Московский Физико-Технический Институт
Факультет Радиотехники и Кибернетики

***Эссе*: "Компьютерные вирусы. Обнаружение и предотвращение."**

***Предмет*:** Защита информации
***Преподаватель*:** Обернихин В.В.
***Автор*:** Козенко С.Е., студент 916 гр.

2003 г.

Введение.

В настоящее время, в связи с широким распространением информационных технологий резко обострилась проблема защиты компьютеров от заражения их компьютерными вирусами. В связи с этим появляется все больше антивирусных *программ,* способных помочь пользователю в борьбе с ними. Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему уже 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. Вот ещё пара случаев нарушения безопасности сети и последствия этого. 2 ноября 1988 года выпускник Корнельского университета Роберт Таппан Моррис запустил свою программу, которая вышла из-под контроля автора и начала быстро перемещаться по сети. В короткий срок вирус-червь Morris заполнил многие узлы Internet, загружая операционные системы Unix своими копиями, вызывая отказы в обслуживании и т.п. Червь инфицировал 6200 компьютеров. Подсчитанные потери, хотя формально червь не наносил какого-либо ущерба данным в инфицированных хостах, были разделены на прямые и косвенные. Прямые потери были оценены более чем в 32 000 000 долларов. Косвенные потери были оценены более чем в 66 000 000 долларов. Общие затраты были оценены на сумму в 98 253 260 долларов. А, например, вирус I love you парализовала некоторые деловые системы, расположенные в Европе и США. Вирус VBS/LoveLetter.bd впервые появился в Европе. Как утверждают эксперты, сначала он размножался и заражал только компьютеры банков в разных частях США. Последняя версия загружает из сети и запускает программу hcheck.exe , которая ворует пароли с инфицированного компьютера. Эта программа посылает сворованные коды для доступа к банковским системам на электронные адреса, зарегистрированные на бесплатных почтовых Web-узлах, заведенные американскими компаниями. Последствия и ущерб этого вируса можете себе представить!

Что такое компьютерные вирусы, какие они бывают, что они делают и как с ними, бороться вы сможете узнать далее. Для начала…

…немного истории.

Первое упоминание о компьютерных вирусах было зафиксировано еще в конце 60-х. На мейнфреймах того времени периодически появлялись программы, которые получили название «кролик» (the rabbit). Эти программы клонировали себя, занимали системные ресурсы и таким образом снижали производительность системы. Скорее всего «кролики» не передавались от системы к системе и являлись сугубо местными явлениями - ошибками или шалостями системных программистов, обслуживавших компьютер. Первый же инцидент, который смело можно назвать эпидемией «компьютерного вируса», произошел в системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам, т.е. во многом делал то же самое, что и тысячи современных компьютерных вирусов. Далее события разворачивались стремительно: каждый год появлялись все новые вирусы и новые алгоритмы их написания. Первая революция в мире вирусов произошла в начале 1970 года, когда под операционную систему Tenex был создан вирус «The Creeper», использовавший для своего распространения глобальные компьютерные сети. Вирус был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. Для борьбы с этим вирусом была создана программа «The Reeper» - первая известная антивирусная программа. Самым же интересным является то, что вплоть до конца 80-х большинство пользователей компьютеров отказывались верить в существование вирусов. Показателен тот факт, что даже компьютерный гуру - человек-легенда Питер Нортон - высказывался против существования вирусов. Он объявил их несуществующим мифом и сравнил со сказками о крокодилах, живущих в канализации Нью-Йорка. Этот казус, однако, не помешал фирме Symantec (www.symantec.com) через некоторое время начать собственный антивирусный проект - Norton Anti-Virus, который и сейчас пользуется огромной популярностью пользователей всего мира.

Подробную хронологию событий развития вирусов и антивирусного софта можно прочитать по адресу www.viruslist.com. Также о событиях в мире компьютерных вирусов, можно узнать на сайте www.virusbtn.com, а о программах троянцов на www.trojan.ru .

Что такое компьютерный вирус?

Официально считается, что термин "компьютерный вирус" впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Основная трудность, возникающая при попытках дать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и проч.) либо присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением

возможности распространения). Основная же особенность компьютерных вирусов - возможность их самопроизвольного внедрения в различные объекты операционной системы - присуща многим программам, которые не являются вирусами. Второй же трудностью, возникающей при формулировке определения компьютерного вируса является то, что данное определение должно быть привязано к конкретной операционной системе, в которой этот вирус распространяется. Например, теоретически могут существовать операционные системы, в которых наличие вируса просто невозможно. Таким примером может служить система, где запрещено создавать и изменять области выполняемого кода, т.е. запрещено изменять объекты, которые либо уже выполняются, либо могут выполняться системой при каких-либо условиях. Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Попробуем всё же дать определение вируса. *Вирус - это программный код способный к самостоятельному размножению и функционированию, и имеющий защитные механизмы от обнаружения и уничтожения.*

Различие между компьютерным вирусом и другими программами - то, что вирусы предназначены, чтобы делать копии себя. Они обычно самокопируют без знания пользователя. Вирусы часто содержат 'полезные грузы' - действия, которые вирус выполняет отдельно от ответа пользователя. Полезные грузы могут изменяться от раздражающего (например, WM97/CLASS-D - вирус, который неоднократно показывает издевательские сообщения пользователю), к бедственному (например, CIH - вирус, который пытается переписывать вспышку BIOS, чем может нанести непоправимый ущерб некоторым компьютерам).

Вирусы могут быть скрыты в программах, доступных на дискетах или компакт-дисках, скрыт в приложениях электронной почты или в материале, разгруженном от сети. Если вирус не имеет никакого очевидного полезного груза, пользователь без антивирусного программного обеспечения даже не может знать, что компьютер поражен.

Как присходит заражение?

По способу заражения файлов вирусы делятся на:

- "overwriting"
- паразитические ("parasitic")
- компаньон-вирусы ("companion")
- "link"-вирусы, вирусы-черви
- вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ

Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

К разновидности *overwriting-вирусов* относятся вирусы, которые записываются вместо DOS-заголовка NewEXE-файлов. Основная часть файла при этом остается без изменений и продолжает нормально работать в соответсвующей операционной системе, однако DOS-заголовок оказывается испорченным. Как только вирус активен на компьютере, он может копировать себя, чтобы заразить другие файлы или диски, поскольку к ним обращается пользователь.

К *паразитическим* относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сими файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов ("prepending"), в конец файлов ("appending") и в середину файлов ("inserting"). В свою очередь, внедрение вирусов в середину файлов происходит различными методами - путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла ("cavity"-вирусы).

К категории "*компаньон"* относятся *вирусы*, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

Link-вирусы, как и компаньон-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла "заставляют" ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.

Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения. При этом вирус добавляет к исходным текстам свой исходный код (в этом случае вирус должен содержать его в своем теле) или свой шестнадцатеричный дамп (что технически легче). Зараженный файл способен на дальнейшее распространение вируса только после компиляции и линковки (см. например, вирусы "SrcVir", "Urphin"). Теперь познакомимся с разнообразием вирусов.

Какие бывают вирусы ?

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 длокументы, 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 ОС - 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 некотоорых 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.

Как бороться с компьютерными вирусами?

Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус). Более того, невозможность существования абсолютного антивируса была доказана математически на основе теории конечных автоматов, автор доказательства - Фред Коэн.

Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

- "Ложное срабатывание" (False positive) - детектирование вируса в незараженном объекте (файле, секторе или системной памяти). Обратный термин - "False negative", т.е. недетектирование вируса в зараженном объекте.
- "Сканирование по запросу" ("on-demand") - поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания (system scheduler).
- "Сканирование на-лету" ("real-time", "on-the-fly") - постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без запроса пользователя.

Типы антивирусов:

- Сканеры
- CRC-сканеры
- Блокировщики
- Иммунизаторы

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаги, полифаги). Следом за ними по эффективности и популярности следуют CRC-сканеры (также: ревизор, checksumer, integrity checker). Часто оба приведенных метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа блокировщики и иммунизаторы.

Принцип работы *антивирусных сканеров* основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т.е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения ("возможно заражен" или "не заражен") для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории - "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поисх и обезвреживание всех типов вирусов вне зависимости от операционной системы,

на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на "резидентные" (мониторы), производящие сканирование "на-лету", и "нерезидентные", обеспечивающие проверку системы только по запросу. Как правило, "резидентные" сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как "нерезидентный" сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам - размеры антивирусных баз, которые сканерам приходится "таскать за собой", и относительно небольшую скорость поиска вирусов. Главный недостаток сканеров - то, что они должны сохраниться модифицированными с самой последней вирусной информацией, чтобы оставаться эффективным.

Принцип работы *CRC-сканеров* основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры 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. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту "слабость" CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

Антивирусные блокировщики - это резидентные программы, перехватывающие "вирусо-опасные" ситуации и сообщающие об этом пользователю. К "вирусо-опасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати,

бывает очень полезно в случаях, когда давно известный вирус постоянно "выползает неизвестно откуда". К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (мне, например, неизвестно ни об одном блокировщике для Windows95/NT - нет спроса, нет и предложения).

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера ("железа"). Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает "ложное срабатывание" защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

Иммунизаторы делятся на два типа: 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 летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время.

Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные (пример - печально известная строка "MsDos", предохраняющая от ископаемого вируса "Jerusalem"). 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.

Такой тип иммунизации не может быть универсальним, поскольку нельзя иммунизировать файлы от всех известных вирусов: одни вирусы считают уже зараженными файлы, если время создания файла содержит метку 62 секунды, а другие - 60 секунд. 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.

Источники:

1. http://www.viruslist.com/viruslistbooks.html?id=31&gloss=8215
2. http://www.uinc.ru/articles/index.shtml
3. http://www.semsk.kz/computers/virus/
4. http://www.itworld.com/Sec/4039/IW010312camentor/
5. Макаров Н.Н., Захаров А.П. “Недетерминированные автоматы”