пару лет назад сказал такие слова: "Видение Trend Micro состоит в построении единого центра (буквально: всемирного сейфа, World safe) для обмена электронной информацией". В самом деле, идея напрашивается сама собой, но боюсь, что придется еще очень долго ждать ее воплощения в глобальном масштабе.

В то же время проблему произвола антивирусных компаний в значительной мере могла бы решить государственная надзорная организация, отслеживающая исполнение стандартов и регулирующая отношения производителя и потребителя на подконтрольной ей территории. Увы, подобного национального центра антивирусной безопасности у нас пока нет. Более того, нет даже единого национального реестра вирусной инфекции. Что же, остается лишь надеяться на честность и бескорыстие безжалостных борцов с вирусной опасностью и уповать на эффективность народного самолечения.