ФЕНОМЕН КОМПЬЮТЕРНЫХ ВИРУСОВ

Д.В. Ращупкин[1] , В.С. Оскерко[2]

[1] - студент 1 курса, факультета МЭО, группы УВЭД-5, Белорусского государственного экономического университета

[2] - научный руководитель, доцент кафедры информационных технологий, Белорусского государственного экономического университета, Минск, 220672, Партизанский пр., 26, тел. (8017) 249-19-81, e-mail: oskerko@bseu.minsk.by.

Аннотация. Работа посвящена явлению компьютерных вирусов как таковому и их месту в мире персональных компьютеров. Кроме того, дана классификация основных видов вирусов.

Ключевые слова: Вирусы, пользователи, компьютерные сети, борьба с вирусами.

1.Введение

Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются сотни (или тысячи) специалистов в десятках (а может быть, сотнях) компаний. Казалось, бы, тема эта не настолько сложна и актуальна, чтобы быть объектом такого пристального внимания.

Однако это не так. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

При этом следует иметь в виду, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов. Примерно так же плохо обстоят дела на другой стороне тандема «человек-компьютер». Как пользователи, так и профессионалы-программисты часто не имеют даже навыков «самообороны», а их представления о вирусе порой являются настолько поверхностными, что лучше бы их (представлений) и не было.

Немногим лучше обстоят дела на Западе, где и литературы побольше (издается аж три ежемесячных журнала, посвященных вирусам и защите от них), и вирусов поменьше (поскольку «левые» китайские компакт-диски особо на рынок не поступают), и антивирусные компании ведут себя активнее (проводя, например, специальные конференции и семинары для специалистов и пользователей).

У нас же, к сожалению, все это не совсем так. И одним из наименее »проработанных» пунктов является литература, посвященная проблемам борьбы с вирусами. На сегодняшний день имеющаяся на прилавках магазинов печатная продукция антивирусного толка либо давно устарела, либо написана непрофессионалами, либо авторами типа Хижняка, что гораздо хуже.

Довольно неприятным моментом является также опережающая работа Российского компьютерного «андеграунда»: только за два года было выпущено более десятка электронных номеров журнала вирусописателей «Infected Voice», появилось несколько станций BBS и WWW-страниц, ориентированные на распространение вирусов и сопутствующей информации.

Все это и послужило толчком к тому, чтобы собрать воедино весь материал, который скопился у меня за восемь лет профессиональной работы с компьютерными вирусами, их анализа и разработке методов обнаружения и лечения.

2. Явление компьютерных вирусов

20-е столетие, несомненно, является одним из поворотных этапов в жизни человечества. Как сказал один из писателей-фантастов, «человечество понеслось вперед, как подстегнутая лошадь», и, определив себя как технократическую цивилизацию, все свои силы наши деды, отцы и мы сами бросили на развитие техники в самых разных ее обличиях - от медицинских приборов до космических аппаратов, от сельскохозяйственных комбайнов до атомных электростанций, от транспорта до систем связи, - список бесконечен, поскольку крайне сложно привести область деятельности человечества, не затронутую развитием техники.

Что являлось причиной столь широкомасштабного и стремительного развития - военное противостояние политических систем, эволюционное «поумнение» человека или его патологическая лень (изобрести колесо, дабы не таскать мамонта на плечах) - пока неясно. Оставим эту загадку для историков последующих столетий.

Человечество захвачено техникой и уже вряд ли откажется от удобств, предоставляемых ею (мало кто пожелает поменять современный автомобиль на гужевую тягу). Уже очень многими напрочь забыта обычная почта с ее конвертами и почтальонами - вместо нее пришла электронная почта с ее ошеломляющей скоростью доставки (до нескольких минут вне зависимости от расстояния) и очень высокой надежностью. Не представляю себе существования современного общества без компьютера, способного многократно повысить производительность труда и доставить любую мыслимую информацию (что-то вроде принципа «пойди туда, не знаю куда, найди то, не знаю что»). Уже не удивляемся мобильному телефону на улице - я и сам к нему привык всего за один день.

20-е столетие также является одним из самых противоречивых, принесших истории человечества немало парадоксов, основной из которых, как мне кажется, является отношение человека к природе. Перестав жить в дружбе с природой, победив ее и доказав себе, что легко может ее уничтожить, человек вдруг понял, что погибнет и сам, - и поменялись роли в драме »Человек-Природа».

Раньше человек защищал себя от природы, теперь же он все больше и больше защищает природу от самого себя. Другим феноменом 20-го века является отношение человека к религии. Став технократом, человек не перестал верить в Бога (или его аналогов). Более того, появились и окрепли другие религии.

К основным техническим феноменам 20-го века относятся, на мой взгляд, появление человека в космосе, утилизация атомной энергии вещества, грандиозный прогресс систем связи и передачи информации и, конечно же, ошеломляющее развитие микро- и макро-компьютеров. И как скоро появляется упоминание о феномене компьютеров, так тут же возникает еще один феномен конца нашего столетия - феномен компьютерных вирусов.

Быть может, многим покажется смешным или легкомысленным то, что факт возникновения компьютерных вирусов поставлен в один ряд с исследованиями космоса, атомного ядра и развитием электроники. Возможно, что я не прав в своих рассуждениях, однако дайте возможность объясниться.

Во-первых, компьютерные вирусы - это серьезная и довольно заметная проблема, возникновения которой никто не ожидал. Даже всевидящие фантасты-футурологи прошлого не говорят об этом ничего (насколько это мне известно). В их многочисленных произведениях с той или иной точностью предсказаны практически все технические достижения настоящего (вспомним, например, Уэллса с его идеей

полета из пушки на Луну и марсиан, вооруженных неким подобием лазера). Если же говорить о вычислительных машинах, то тема эта вылизана донельзя - однако нет ни одного пророчества, посвященного компьютерным вирусам. Тема вируса в произведениях писателей появилась уже после того, как первый реальный вирус поразил свой первый компьютер.

Во-вторых, компьютерные вирусы - это первая вполне удачная попытка создать жизнь. Попытка удачная, но нельзя сказать, что полезная - современные компьютерные «микроорганизмы» более всего напоминают насекомых-вредителей, приносящих только проблемы и неприятности.

Но все-таки - жизнь, поскольку компьютерным вирусам присущи все атрибуты живого - способность к размножению, приспособляемости к среде, движению и т.д. (естественно, только в пределах компьютеров - так же как все вышесказанное верно для биологических вирусов в пределах клеток организма). Более того, существуют «двуполые» вирусы (см. вирус RMNS), а примером «многоклеточности» могут служить, например, макро-вирусы, состоящие из нескольких независимых макросов.

И, в-третьих, тема вирусов стоит несколько особняком от всех остальных задач, решаемых при помощи компьютера (забудем о таких специфичных задачах, как взлом защиты от копирования и криптографию). Практически все проблемы, решаемые при помощи вычислительной техники, являются продолжением целенаправленной борьбы человека с окружающей его природой. Природа ставит человеку длинное нелинейное дифференциальное уравнение в трехмерном пространстве - человек набивает компьютер процессорами, памятью, обвешивает пыльными проводами, много курит и в итоге решает это уравнение (или пребывает в состоянии уверенности, что решил). Природа дает человеку кусок провода с вполне определенными характеристиками - человек придумывает алгоритмы передачи как можно большего объема информации по этому проводу, терзает его модуляциями, сжимает байты в биты и терпеливо ждет сверхпроводимости при комнатной температуре. Природа (в лице фирмы IBM) дает человеку очередное ограничение в виде очередной версии IBM PC - и человек не спит ночами, опять много курит, оптимизируя коды очередной базы данных, дабы уместить ее в предоставленные ему ресурсы оперативной и дисковой памяти. И так далее.

А вот борьба с компьютерными вирусами является борьбой человека с человеческим же разумом (в некотором смысле тоже проявлением природных сил, хотя на этот счет имеется более одного мнения). Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди. Они придумывают новый вирус - а нам с ним разбираться. Затем они придумывают вирус, в котором разобраться очень тяжело - но мы с ним разбираемся. И сейчас наверняка где-то сидит за компьютером парень, который не глупее меня, страдающий над очередным монстром, в котором мне придется разбираться целую неделю, а потом еще одну неделю отлаживать алгоритм антивируса. Кстати, чем не эволюция живых организмов?

Итак, появление компьютерных вирусов - один из наиболее интересных моментов в истории технического прогресса 20-го века, и настал момент закончить с околофилософскими рассуждениями и перейти к конкретным вопросам. И вопрос об определении понятия «компьютерный вирус» будет стоять на первом месте.

Так что же такое компьютерный вирус?

3. Объяснение для домохозяйки

Объяснение будет дано на примере клерка, работающего исключительно с бумагами. Идея такого объяснения принадлежит Д.Н.Лозинскому, одному из известнейших «докторов».

Представим себе аккуратного клерка, который приходит на работу к себе в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий, которые он должен выполнить за рабочий день. Клерк берет верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает «отработанный» лист в мусорное ведро и переходит к следующему листу. Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку бумаг лист, на котором написано следующее:

«Переписать этот лист два раза и положить копии в стопку заданий соседей»

Что сделает клерк? Дважды перепишет лист, положит его соседям на стол, уничтожит оригинал и перейдет к выполнению второго листа из стопки, т.е. продолжит выполнять свою настоящую работу. Что сделают соседи, являясь такими же аккуратными клерками, обнаружив новое задание? То же, что и первый: перепишут его по два раза и раздадут другим клеркам. Итого, в конторе бродят уже четыре копии первоначального документа, которые и дальше будут копироваться и раздаваться на другие столы.

Примерно так же работает и компьютерный вирус, только стопками бумаг-указаний являются программы, а клерком - компьютер. Так же как и клерк, компьютер аккуратно выполняет все команды программы (листы заданий), начиная с первой. Если же первая команда звучит как «скопируй меня в две другие программы», то компьютер так и сделает, - и команда-вирус попадает в две другие программы. Когда компьютер перейдет к выполнению других »зараженных» программ, вирус тем же способом будет расходиться все дальше и дальше по всему компьютеру.

В приведенном выше примере про клерка и его контору лист-вирус не проверяет, заражена очередная папка заданий или нет. В этом случае к концу рабочего дня контора будет завалена такими копиями, а клерки только и будут что переписывать один и тот же текст и раздавать его соседям - ведь первый клерк сделает две копии, очередные жертвы вируса - уже четыре, затем 8, 16, 32, 64 и т.д., т.е. количество копий каждый раз будет увеличиваться в два раза.

Если клерк на переписывание одного листа тратит 30 секунд и еще 30 секунд на раздачу копий, то через час по конторе будет «бродить» более 1.000.000.000.000.000.000 копий вируса! Скорее всего, конечно же, не хватит бумаги, и распространение вируса будет остановлено по столь банальной причине.

Как это ни смешно (хотя участникам этого инцидента было совсем не смешно), именно такой случай произошел в 1988 году в Америке - несколько глобальных сетей передачи информации оказались переполненными копиями сетевого вируса (вирус Морриса), который рассылал себя от компьютера к компьютеру. Поэтому «правильные» вирусы делают так:

«Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них еще нет этого листа».

Проблема решена - «перенаселения» нет, но каждая стопка содержит по копии вируса, при этом клерки еще успевают справляться и с обычной работой.

«А как же уничтожение данных?» - спросит хорошо эрудированная домохозяйка. Все очень просто - достаточно дописать на лист примерно следующее:

«1. Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них еще нет этого листа. 2. Посмотреть на календарь - если сегодня пятница, попавшая на 13-е число, выкинуть все документы в мусорную корзину»

Примерно это и выполняет хорошо известный вирус «Jerusalem» (другое название - «Time»).

Кстати, на примере клерка очень хорошо видно, почему в большинстве случаев нельзя точно определить, откуда в компьютере появился вирус. Все клерки имеют одинаковые (с точностью до почерка) КОПИИ, но оригинал-то с почерком злоумышленника уже давно в корзине!

Вот такое простое объяснение работы вируса. Плюс к нему хотелось бы привести

две аксиомы, которые, как это ни странно, не для всех являются очевидными:

Во-первых, вирусы не возникают сами собой - их создают очень злые и нехорошие программисты-хакеры и рассылают затем по сети передачи данных или подкидывают на компьютеры знакомых. Вирус не может сам собой появиться на Вашем компьютере - либо его подсунули на дискетах или даже на компакт-диске, либо Вы его случайно скачали из компьютерной сети передачи данных, либо вирус жил у Вас в компьютере с самого начала, либо (что самое ужасное) программист-хакер живет у Вас в доме.

Во-вторых: компьютерные вирусы заражают только компьютер и ничего больше, поэтому не надо бояться - через клавиатуру и мышь они не передаются.

4.Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

По СРЕДЕ ОБИТАНИЯ вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии.

Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая ОПЕРАЦИОННАЯ СИСТЕМА (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д. Макро-вирусы заражают файлы форматов Word, Excel, Office97. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

РЕЗИДЕНТНЫЙ вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и

являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

В многозадачных операционных системах время «жизни» резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование СТЕЛС-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ — запрет вызовов меню просмотра макросов.

Один из первых файловых стелс-вирусов — вирус «Frodo», первый загрузочный стелс-вирус — «Brain».

САМОШИФРОВАНИЕ и ПОЛИМОРФИЧНОСТЬ используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса.

Полиморфик-вирусы (polymorphic) - это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные НЕСТАНДАРТНЫЕ ПРИЕМЫ часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ вирусы можно разделить на:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков (например, вполне безобидный на первый взгляд вирус «DenZuk» довольно корректно работает с 360K дискетами, но может уничтожить информацию на дискетах большего объема). До сих пор попадаются вирусы, определяющие «COM или EXE» не по внутреннему формату файла, а по его расширению. Естественно, что при несовпадении формата и расширения имени файл после заражения оказывается неработоспособным. Возможно также «заклинивание» резидентного вируса и системы при использовании новых версий DOS, при работе в Windows или с другими мощными программными системами. И так далее.

5. Заключение

А что же будет дальше? И как долго вирусы будут нас беспокоить? - вопросы, который в той или иной мере беспокоит практически всех пользователей.

Чего ожидать от компьютерного андеграунда в последующие годы? Скорее всего основными проблемами останутся:

1) полиморфик-DOS-вирусы, к которым добавятся проблемы полиморфизма в макро-вирусах и вирусах для Windows и OS/2;
2) макро-вирусы, которые будут находить все новые и новые приемы заражения и скрытия своего кода в системе;
3) сетевые вирусы, использующие для своего распространения протоколы и команды компьютерных сетей.

Пункт 3) находится пока только на самой ранней стадии - вирусы делают первые робкие попытки самостоятельно распространять свой код по MS Mail и пользуясь ftp, однако все еще впереди.

Не исключено, что появятся и другие проблемы, которые принесут немало неприятностей пользователям и достаточное количество неурочной работы разработчикам антивирусных программ. Однако я смотрю на будущее с оптимизмом: все проблемы, когда-либо вставшие в истории развития вирусов, были довольно успешно решены. Скорее всего так же успешно будут решаться и будущие проблемы, пока еще только витающие идеями в воспаленном разуме вирусописателей.

Что будет послезавтра и как долго вообще будут существовать вирусы? Для того, чтобы ответить на этот вопрос следует определить, где и при каких условиях водятся вирусы.

Основная питательная среда для массового распространения вируса в ЭВМ, на мой взгляд, обязана содержать следующие необходимые компоненты:

- незащищенность операционной системы (ОС);
- наличие разнообразной и довольно полной документации по ОС и «железу»;
- широкое распространение этой ОС и этого «железа».

Следует отметить, что понятие операционной системы достаточно растяжимое. Например, для макро-вирусов операционной системой являются редакторы Word и Excel, поскольку именно редакторы, а не Windows предоставляют макро-вирусам (т.е. программам на Бейсике) необходимые ресурсы и функции.

Если в операционной системе присутствуют элементы защиты информации, как это сделано практически во всех ОС, вирусу будет крайне трудно поразить объекты своего нападения, так как для этого потребуется (как минимум) взломать систему паролей и привилегий. В результате работа, необходимая для написания вируса, окажется по силам только профессионалам высокого уровня (вирус Морриса для VAX - пример этому). А у профессионалов, на мой взгляд, уровень порядочности все-таки намного выше, чем в среде потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов еще более сократится.

Для массового производства вирусов также необходимо и достаточное количество информации о среде их обитания. Какой процент от числа системных программистов, работающих на мини-ЭВМ в операционках UNIX, VMS и т.д. знает систему управления процессами в оперативной памяти, полные форматы выполняемых файлов и

загрузочных записей на диске? (т.е. информацию, необходимую для создания вируса). И следовательно, какой процент от их числа в состоянии вырастить настоящего полноценного зверя?

Другой пример - операционная система Novell NetWare, достаточно популярная, но крайне слабо документированная. В результате мне пока не известно ни одного вируса, поразившего выполняемые файлы Novell NetWare, несмотря на многочисленные обещания вирусописателей выпустить такой вирус в ближайшее время.

Ну а по поводу широкого распространения ОС как необходимого условия для вирусного нашествия и говорить надоело: на 1000 программистов только 100 способны написать вирус, на эту сотню приходится один, который эту идею доведет до завершения. Теперь полученную пропорцию умножаем на число тысяч программистов - и получаем результат: с одной стороны 15.000 или даже 20.000 полностью IBM-совместимых вирусов, с другой - несколько сот вирусов для Apple-Macintosh. Такое же несоответствие пропорций наблюдается и в сравнении общего количества вирусов для Windows (несколько десятков) и для OS/2 (несколько штук).

Приведенным выше трем условиям «расцвета» компьютерных вирусов удовлетворяют сразу несколько OS (включая редакторы), производимых фирмой Microsoft (DOS, Windows, Win95/NT и Word, Excel, Office97), что дает благодатную почву для существования самых разнообразных файловых и макро-вирусов. Удовлетворяют приведенным условиям также и стандарты разбиения жестких дисков. Результат - разнообразные варианты загрузочных вирусов, поражающих систему в момент ее загрузки.

Для того, чтобы прикинуть продолжительность нашествия компьютерных вирусов в какой-либо ОС, надо оценить время сосуществования приведенных выше необходимых условий.

Довольно очевидно, что в обозримом будущем фирмы IBM и Apple не собираются уступать массовый рынок своим конкурентам (на радость Apple- и IBM-программистам), даже если для этого этим фирмам придется объединить усилия.

Не представляется возможным и усечение потока информации по наиболее распространенным системам, так как это ударит по числу приложений для них, а, следовательно, и по их «продаваемости».

Остается только одно - защита ОС. Однако, защищенность ОС требует исполнения некоторых правил (паролей и т.п.), что приводит к ряду неудобств.

Поэтому мне кажется маловероятным, что такие ОС станут популярными в среде обычных пользователей - секретарш, бухгалтеров, на домашних компьютерах, и т.д., и т.п., либо функции защиты будут отключаться пользователем еще при установке ОС.

Исходя из вышесказанного можно сделать единственный вывод: вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются.

Список использованных материалов:

1. http://www.symantec.ru/region/ru/product/navbrochure/index.htm
2. http://www.symantec.ru
3. http://www.dials.ru/
4. http://www.avp.ru/
5. http://www2.dialognauka.ru/
6. http://www.apl.ru/isvwsolaris.htm
7. http://www.act.ru/av/Solomon/DrSolom_report.asp