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 своровванные 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 компактдисках, 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.