Антивирусные средства защиты информации

Компьютерные вирусы. Первая массовая эпидемия компьютерного вируса произошла в *1986* году, когда вирус Brain «заражал» дискеты для первых массовых персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры с различными операционными системами и распространяющихся по компьютерным сетям.

Обязательным свойством компьютерного вируса является способность к размножению (самокопированию) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы. Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

После заражения компьютера вирус может активизироваться и заставить компьютер выполнять какие-либо действия. Активизация вируса может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программы, открытием документа и так далее).

Компьютерные вирусы – это программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

Разнообразны последствия действия вирусов; по величине вредных воздействий вирусы можно разделить на:

• *неопасные*, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;

• *опасные*, которые могут привести к сбоям и зависаниям при работе компьютера;

• *очень опасные*, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и так далее.

По «среде обитания» вирусы можно разделить на *файловые, загрузочные, макровирусы* и *сетевые.*

Файловые вирусы. Файловые вирусы различными способами внедряются в исполнимые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (то есть может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

При этом файловые вирусы не могут заразить файлы данных (например, файлы, содержащие изображение или звук).

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

Загрузочные вирусы. Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера.

Профилактическая защита от таких вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.

Макровирусы. Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ.

После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе.

Сетевые вирусы. По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это может происходить, например, при получении зараженных файлов с серверов файловых архивов. Однако существуют и специфические сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину.

Интернет-черви (worm) – это вирусы, которые распространяются в компьютерной сети во вложенных в почтовое сообщение файлах. Автоматическая активизация червя и заражение компьютера могут произойти при обычном просмотре сообщения. Опасность таких вирусов состоит в том, что они по определенным датам активизируются и уничтожают файлы на дисках зараженного компьютера.

Кроме того, интернет-черви часто являются *троянами,* выполняя роль «троянского коня», внедренного в операционную систему. Такие вирусы «похищают» идентификатор и пароль пользователя для доступа в Интернет и передают их на определенный почтовый адрес. В результате злоумышленники получают возможность доступа в Интернет за деньги ничего не подозревающих пользователей.

Лавинообразная цепная реакция распространения вируса базируется на том, что вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя. Кроме того, может происходить заражение и по локальной сети, так как червь перебирает все локальные диски и сетевые диски с правом доступа и копируется туда под случайным именем.

Профилактическая защита от интернет-червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами *(скрипт-вирусами)*. Такие программы передаются по Всемирной паутине в процессе загрузки Web-страниц с серверов Интернета в браузер локального компьютера.

Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

Антивирусные программы. Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Антивирусные программы могут использовать различные принципы для поиска и лечения зараженных файлов.

Полифаги. Самыми популярными и эффективными антивирусными программами являются антивирусные программы *полифаги* (например, Kaspersky Anti-Virus, Dr.Web). Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

Для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса. Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.

Для поиска новых вирусов используются алгоритмы «эвристического сканирования», то есть анализ последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то полифаг выдает сообщение о возможном заражении объекта.

Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются антивирусными *мониторами.*

К достоинствам полифагов относится их универсальность. К недостаткам можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

Ревизоры. Принцип работы ревизоров (например, *ADinf*) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о

файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики. Антивирусные *блокировщики* – это программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.

Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

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

Антивирусные программы (далее антивирусы) являются основной частью современной *антивирусной защиты* (если рассматривать *антивирусную защиту* как комплекс программ, которые противостоят зловредным программам). Как правило, их мощностей хватает, чтобы справиться с большинством зловредных программ, но иногда бывает и так, что *по* тем или иным причинам, они справиться не могут (в целях удобства для чтения все типы зловредных программ будем называть общим понятием вирусы). А с чего началась эта борьба антивирусов с различными вирусами?

История возникновения антивирусных программ

Самый первый *вирус*, действовавший уже точно на поражение, появился в конце 60-ых. Ему пожертвовали тот же *компьютер*, на котором его и создали (впервые, с целью развлечения). Но все эти развлечения, может, так и остались бы только игрушками программистов, если бы не рождение Интернета. Еще в 1975 году через *сеть* Telenet разошелся и самый первый сетевой *вирус*"The Creeper", и впервые была создана *программа* - *антивирус* "Reeper". Но уже в следующем десятилетии Ф. Коэн делал эксперименты с программами, которые смогут размножаться и иметь возможность распространиться, его "детище" создавало свои копии и находило выходы для них в большую компьютерную *сеть*. Так *по* этому принципу вирусы распространились и в наше время через глобальную *сеть*. А тогда, в 1984 г., Коэн выступил на седьмой конференции *по* безопасности информации в Соединенных Штатах, высказывая свои мысли *по* поводу новой угрозы в этой сфере деятельности. Также два брата Амджад в Пакистане в 86 г открыли неизвестный доселе *вирус*. Братья торговали

программным обеспечением и вдруг нечаянно увидели, что кто-то его несанкционированно копирует и множит, лишая их честно заработанных денег. Чтобы как-нибудь остановить любителей "халявы", они написали программку "THE BRAIN" и внедрили ее в свои работы. Она стала активной при попытке копирования. Именно это было началом и прообразом всех будущих вирусов. THE BRAIN резко перешел границу Пакистана и поверг в шок неготовый к этому необычному явлению мир. А уже в 1987 году появилась первая литература о вирусах и борьбе с ними. С этого момента стало абсолютно очевидно, что для борьбы с вирусами необходимо создавать специальные программы "антивирусы", которые могли бы бороться с вирусами, тем самым "лечa" зараженную машину. Первые антивирусы были далеки от современных антивирусных программ. Фактически, они были одноразовыми программами, которые предназначались для лечения определенного вируса. Само же распространение такого *антивируса* было достаточно дорогим и долгим занятием, так как антивирусы записывались на дискеты и высылались своим подписчикам в разные уголки мира. Естественно, такая доставка была достаточно долгой, и было весьма сложно своевременно получить нужную копию *антивируса*. Часто бывало и так, что жители особо удаленных мест от места отсылки дискеты с антивирусом к моменту получения *антивируса* были заражены парой еще других вирусов. Все это создавало плохую репутацию для антивирусов, но с развитием сети *Интернет* антивирусы стали высылать сначала на почтовые ящики пользователей, а потом и появилась возможность динамически обновлять специальные антивирусные базы. Сама же схема работы первых антивирусов была далека от идеала: они не умели постоянно работать на зараженной машине, а были, *по* сути дела, лишь сканером, который искал определенный *вирус* и далее пытался с ним справиться. Создатели вирусов нашли достаточно простой способ для борьбы с такими антивирусами: они стали создавать вирусы, которые уничтожали *антивирус* до того, как им мог воспользоваться *пользователь* (то есть они просто стирали *антивирус* с дискеты, которая приходила пользователю). Создатели же антивирусов в свою *очередь* стали оснащать свои антивирусы специальными "протекторами", которые не позволяли удалить антивирусную программу. Тогда стали появляться вирусы, которые маскировались под системные файлы или папки, а потом начали появляться вирусы, которые даже могли изменять свой собственный код (чтобы *антивирус* не мог их обнаружить). Но антивирусные программы также совершенствовались (работало правило "на каждый меч найдется свой щит"), и стала очевидна борьба создателей антивирусов с создателями вирусов. В свою *очередь* пресса стала распространять слухи, что антивирусные компании сами пишут различные вирусы, с целью поддержания интереса к антивирусным программам (в какой-то мере это может быть вполне логичным заключением), но подобные слухи до сих пор не могут найти своего подтверждения. Интересно и то, что создатели антивирусов составляют конкуренцию друг другу в борьбе за покупателей, и поэтому вполне логичным является *вывод*, что держать

несколько антивирусов на компьютере нецелесообразно, так как они будут конфликтовать друг с другом, что будет играть на руку самим вирусам.

Механизм работы современных антивирусов

Современный *антивирус* является сложным программным средством, которое должно обеспечить надежную защиту компьютерного устройства (компьютера, карманного компьютера или нетбука) от различных вирусов (зловредных программ). Общая схема *антивируса* представлена на рисунке ниже:

Схема антивируса

Как видно из схемы, *антивирус* состоит из следующих частей:

1. Модуль резидентной защиты
2. Модуль карантина
3. Модуль "протектора" *антивируса*
4. *Коннектор* к *антивирусу*-серверу
5. Модуль обновления
6. Модуль сканера компьютера

Модуль резидентной защиты является основным компонентом *антивируса*, находящийся в оперативной памяти компьютера и сканирующий в режиме реального времени все файлы, с которыми осуществляется взаимодействие пользователя, операционной системы или других программ. *Слово* "резидентный" означает "невидимый", "фоновый". Резидентная защита проявляет себя только при нахождении вируса. Именно на резидентной защите основывается главный принцип антивирусного *ПО* – предотвратить заражение компьютера. В ее состав входят такие компоненты, как активная защита (сравнение антивирусных сигнатур со сканируемым файлом и выявление известного вируса) и проактивная защита (совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых является предотвращение заражения

системы пользователя, а не *поиск* уже известного вредоносного программного обеспечения в системе).

Модуль карантина является модулем, который отвечает за помещение подозрительных файлов в специальное *место*, именуемое карантином. Файлы, перемещенные в карантин, не имеют возможности выполнять какие-либо действия (они заблокированы) и находятся под наблюдением *антивируса*. *Антивирус* принимает решение поместить *файл* на карантин при обнаружении в файле признака вирусной деятельности (при этом сам *файл* с точки зрения *антивируса* вирусом в этом случае не является, просто *файл*является потенциальной угрозой), либо если *файл* действительно заражен вирусом, но его необходимо излечить, а не удалять целиком (например, важный документ пользователя, в который попал *вирус*). В последнем случае *файл* будет помещен в карантин для последующего излечения от вируса (если же *антивирус* не сможет вылечить *файл*, его придется удалить, либо оставить, в надежде на то, что с новым обновлением *антивирус* сможет вылечить этот *файл*). Обычно карантин создается в особой папке антивирусной программы, которая изолирована от каких-либо действий, кроме действий со стороны *антивируса*.

Модуль протектора *антивируса* является модулем, который защищает *антивирус* от стороннего вмешательства со стороны различных программных средств. Этот *модуль* является защитником *антивируса*. Часто вирусы хотят стереть *антивирус* или предотвратить его работу путем блокировки *антивируса*. *Модуль* протектора *антивируса* не даст это сделать. Впрочем, не все современные антивирусы снабжены качественными протекторами. Некоторые из них ничего не могут сделать против современных вирусов, а вирусы в свою *очередь* могут спокойно и беспрепятственно полностью стереть *антивирус*. Также появились вирусы, которые имитируют удаление *антивируса* со стороны пользователя, то есть протектор *антивируса* считает, что сам *пользователь по* каким-либо причинам хочет удалить *антивирус*, и поэтому не препятствует этому, хотя на самом деле это *деятельность* вируса. В настоящее время антивирусные компании стали более серьезно подходить к выпуску протекторов, и становится очевидно, что если *антивирус* не будет иметь хороший протектор, его эффективность в борьбе с вирусами будет очень мала.

Коннектор к *антивирусу*-серверу является важной частью *антивируса*. *Коннектор* служит для соединения *антивируса* к серверу, с которого *антивирус* может скачать актуальные базы с описанием новых вирусов. При этом соединение должно проходить *по*специальному защищенному *Интернет*-каналу. Это очень важный момент, так как *злоумышленник* может подложить неверные антивирусные базы с лживым описанием вирусов, если *антивирус* будет соединяться с сервером *по* незащищенному *Интернет*-каналу. Также в современных антивирусах *коннектор* служит еще и для соединения к специальному серверу, который управляет антивирусом. Подобное соединение изображено на рисунке ниже:

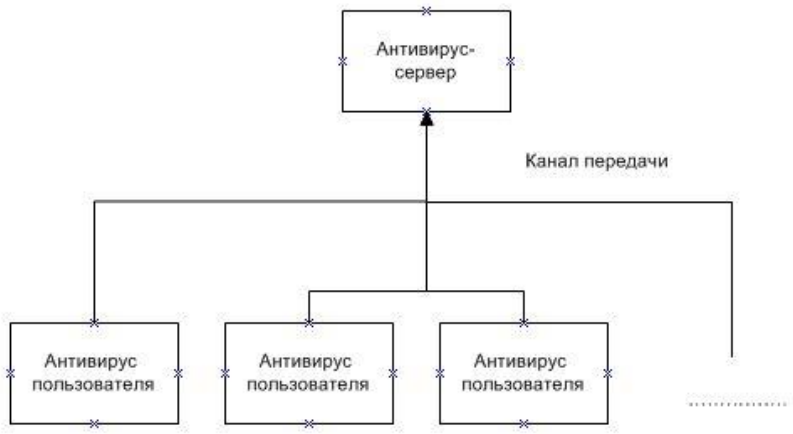

Схема соединения к серверу

Как видно из рисунка, *коннектор* позволяет соединять множество антивирусов пользователей с единым антивирусом-сервером, с которого антивирусы пользователя могут скачивать обновления, а также если на стороне *антивируса* пользователя возникли какие-либо неразрешимые проблемы, то *антивирус-сервер* будет удаленно их решать (например, у *антивируса* пользователя стал неисправен какой-либо из модулей и *антивирус-сервер* предоставит этот *модуль* отдельно для скачивания). В этом случае также очень важную роль играет защищенность канала передачи (канала связи) информации. Со стороны злоумышленников стала применяться интересная практика, в результате которой захватывается *контроль* над самим каналом передачи информации, и фактически *злоумышленник* становится управляющим для антивирусов пользователя (для всех или частично, в зависимости от того, какой именно участок канала передачи будет перехвачен злоумышленником). В свою *очередь*, создатели антивирусов стали зашифровывать данные на канале информации, чтобы *злоумышленник* не мог получить к ним *доступ* и как-либо завладеть ими.

Модуль обновления отвечает за то, чтобы обновление *антивируса*, его отдельных частей, а также его антивирусных баз прошло правильно. В современной практике создания антивирусов стала применяться следующая идея: *модуль* обновления также должен определять подлинные или нет антивирусные базы скачивает сам *модуль*. Подлинность при этом может проверяться различными методами - от проверок контрольной суммы файла с базами до поиска внутри файла с базами специальной метки, которая говорит о том, что этот *файл* является подлинным. Подобные действия стали вводиться после того, как участились случаи подмены антивирусных баз со стороны злоумышленников.

Модуль сканера компьютера является, пожалуй, самым старым модулем в современных антивирусах, так как раньше антивирусы состояли только из этого модуля. Этот *модуль* отвечает за то, чтобы сканировать *компьютер* на наличие вирусов, если этого будет требовать *пользователь* компьютера. Сам *модуль* при сканировании компьютера использует антивирусные базы, которые были добыты с помощью модуля обновления

антивируса. Если *сканер* найдет, но не справится с вирусом сразу же, то он поместит *файл* с вирусом в карантин. Потом, впоследствии, *модуль* сканера компьютера может связаться через *коннектор* с антивирусом-сервером и получить инструкции *по* обезвреживанию зараженного файла. Следует отметить, что *модуль* сканера компьютера предназначен для профилактики компьютера от вирусов, так как основную защиту представляет *модуль* резидентной защиты. В модуле сканера компьютера используются только антивирусные базы, в которых четко описаны вирусы. Различные элементы проактивной защиты (например, *эвристика*) не используются в модуле сканера компьютера. Обычно создатели вирусов не строят специальную защиту для своих вирусов от модулей сканера компьютера, так как знают, что *пользователь* не часто проверяет *компьютер* сканером, и этого промежуточного времени от проверки до проверки хватит, чтобы украсть *персональные данные* пользователя.

Задание: написать конспект в тетрадь.