



Антивирусные программы

Армянский научно-исследовательский институт
научно-технической информации
(АрмНИИНТИ)
Республиканская научно-техническая библиотека
(РНТБ)

Ереван - 2000

Автор: . Н. Л. Хачатрян
Научный руководитель:
к.т.н. Р. В. Арутюнян

УДК 681.3.067

ББК 32.973.2-018

В обзоре рассматриваются макровирусы, их происхождение, реальная оценка их угрозы и ущерба, методы защиты от них: алгоритмические, программные и операционно-технические, разработанные в "Лаборатории Касперского" на базе макроязыка VBA, соответствующего международным требованиям.

Приведена сравнительная характеристика некоторых антивирусных утилит.

Macroviruses, their origin, real estimation of their menace and damage, have been considered in this review, as well as methods of protection, such algorithm program, technology and operation methods, developed in "Casper Laboratory", on the basis of VBA macro-language, according to the international standards.

A comparative characteristics of some antivirus utilities, has been adduced.

Տեսության մեջ քննարկվում են մակրովիրուսները, դրանց ծագումը, սպանացող վլանիք և վնասների իրատեսական զնահատականը, դրանցից պաշտպանվելու մեթոդները. ալգորիթմական, ծրագրային և օպերացիոն տեխնոլոգիան, որոնք մշակվել են «Կասպերսկի լաբորատորիայում» միջազգային պահանջներին համապատասխանող VBA մակրոլեզվի հիման վրա: Տրված է մի քանի հակավիրուսային ուժիշտների համեմատական բնութագիրը:

ИНФОРМАЦИОННЫЕ ИЗДАНИЯ АРМНИИНГИ, РНТБ	
N	Наименование издания
1.	Инвестируйте в экономику Армении. Справочник (англ.)
2.	Объективные факторы для инвестирования в экономику РА. Справочник (русск., англ.)
3.	Информация о предприятиях, приватизированных в виде акционерных обществ открытого типа. 1995, 1996, 1997, 1998 гг. (арм., русск., англ.)
4.	Арутюнова Э. Д., Арутюнян Р. В. Бытовые фильтры для доочистки питьевой воды. Аналитический обзор
5.	Геворкян Р. Г. Прогнозная оценка офиолитовой ассоциации на алмаз. Аналитический обзор
6.	Арутюнян Р. В., Саркисян А. П. Основные тенденции в развитии мирового энергетического хозяйства. Аналитический обзор
7.	Лалаян Ж. Е. Утилизация, переработка и хранение радиоактивных отходов. Обзор
8.	Арутюнова Э. Д., Арутюнян Р. В. Пастеризация молока в условиях мелкого хозяйственника-фермера. Информационный обзор
9.	Хачатрян Н. Л., Арутюнян Р. В. XX век в зеркале geopolитики. Аналитический обзор
10.	Мелоян В., Арутюнян Р. В. Раскрывая завесу над колокольным звоном. Обзор
11.	Арутюнян Р. В. Российские производства черных и цветных металлов. Информационный обзор
12.	Арутюнян Р. В. Индустрия гражданской авиации. Обзор
13.	Рак можно победить, но нужно обязательно верить в победу
14.	Հայ գինվորի գրանցան Մատենաշար բողարկումներ թիվ 1-15
15.	Иванова Е. А., Арутюнян Р. В. Технология и оборудование первичной обработки шерсти. Информационный обзор.
16.	Бутейко В. К., Бутейко М. М. Дыхание по Бутейко. Методическое пособие для обучающихся методу волевой ликвидации глубокого дыхания.
17.	Нерсесян И.Г., Арутюнян Р.В. Инновационная деятельность предприятий и венчурный капитал-мощные рычаги для подъема экономики. Обзор.
18.	Иванова Е. А., Арутюнян Р.В. Перспективы развития декоративно-прикладного искусства и народных промыслов в РА. Обзор.
19.	Егиазарян А. В., Арутюнян Р. В. Технология производства красных столовых вин.
20.	Джаганян Э.В., Арутюнян Р.В. Концепция защиты от воздействия информационного оружия. Обзор.
21.	Саркисян А.П., Арутюнян Р.В. Каталитические нейтрализаторы, этилированный и неэтилированный бензин. Обзор.
22.	Хачатрян Н. Л., Арутюнян Р.В. Прогноз роста населения Земли. Обзор.
23.	Цатурян В. А., Арутюнян Р. В. Производство черепицы. Обзор.
24.	Иванова Е. А. Финансовый и экономический кризис в России. Опыт стран мира по выходу из кризиса в XX веке. Обзор.
25.	Нерсесян И. Г., Реалии каспийской нефти. Обзор.
26.	Саркисян А. П., Маркетинг и система дилерской продажи автомобилей.
27.	Сборник рефератов НИР и ОКР (русский, английский).
28.	Иванова Е. А. Кожевенно-обувная промышленность Армении. Обзор.
29.	Джаганян Э.В., Арутюнян Р. В. Государственная политика в области сохранения рекреационных ресурсов. Обзор.
30.	Егиазарян А. В., Арутюнян Р.В. Добыча камня промышленными способами.
31.	Егиазарян А. В., Арутюнян Р.В. Ферментация табака. Обзор.
32.	Иванова Е. А., Арутюнян Р.В. Финансы и экономика Армении в 1999году. Рынок капитала. Обзор.
33.	Нерсесян И. Г., Арутюнян Р.В. Основные направления развития и поддержания науки в странах ЕС. Обзор.
34.	Саркисян А.П., Арутюнян Р.В. Роль образования и науки в обществе. Обзор.
35.	Джаганян Э. В., Арутюнян Р. В. Косовский кризис - полигон информационной войны. Обзор.

ISBN 99930-3-027-9

© Лрату

Введение

Вирус представляет собой программу, которая несанкционированно проникает в компьютер и выполняет в нем определенные действия. Сложность борьбы с вирусом заключается в том, что часто он размножается быстрее, чем его успевают обнаружить и обезвредить. Самые опасные вирусы начинают работать только после того, как создадут определенное число собственных копий.

Своим названием компьютерные вирусы обязаны определенному сходству с вирусами естественными: они обладают высокой скоростью распространения, избирательностью, т.е. способностью поражать определенные участки, иногда способностью заражать всю систему.

Большинство вирусов паразитирует на конкретных программах или файлах, гарантированно присутствующих в системе. Зараженный компьютер сообщает, что ему не хватает памяти, заявляет о сбое в работе программ, перестает выполнять команды, на дисплее возникают непонятные надписи (иероглифы) и т.д.

Защита не позволит вирусу проникнуть в компьютер. Если же он каким-то образом все-таки туда попал, антивирусная программа его обнаружит и по команде уничтожит. Конечно, остается опасность появления новых вирусов, еще неизвестных разработчикам антивирусной продукции, но, с другой стороны, она постоянно обновляется.

Вирусы делятся на несколько видов. Так называемые вирусы загрузочного сектора заражают ту область диска, на которой расположены файлы, необходимые для загрузки компьютера. Однако нацеленность вирусов на системные программы облегчает борьбу с заразой: все они сосредоточены на одном участке диска. Поэтому и вирус легче найти.

Макровирусы — самые распространенные и заразные. Они быстро распространяются, действуют на различные участки системы и способны вредить на всех уровнях вычислительной среды, будь то домашний персональный компьютер, компьютерная станция в офисе, сервер или шлюз Интернета.

Однако у всех компьютерных вирусов есть одно существенное отличие от вирусов естественных. Они появляются не сами по себе, а создаются хакерами — компьютерщиками-профессионалами, фанатично увлеченными своим делом.

В последнее время хакеры серьезно заинтересовались компьютерными вирусами как одним из наиболее эффективных и безликих способов внедрения в чужие компьютерные системы. Для многих из них нелегальное проникновение в чужие владения стало своего рода наркотиком.

Большинство сложнейших вирусов было создано исключительно из спортивного интереса. Написать самый современный вирус, максимально затруднить его обнаружение и обезвреживание для хакера то же, что для альпиниста — покорить новую горную вершину.

Впрочем, вирусы могут создавать и компьютерные хулиганы, преследующие корыстные цели, например, разрушить компьютерную систему конкурирующей фирмы.

Ну и, наконец, есть вирусы, которые используются в целях шпионажа. Проникая в чужой компьютер, они могут вскрыть пароли и коды и просмотреть чужую почту или скачать всю информацию из чужого компьютера.

Появление Интернета и расширение круга его пользователей придало проблеме вирусов глобальный характер (1).

Антивирусные программы лаборатории Касперского

Скоро исполняется пять лет как название "макровирус" прочно вошло в лексикон компьютерных пользователей всего мира. Несмотря на разработку надежных средств защиты против этой "заразы" и многочисленные обзоры методов борьбы с ней, это словосочетание до сих пор заставляет миллионы пользователей содрогаться и запускать на всякий случай антивирусные сканеры. Что же такое макровирусы, чем они отличаются от других представителей компьютерной "фауны" и есть ли средства защиты против них?

Макровирусы являются разновидностью компьютерных вирусов, созданной при помощи специальных макроязыков, встроенных в популярные офисные приложения наподобие Word, Excel, Access, PowerPoint, CorelDraw! и др.

Макроязыки используются для написания специальных программ (макросов) для повышения эффективности работы в этих приложениях.

Например, с помощью макроса Word можно автоматизировать процесс заполнения и рассылки факсов. Пользователю достаточно будет только ввести данные в поля формы и нажать на кнопку – все остальное макрос сделает сам.

Таким образом, использование макросов позволяет максимально упростить и автоматизировать работу. Проблема заключается в том, что это можно сделать незаметно для пользователя. Более того, можно незаметно совершить гораздо более опасные действия: изменить содержание документа, стереть файл или директорию. Вредоносные макросы, обладающие способностью создавать свои копии и совершающие некоторые действия без ведома пользователя, и называются макровирусами.

Функциональные возможности этого типа вирусов ограничены возможностями макроязыков, с помощью которых они созданы. Именно с помощью этих языков они размножаются, распространяются, наносят вред зараженным компьютерам.

Таким образом, чем более продвинутый макроязык, тем более хитрыми, изощренными и опасными могут быть макровирусы. Наиболее распространенный макроязык Visual Basic for Applications (VBA) предоставляет вирусам наиболее полный спектр возможностей. Причем, с каждой новой версией эти возможности стремительно расширяются. Таким образом, чем более совершенными будут офисные приложения, тем опаснее будет становиться работа в них.

Первый макровирус для MS Word "Concept" заявил о себе в августе 1995г., когда все прогрессивное человечество праздновало торжественный запуск Windows 95 и очередной версии MS Office. В считанные дни вирус вызвал настоящую пандемию, заразив десятки тысяч компьютеров по всему миру и прочно заняв первое место в статистических отчетах различных научно-исследовательских организаций и компьютерных изданий. Важно отметить, что многие антивирусные компании оказались просто не готовы к такому повороту событий и им пришлось вносить значительные изменения в используемые антивирусы "движки" или вообще заново их создавать.

В июле 1996 г. в "диком виде" обнаружен первый макровирус для MS Excel – "Laroux", практически одновременно парализовавший работу двух нефтедобывающих компаний в разных концах земного шара – в ЮАР и на Аляске.

Март 1997 г. ознаменовался появлением макровируса "ShareFun", идея которого была позднее позаимствована недавно осужденным Дэвидом Смитом, автором нашумевшего в конце марта 1999г. вируса Melissa. В ShareFun был

впервые использован метод распространения через электронную почту, посредством рассылки зараженных сообщений почтовой программой MS Mail.

В марте 1998г. жертвой компьютерных вирусов ("Accessi V") пало еще одно офисное приложение – система обработки баз данных MS Access. А в самом конце того же года макровирус "Attach" "сразил" программу создания презентаций MS PowerPoint.

В 1999г. макровирусы продолжили свой "качественный" рост и распространяли свое влияние на файлы графического редактора Corel Draw! (обнаруженный в мае вирус "Gala") и документы планировщика MS Project (вирус "Corner", открытый в конце октября).

Вместе с тем, все в большем количестве стали появляться так называемые многоплатформенные макровирусы, т.е. вирусы, способные внедряться сразу в несколько офисных приложений. Классическим примером тому может служить "Triplicate" – первый известный макровирус, одновременно заражающий документы Word, Excel и PowerPoint. Кроме того, они берут на вооружение все новые уловки для усложнения процедуры их обнаружения и удаления. В первую очередь это – Stealth – технология (уловка, делающая вирус невидимым в зараженном документе) и полиморфизм (модификация, шифрование исходного кода вируса при сохранении его функциональности).

За последние несколько лет макровирусы прочно занимают первые места в списках наиболее распространенных вирусов. По данным Международной ассоциации компьютерной безопасности (www.icsa.net), доля представителей этого класса компьютерной "фауны" в общем числе "диких" вирусов составляет 2/3. Согласно статистике "Лаборатории Касперского", это число меньше (около 55%), однако оно все равно наглядно демонстрирует преобладание макровирусов.

Такая высокая распространенность макровирусов имеет разумное объяснение.

Во-первых, это высокое распространение объектов их поражения, т.е. офисных приложений. Сегодня практически нет таких людей, которые бы не использовали в своей повседневной работе текстовый процессор, электронные таблицы, систему обработки базы данных или мастер-презентаций.

Во-вторых, очень низкий уровень встроенной антивирусной защиты этих приложений. Несмотря на все уверения Microsoft об изменении ситуации в новом MS Office 2000, имеющийся многолетний профессиональный опыт позволяет утверждать обратное: офисные приложения остались столь же уязвимыми для вирусов, как и их предшественники.

В-третьих, простота создания макровирусов.

Для того чтобы написать вирус, например, для MS Word, достаточно изучить азы языка программирования VBA. Несмотря на то, что он является самым простым и доступным среди всех остальных языков, он предоставляет вирусописателям все необходимые рычаги для того, чтобы уничтожить важную информацию и надолго вывести компьютер из строя.

Наконец, в-четвертых, наиболее популярные офисные приложения (в первую очередь из пакета MS Office), как правило, интегрированы с почтовыми программами (например, MS Outlook). Это обстоятельство определяет доступ макровирусов к электронной почте – наиболее удобному и быстрому способу распространения. Таким образом, они имеют неограниченные возможности для молниеносного поражения миллионов компьютеров по всему миру.

Макровирусы представляют реальную угрозу компьютерным пользователям. По прогнозам, одновременно с совершенствованием макроязыков и обнаружением новых "дыр" в системах безопасности офисных приложений макровирусы будут становиться все более неуловимыми и опасными, а скорость их распространения достигнет небывалых величин.

Несмотря на столь мрачные прогнозы, необходимо помнить главное условие борьбы с компьютерными вирусами – не паниковать.

Круглосуточно на страже компьютерной безопасности находятся тысячи высококлассных антивирусных специалистов по всему миру. Их профессионализм многократно превосходит совокупный потенциал всего хакерского движения. За многие годы существования антивирусная индустрия изобрела много способов противодействия компьютерным вирусам. На сегодняшний день выделяется пять основных подходов к обеспечению антивирусной безопасности.

Во-первых, это классический сканер – пионер антивирусного движения, впервые появившийся на свет практически одновременно с самими компьютерными вирусами. Принцип его работы заключается в поиске в файлах, памяти и загрузочных секторах вирусных сигнатур, т.е. уникального программного кода вируса. Здесь возникает первая проблема, потому что малейшие модификации вируса могут сделать его невидимым для сканера.

К примеру, существует несколько десятков вариантов вируса Melissa, и почти для каждого из них приходилось выпускать отдельное обновление антивирусной базы. Последнее обстоятельство означает вторую проблему: время между появлением вируса и выходом соответствующего обновления пользователь оставался практически незащищенным от атак новых вирусов.

Позднее, эксперты придумали и внедрили в сканеры оригинальный способ обнаружения неизвестных вирусов – эвристический анализатор, т.е. анализ кода программы на предмет возможного присутствия в нем компьютерного вируса. Однако данный метод характеризуется высоким уровнем ложных срабатываний (false alarm), недостаточной надежностью и невозможностью вылечить обнаруженные вирусы.

Наконец, третья проблема: антивирусный сканер проверяет файлы только тогда, когда пользователь "попросит" его это сделать, т.е. запустить сканер. Это требует от пользователя постоянного внимания и концентрации. Очень часто он забывает проверить сомнительный, загруженный, например, из Интернета что? и, в результате, своими руками заражает компьютер. Сканер способен определить факт заражения постфактум, т.е. уже после того, как в системе появился вирус.

Для устранения такой возможности был разработан второй вид антивирусных программ – антивирусные мониторы. По своей сути они являются разновидностью сканеров, которые постоянно находятся в памяти компьютера и осуществляют фоновую проверку файлов, загрузочных секторов и памяти в масштабе реального времени. Для включения антивирусной защиты пользователю достаточно загрузить монитор при загрузке операционной системы. Все запускаемые файлы будут автоматически проверяться на вирусы.

Третья разновидность антивирусов - ревизоры изменений (integrity checkers). Их принцип работы основан на снятии оригинальных "отпечатков" (CRC-сумм) с файлов и системных секторов. Эти "отпечатки" сохраняются в базе данных. При следующем запуске ревизор сверяет "отпечатки" с их оригиналами и сообщает пользователю о произошедших изменениях. У этого типа антивирусных

программ тоже есть свои недостатки. Во-первых, ревизоры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время уже после того, как вирус разошелся по компьютеру. Во-вторых, они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из резервной копии или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Этим пользуются некоторые вирусы, которые используют эту "слабость" ревизоров и заражают только вновь создаваемые файлы, оставаясь, таким образом, невидимыми для них. В-третьих, ревизоры требуют регулярного запуска - чем чаще это будет происходить, тем надежнее будет контроль за вирусной активностью.

Необходимо также упомянуть такую разновидность антивирусных программ, как иммунизаторы. Они делятся на два вида: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он принципиален: абсолютная неспособность обнаружить заражение stealth-вирусами (вирусами-невидимками), которые хитро скрывали свое присутствие в зараженном файле.

Второй тип иммунизаторов защищает систему от поражения каким-либо вирусом. Файлы модифицируются таким образом, что вирус принимает их за уже зараженные. Например, чтобы предотвратить заражение СОМ-файла вирусом Jerusalem, достаточно дописать в его конец строку MSDos. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натыкается на нее и считает, что система уже заражена.

Второй тип иммунизации не может быть признан универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов: у каждого из них свои приемы определения зараженности файлов. Однако, несмотря на это, подобные иммунизаторы в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Из-за описанных выше недостатков иммунизаторы не получили большого распространения и в настоящее время практически не используются.

Все перечисленные выше типы антивирусов не решают главной проблемы – защиты от неизвестных вирусов. Таким образом, компьютерные системы оказываются беззащитны перед ними до тех пор, пока антивирусные вендоры не разработают противоядия. Иногда на это требуется до нескольких недель. Все это время компании по всему миру имеют реальную "возможность" потерять важнейшие данные, от которых зависит их будущее.

Однозначно ответить на вопрос "что же делать с неизвестными вирусами?" предстоит лишь в грядущем тысячелетии. Однако уже сейчас можно сделать прогноз относительно наиболее перспективных путей развития антивирусного программного обеспечения. Таким направлением станут так называемые поведенческие блокираторы (behaviour blocker/gandbox). Именно они имеют реальную возможность со 100% -ой гарантией противостоять атакам новых вирусов.

Поведенческий блокиратор – это резидентная программа, которая перехватывает различные события и в случае "подозрительных" действий (действий,

которые может производить вирус или другая вредоносная программа), запрещает это действие или запрашивает разрешение у пользователя. Иными словами, блокиратор совершаet не поиск сигнатурьы, т.е. кода вируса, а отслеживает и предотвращает его действие. Идея блокираторов не нова. Они появились давно, однако эти антивирусные программы не получили широкого распространения из-за сложности настройки, требующей от пользователей глубоких знаний в области компьютерных технологий.

Теоретически поведенческий блокиратор может предотвратить распространение любого как известного, так и неизвестного (написанного после блокиратора) вируса, предупреждая пользователя до того, как вирус заразит другие файлы или нанесет какой-либо вред компьютеру. Но вирусоподобные действия может производить и сама операционная система или полезные утилиты. Поведенческий блокиратор (здесь имеется в виду "классический" блокиратор, который используется для борьбы с файловыми вирусами) не может самостоятельно определить, кто же выполняет подозрительное действие – вирус, операционная система или какая-либо утилита и вынужден спрашивать подтверждения у пользователя. Т.е. в конечном счете решение зачастую принимает пользователь, который должен обладать достаточными знаниями и опытом, чтобы дать правильный ответ. В противном случае ОС или утилита не сможет произвести требуемое действие, либо вирус проникнет в систему. Именно по этой причине блокираторы и не стали популярными: их достоинства зачастую становились их недостатками, они казались слишком навязчивыми своими запросами и пользователи просто удаляли эти программы. Ситуацию сможет исправить лишь приобретение искусственного интеллекта, который сможет самостоятельно разобраться в причинах того или иного подозрительного действия.

Возвращаясь к макровирусам, необходимо заметить, что здесь ситуация совсем иная. Если рассматривать программы, написанные на наиболее распространенном макроязыке VBA, то тут можно с очень большой долей вероятности отличить вредоносные действия от полезных. В конце 1999 г. "Лаборатория Касперского" разработала уникальную систему защиты от макровирусов пакета MS Office (версий 97 и 2000), основанную на новых подходах к принципам поведенческого блокиратора – AVP Office Guard. Благодаря проведенному анализу макровирусов в процессе моделирования их поведения, были определены наиболее часто встречающиеся последовательности их действий. Это позволило внедрить в программу новую, высокоинтеллектуальную систему фильтрации действий макросов и с высокой долей достоверности безошибочно выявлять те из них, которые представляют собой реальную опасность. Именно благодаря этому AVP Office Guard не столь "навязчив". Но, задавая меньше вопросов пользователю, этот блокиратор не стал менее надежным. Используя его, пользователь практически на 100% защищен от макровирусов, как известных, так и еще не написанных.

AVP Office Guard перехватывает и блокирует выполнение даже многоплатформенных макровирусов, т.е. способен работать сразу в нескольких приложениях. Программа одинаково надежно предотвращает их действие в MS Word, Excel, Access (только версия 2000), PowerPoint.

AVP Office Guard контролирует работу макровирусов с внешними приложениями, в том числе с почтовыми программами. Тем самым полностью исключается возможность распространения макровирусов через электронную почту.

Именно таким способом в марте 1999 г. вирусы Melissa и Para поразили десятки тысяч компьютеров по всему миру. AVP Office Guard, в отличие от обычных антивирусов, полностью решает эту проблему блокировкой доступа макросов к электронной почте.

Эффективность блокиратора была бы нулевой, если макровирусы могли бы произвольно отключать его. Именно это является одним из недостатков встроенной в приложения MS Office антивирусной защиты. В AVP Office Guard реализован новейший механизм противодействия атакам макровирусов на него самого, с целью его отключения и устранения из системы. Этот алгоритм делает невозможным снятие антивирусного блокиратора без вмешательства самого пользователя.

Использование AVP Office Guard избавляет пользователя от вечной головной боли по поводу загрузки и подключения новых обновлений антивирусной базы для защиты от новых макровирусов, потому что любой новый макровирус уже по определению будет перехватываться программой. Это означает, что ликвидируется наиболее опасный отрезок времени между появлением вируса и антивируса. Однажды установленный, он надежно защитит компьютер от макровирусов вплоть до выхода новой версии языка программирования VBA с реализацией новых функций, которые могут использоваться для написания вирусов.

Поведенческий блокиратор решает проблему обнаружения и предотвращения распространения макровирусов. Однако, по определению, он не предназначен для их удаления. Именно поэтому его необходимо использовать совместно с антивирусным сканером, который будет способен успешно уничтожить вирус. Блокиратор позволит безопасно переждать период между обнаружением нового вируса и выпуском обновления антивирусной базы для сканера, не прибегая к остановке работы компьютерных систем из-за боязни навсегда потерять ценные данные или серьезно повредить аппаратную часть компьютера.

В 1999 г. уже более 100 компаний – производителей программного обеспечения лицензировали макроязык VBA для использования в своих продуктах. Это означает, что макровирусы из MS Office будут без труда переноситься в новые приложения, которые будут использоваться, а возможно уже используются. Это, несомненно, увеличит угрозу.

Поведенческий блокиратор является на данный момент наиболее эффективным средством решения этой проблемы. С развитием компьютерных технологий, особенно в области разработки элементов искусственного интеллекта, значение, эффективность и простота использования блокираторов будут стремительно возрастать. Именно этот тип антивирусных программ в ближайшее время станет основным средством антивирусной защиты, обеспечивая ее наиболее ответственный передний край – блокировку проникновения и распространения новых, ранее неизвестных вирусов (2).

Макровирусы

До 80% всех заражений компьютерными вирусами приходится на так называемые макровирусы. В отличие от обычных вирусов они "живут" не в исполняемых файлах и загрузочных секторах, а в документах MS Word и пишутся не в машинных кодах, а на встроенном макроязыке WordBasic. Подхватить такой вирус проще простого: достаточно открыть в своем редакторе зараженный документ и макровирус перепишет себя в главный шаблон Normal.dot.

В результате каждый ваш документ будет содержать эту заразу. Все макровирусы перехватывают команды открытия и сохранения документов — это позволяет им внедряться в каждый сохраняемый документ (3).

Приведем краткое истолкование наиболее распространенных вирусов.

Загрузочный вирус. Поражает область дискеты или жесткого диска, в которой хранится информация операционной и файловой систем. Каждый запуск машины с оставленной в дисководе зараженной дискетой может привести к попаданию туда вируса.

Файловый вирус. Внедряется в программные (exe- и com-) файлы. После этого копирует себя при каждом выполнении зараженной программы.

"Дикий вирус". Тот, который реально циркулирует. На сегодня насчитывается около 250 "диких" вирусов.

"Лабораторный вирус". Обитает в основном в стенах исследовательских лабораторий, не сумев включиться в общую циркуляцию. К настоящему времени известно около 1800 "лабораторных" вирусов.

Макровирус. Наиболее распространенный вид вирусов; на долю макровирусов сейчас приходится около 80% всех случаев заражения компьютеров. Макрокоманды Microsoft Word и Excel могут автоматически выполнять определенную последовательность действий при открытии документа. Такая макроМакровирус команда, зараженная вирусом, способна нести вред любому документу Word или Excel, который вы откроете.

Многосторонний вирус. Использует несколько механизмов распространения; наиболее распространенный вариант — комбинация файлового и загрузочного вирусов (файльово-загрузочный вирус).

Полиморфный вирус. Меняет себя всякий раз, когда размножается. Из-за того, что сигнатуры таких вирусов меняются (в ряде случаев произвольным образом), традиционная техника определения вируса по сигнатуре часто не позволяет их выявить; для поиска полиморфных вирусов антивирусные утилиты должны использовать эвристическую.

Стелс-вирус. Использует специальные приемы, чтобы скрыться от антивирусных программ. По большей части стелс-вирусы действуют в DOS(4).

Каких же вирусов следует опасаться в первую очередь? Из 250 с лишним циркулирующих вирусов действительно распространены лишь очень немногие. Вот пять наиболее часто встречающихся.

1. Concept. Первый и самый известный макровирус, поражающий файлы Word; он был разработан с целью доказать жизненность идеи макровируса.

Не причиняет вреда, а проявляется в том, что поражает файл шаблона normal.dot и выводит всплывающее окно с числом 1. Если машина заражена

этим вирусом, он попадает во все файлы, сохраненные в Word как документы Word.

2. Cap. Этот макровирус Word причиняет больше беспокойства, чем вреда; он удаляет все имеющиеся макрокоманды и заменяет их собственными. Cap. — мутирующий вирус и поэтому продолжает менять макросы все то время, в течение которого активен. Удалить его несложно, но восстановление уничтоженных им макрокоманд может оказаться трудоемким.

3. Wazzu. Макровирус, поражающий команду AutoOpen; повреждает каждый открываемый документ Word: переставляет в нем несколько слов и вставляет в произвольное место слово Wazzu.

4. Npad. Как и Concept, поражает файл normal.dot. Не причиняет особого вреда, лишь каждый двадцать третий раз при открытии документа Word выводит сообщение DOEUNPAD94, v.2.21.

5. Mdma. Довольно зловредный макровирус Word. Начинает пакостить первого числа следующего после заражения месяца. Причиняемый им ущерб различен в зависимости от операционной системы; серьезнее всего страдают Windows3.x и DOS, где он модифицирует файл autoexec.bat так, что при следующей перезагрузке последний стирает все файлы с жесткого диска. На машинах с Windows 95 вирус меняет настройку специальных возможностей "Залипание клавиш" (Sticky keys) и "Высокая контрастность" (High Contrast), а также настройку способа входа в сеть (Network Logon), стирает все справочные файлы Windows и некоторые системные файлы. После удаления вируса, как правило, требуется переустановка Windows 95(5).

Более важной характеристикой вируса, чем его тип, является степень разрушительности. Вирус, который сразу после внедрения причиняет значительный ущерб, фактически убивает пораженную машину, останавливая тем собственное распространение. Большинство существующих вирусов представляют собой вариации на небольшое число относительно простых тем, и вред от самых "популярных" либо очень незначительный, либо причиняется не сразу, а по прошествии нескольких дней, недель или даже месяцев после заражения компьютера.

Примером вируса замедленного действия может служить СИН, активизирующийся 26 числа каждого месяца и способный уничтожить данные на жестком диске.

Макровирусы в последнее время делаются все зловреднее. Правда, по большей части они не портят данные в масштабах всего компьютера, но, например, вирусы, внедряющиеся в таблицы Excel, способны производить серьезные разрушения в зараженных файлах.

Так, XM/Compat просматривает рабочий лист Excel в поисках незащищенных данных, а обнаружив их, вносит в произвольные места мелкие изменения, не меняя числа символов. И хотя современные антивирусные программы без труда распознают и удаляют XM/Compat, исправить нанесенный им ущерб можно, только восстановив данные с резервной копии — если она есть.

Возможно, многие время от времени получают сообщения о новых вирусах — в основном по электронной почте. Однако многих из них в действительности не существует, а письмо с предупреждением само размножается, как вирус. Чтобы отличить реальную угрозу от мифической, можно навести справки на Web-узле ciac.llnl.gov/ciac или на независимом узле www.kumite.com/myths, специально посвященном компьютерным мифам (4).

Антивирусные утилиты

Компьютерный мир окружают если не джунгли, то по крайней мере весьма богатый зоопарк. Несмотря на популярность антивирусных программ, вирусы продолжают плодиться и множиться. В среднем в месяц появляется около 200 новых разновидностей, а всего на сегодня их известно почти 18 тыс. Интенсивный обмен информацией по каналам электронной почты и Internet увеличивает риск заражения.

"Диких", т.е. реально циркулирующих вирусов насчитывается чуть больше 250, но многие из них способны причинить значительный финансовый ущерб и отнять уйму времени. По оценке экспертов ICSA (International Computer Security Association – Международная ассоциация за компьютерную безопасность), у вас примерно один шанс из тридцати подцепить вирус; в фирме, где есть 100 компьютеров, как минимум, три в течение следующего года заразятся.

Впрочем, как показало тестирование, большинство антивирусных пакетов вполне эффективно защищают от нынешних штаммов и умеют распознавать заражение еще не известными видами.

Рассмотрев несколько ведущих антивирусных программ, можно сказать, что, обладая примерно одинаковым талантом к вылавливанию вирусов, они существенно различаются по остальным показателям. Одни позволяют легко модифицировать сигнатуры (строки двоичного кода, идентифицирующие вирусы), а ведь регулярное обновление – лучший способ борьбы с новыми вирусами. Другие отличаются удачным интерфейсом, высокой скоростью работы, хорошо организованным сопровождением. А самые выдающиеся совершенны во всем: пакет Norton AntiVirus 5.0 – проверил диск объемом в 1 Гбайт менее чем за 13 мин., поймав там почти все вирусы, которые были туда занесены, и одновременно продемонстрировал простоту использования и обновления.

Рассмотрим шесть антивирусов – Command AntiVirus 4.52, McAfee VirusScan 4.0, Norton AntiVirus 5.0, Panda AntiVirus 6.005 Platinum, Sophos AntiVitus 3.13 и предварительную версию пакета PC-cillin компании Trend, а также новый продукт InDefense 2.10.

Command AntiVirus 4.52

Достоинства: низкая цена, почти безупречное распознавание вирусов, простой интерфейс.

Недостатки: сложная процедура обновления, некоторые проблемы с удалением "диких" вирусов.

McAfee VirusScan 4.0

Достоинства: великолепное распознавание и удаление вирусов, интерфейс, имитирующий дистанционное управление, простота использования.

Недостатки: самое длительное время сканирования.

Norton AntiVirus 5.0

Достоинства: великолепное распознавание и удаление вирусов, новые эффективные средства, такие, как Quarantine, усовершенствованный интерфейс.

Недостатки: через год обновление сигнатур становится платным.

Panda AntiVirus 6.005 Platinum

Достоинства: ясный пользовательский интерфейс, самая высокая скорость, простое обновление.

Недостатки: проблемы с выявлением макровирусов, много ложных срабатываний.

Sophos AntiVirus 3.13

Достоинства: отличное качество распознавания вирусов, гибкая настройка работы по расписанию, хорошо организованный интерфейс.

Недостатки: дороговизна, проблемы с восстановлением пораженных файлов.

Trend PC-cillin 6

Достоинства: замечательный интерфейс, мощные дополнительные функции, низкая цена.

Недостатки: предварительная версия не справилась с удалением одного из загрузочных вирусов.

In Defence – это новый продукт и его невозможно было проверить как другие пакеты. Он не нуждается в обновлении файлов сигнатур, но требует установки на "чистой" машине, так что ее сначала необходимо проверить каким-либо традиционным антивирусом. Поскольку он не является сканером, его невозможно подвергнуть тем же тестам, что и остальные пакеты. В отличие от других антивирусов этот пакет предполагает довольно высокую техническую грамотность пользователя.

К тестированию пакетов был привлечен эксперт по вирусам Джо Уэллс – автор ежемесячного электронного бюллетеня WildList, в котором отслеживается циркуляция "диких" вирусов.

Уэллс проверил каждый продукт на 254 имеющих сейчас хождение "диких" вирусах (из них 80 загрузочных, 89 файловых и 85 макровирусов) и 10606 образцах 7860 "лабораторных" вирусов.

Три антивируса – Command AntiVirus, McAfee VirusScan и Norton AntiVirus – распознали все "дикие" вирусы. Sophos пропустил один, а предварительная версия Trend – восемь, но статистически это неотличимо от стопроцентного распознавания. Panda не распознал 15 вирусов (все они были макровирусами), и сейчас фирма работает над исправлением программы. Ни один из пакетов не сумел обнаружить все "лабораторные" вирусы: для самых новых из них текущие версии еще не содержали детекторов. Command, McAfee, Norton, Sophos и Trend добились очень высоких показателей (от 97 до 99%); Panda нашел всего 78,4%, и фирма сейчас пытается усовершенствовать механизм обнаружения вирусов. У всех пакетов, за исключением McAfee, сканирование гигабайтного диска заняло менее 14 мин., а у McAfee длилось почти полчаса. Пакет InDefence невозможно было тестировать описанными методами.

В таблице 1 приводится сравнение возможностей антивирусных пакетов (4).

Таблица 1

Продукт 1	Цена в США. долл. 2	Поддерживаемые платформы 3	Сканирова- ние по расписанию 4	Автоматиче- ское обновление базы сигнатур 5
Command AntiVirus 4,52,561/575-3200, www.commandcom	40	Windows 95/98, NT, 3,1; Dos:OS/2 NetWare	•	□
McAfee VirusScan 4.0, 800/338-8754, www.mcafee.com ; российское представительство, www.mcafee.ru	49	Windows 95/98, NT, 3,1; DOS:OS/2	•	•

1	2	3	4	5
* Norton AntiVirus 5.0, 800/441-7234, www.symantec.com ; российское представительство, www.symantec.ru	40	Windows 95/98, ¹	•	■
Panda AntiVirus 6.005 Platinum:800/603-4922, www.pandasoftware.com	59	Windows95/98, NT, 3.1; DOS;OS/2	•	•
SophosAntiVirus 3.13,888/767-4679, www.sophos.com	99	Windows95/98, NT, 3.1; DOS;OS/2; NetWare	•	□ ²
Trend PC-cillin 6 ² , 800/228-5651, www.antivirus.com ; в России распространяется компанией "Прикладная логистика", www.apl.ru	40 ³	Windows95/98	•	•
InDefense 2.10, 877/472-3372, www.indefense.com	50	Windows95/98, NT, 3.1; DOS	□	N/A ⁴

* Лучший выбор

• - да

□ - нет

¹ - В состав пакета входит версия 4.0, поддерживающая также Windows 3.1 DOS и NT 3.51

² - Версия, предусматривающая обновления в течение года, стоит 249 долл.

³ - Цена версии на диске. При загрузке с Web-сервера программа стоит 30 долл.

⁴ - Программа не нуждается в обновлении сигнатур.

Рассмотрим еще несколько антивирусных программ, которые были тестированы ведущими в этой области специалистами.

Dr Solomon's Anti-Virus 7.0

Достоинства: безукоизненное распознавание и обезвреживание "диких" вирусов и почти безошибочное – "лабораторных", четкий интерфейс.

Недостатки: отсутствует автоматический запуск по заданному графику, не осуществляется проверка гибкого диска при закрытии системы, только одно бесплатное обновление.

F-Prot Professional 2.15

Достоинства: безукоизненное распознавание и обезвреживание "диких" вирусов, развитая поддержка работы в сети.

Недостатки: не распознаются некоторые "лабораторные" вирусы, для получения обновлений нужно пройти процедуру регистрации.

IBM AntiVirus 3.0.1

Достоинства: безукоизненное распознавание и обезвреживание "диких" вирусов, хорошее распознавание "лабораторных", богатый набор возможностей, самая высокая скорость проверки, поддержка всех основных операционных систем.

Недостатки: чрезвычайно сложная процедура обновления, проблемы с удалением некоторых макровирусов.

Inoculan AntiVirus 5.0 for Windows 95

Достоинства: великолепный интерфейс, богатый выбор режимов сканирования, дешевизна, почти безукоизненное распознавание и обезвреживание "диких" вирусов.

Недостатки: сравнительно слабое распознавание "лабораторных" вирусов, многочисленные ложные срабатывания, самое медленное сканирование, возможны конфликты с видеоплатой STB Nitro 3D.

McAfee VirusScan 3.0

Достоинства: почти безуказненное распознавание всех вирусов, полезные возможности конфигурирования, поддерживает все основные операционные системы.

Недостатки: непонятная политика обновления, некоторые продвинутые возможности трудно найти.

Norton AntiVirus 4.0

Достоинства: безуказненное распознавание и обезвреживание "диких" вирусов, хорошее распознавание "лабораторных", тонкая настройка интерфейса.

Недостатки: в уровнях настройки можно запутаться.

PC-cillin AntiVirus 3.0

Достоинства: почти безуказненное распознавание и обезвреживание "диких" вирусов, богатый выбор функций.

Недостатки: многочисленные ложные срабатывания, самое слабое распознавание "лабораторных" вирусов, несколько запутанный интерфейс.

ThunderByte Anti-Virus Utilities 8.0.3

Достоинства: почти безуказненное распознавание "диких" вирусов, хорошее распознавание "лабораторных", всеобъемлющая система настройки, поддержка всех главных операционных систем, высокая скорость.

Недостатки: самый дорогой из всех пакетов, при обезвреживании "диких" вирусов может удалять файлы и макросы, не предусмотрено восстановление с аварийной дискеты, сложен в установке, невозможна полная deinсталляция (5).

Обычно антивирусные программы обеспечивают два типа защиты: по **требованию**, в этом случае проверка файлов на вирусы производится по указанию пользователя; и в **реальном времени** – программа функционирует в фоновом режиме и любые вычислительные действия исследуются на наличие признаков вирусного заражения. Большинство антивирусных утилит имеют сертификат Международной ассоциации по компьютерной безопасности ICSA – это означает, что их механизмы поиска по требованию должны обнаруживать 100% обычно встречающихся вирусов и 90% оставшихся мало распространенных "лабораторных" (ZOO) вирусов, редко встречающихся.

В ходе тестирования оценивалась способность каждого продукта обнаруживать макровирусы при открывании файлов.

Ниже, в таблице 2 приводится сводка характеристик антивирусных утилит для Microsoft Windows 95

Антивирусные программы

Таблица 2

<input checked="" type="checkbox"/> Да <input type="checkbox"/> Нет	Dr. Solomon's Anti-Virus 7.79	Dr. Solomon's Anti-Virus Toolkit for Windows 95	eSafe Protect 1.02	F-Prot Professional 3.01	IBM AntiVirus 3.0.1	InocuLAN AntiVirus 5.0 for Windows 95	McAfee VirusScan 3.1.1
Рекомендуемая изготовителем цена, долл.	49.95	125.00	49.00	49.95	49.00	69.00	49.00
Дискета для восстановления системы	■	■	■	■	■	■	■
Поиск вирусов в процессе инсталляции	■	■	■	■	■	■	■
Поиск вирусов в загрузочном секторе	■	■	■	■	■	■	■
Сохранение резервной копии головной записи загрузки	□	□	■	■	□	■	□
Открывание и проверка сжатых файлов	■	■	■	■	■	■	■
Поиск вирусов в памяти	■	■	■	■	■	■	■
Планирование автоматических проверок	□	■	■	■	■	■	■
Проверка файлов при обращениях к ним	■	■	■	■	■	■	■
Выбор файлов по типу	■	■	■	■	■	■	■
Поиск вирусов в фоновом режиме	■	■	■	■	■	■	■
Обнаружение и удаление макровирусов	■	■	■	■	■	■	■
Вывод отчетов на экран/регистрационный файл	■ ■	■ ■	■	■ □	■ ■	■ ■	■ ■
Обновление информации через Internet	■	□	■	■	■	■	■
Автоматическое обновление информации	■	□	■	■	□	■	■

<input checked="" type="checkbox"/> Да <input type="checkbox"/> Нет	Norton AntiVirus 4.0	PC-cillin 3.0	Thunder-Byte AntiVirus Utilities 8.03a	Vet Premium Anti-Virus 9.6	VirusSweep 1.0
Рекомендуемая изготавителем цена, долл.	49.95	44.95	99.95	65.00	39.95
Дискета для восстановления системы	■	■	■	■	■
Поиск вирусов в процессе инсталляции	■	■	■	■	■
Поиск вирусов в загрузочном секторе	■	■	■	■	■
Сохранение резервной копии головной записи загрузки	■	■	■	■	■
Открывание и проверка сжатых файлов	■	■	■	□	■
Поиск вирусов в памяти	■	■	■	■	■
Планирование автоматических проверок	■	■	□	□	■
Проверка файлов при обращениях к ним	■	■	■	■	■
Выбор файлов по типу	■	■	■	■	■
Поиск вирусов в фоновом режиме	■	■	■	■	■
Обнаружение и удаление макровирусов	■	■	■	■	■
Вывод отчетов на экран/регистрационный файл	■ ■	■ ■	■ ■	■ ■	■ ■
Обновление информации через Internet	■	■	■	■	■
Автоматическое обновление информации	■	■	■	■	■

ICSA провела несколько дополнительных тестов. Сертифицированные продукты обнаруживали макровирусы в ходе проверки накопителя, однако необходимо было исследовать их поведение в других ситуациях, в том числе выяснить, как проходит инсталляция программы на уже зараженной машине, способна ли программа находить макровирусы при открывании зараженного файла и определять наличие гибкого диска в накопителе при выключении ПК.

В ходе теста Macro Virus пятью продуктами были пропущены макровирусы. Тест Installation также важен, поскольку инсталляция антивирусной программы на уже зараженном компьютере может повлиять на ее способность защитить машину и повредить сам антивирусный продукт.

Тест Floppy Disk Detection (обнаружение гибкого диска) показывает, выдается ли программой предупреждение о наличии дискеты в НГМД во время отключения ПК.

В ходе выполнения теста Program Files Scanned (проверенные программные файлы) измерялось время, необходимое для проверки программных файлов в машине.

Просмотр только программных файлов не всегда эффективен при поиске макровирусов, поэтому в ходе теста All Files Scanned (все проверенные файлы) измерялось время, необходимое каждому пакету для проверки всех файлов в компьютере.

Тест Performance позволяет определить, каким образом поиск вирусов влияет на системную производительность.

Результаты тестирования приведены в таблице 3 (6).

Таблица 3

	Обезвре- жи- вание Число пропущенных макровирусов	Поиск Программные файлы, файл/с	Все файлы файл/с	Сжатые файлы, файл/с	Снижение производитель- ности (измеренное на тестах Windows 98), %
Dr Solomon's Anti-Virus	0	35.6	37.6	0.60	2
Dr Solomon's Anti-Virus Toolkit for Windows 95	0	35.5	37.0	0.26	2
eSafe Protect	4	36.6	36.5	1.09	2
F-Prot Professional	0	37.8	43.7	0.33	1
IBM AntiVirus	1	55.7	38.1	1.12	1
InocuLan AntiVirus	1	15.1	20.6	0.33	0
McAfee VirusScan	0	18.0	17.4	0.38	1
Norton AntiVirus	0	30.2	39.2	0.25	1
PC-cillin	1	32.1	30.5	0.31	7
ThunderByte AntiVirus Utilities	1	58.4	63.6	0.04	1
Vet Premium Anti-Virus	0	41.8	46.6	N/A	5
ViruSweep	0	41.1	38.7	0.49	1

Заключение

С течением времени, вопреки ожиданиям многих пользователей, компьютерные вирусы не стали меньшей проблемой нежели раньше, скорее наоборот. Теперь вирусы попадают на компьютер не только с зараженных дисков, но и из Internet, и из сообщений, приходящих по электронной почте.

Проблема борьбы с вирусами, некогда волновавшая лишь крупные корпорации, которые нуждались в защите критически важной информации, отныне должна интересовать каждого пользователя, чей ПК (персональный компьютер) подключен к Internet (7).

Компьютерное общество в последнее время весьма энергично реагирует на появление новых вирусов. Опасность, которую таят в себе вирусы, настолько велика, что специалисты, не жалея ни средств, ни времени, стараются немедленно предотвратить угрозу очередной эпидемии (1).

Можно сказать, что современное положение с компьютерными вирусами несколько напоминает гонку вооружений: "хакеры" пишут все новые и новые вирусы, способные обходить существующие средства защиты, а разработчики средств защиты совершенствуют свои программы так, чтобы они могли распознавать эти новейшие вирусы (8).

Литература

1. Федоров В. Осторожно, зараженные участки // Профиль.-1999.-N14.-с.40-41
2. Никишин А. В., Павлющик М. А., Зенкин Д. В. Компьютерные вирусы: рискуют все. Антивирусные программы "Лаборатории Касперского" //НТИ.-сер.1.-2000.-N6.-с.14-17
3. Дронов В. Один на один с макровирусом //Мир ПК.-1998.-N4.-с.66-67
4. Мястковский Стен. Смерть вирусам//Мир ПК.-1999.-N4.-с.48-58
5. Мястковский Стен. Антивирусы 1998// Мир ПК.-1998.-N4.-с.52-65
6. Фасти Уилл. Защита файлов // PC Magazine.-1998.- N7.-с.110-124
7. Михайлов Е. Защитите ваши данные // Мир ПК.-1998.-N4.-с.70-73
8. Насыпный В. Комплексная защита компьютерных систем // Мир ПК.-1998.-N4.-с.68-69

Содержание

Введение.....	3
Антивирусные программы лаборатории Касперского.....	4
Макровирусы.....	10
Антивирусные утилиты.....	12
Заключение.....	19
Литература.....	20

Редактор и корректор Б. Чубарян

Объем 1,1 уч.-изд. Формат 60x84 1/16

Отдел оперативной полиграфии

375051, Ереван, Комитаса, 49/3, АрмНИИНТИ