Презентация подготовлена для конкурса «Интернешка» http://interneshka.org/

# Вирусы и антивирусные программы

Презентация ученика
9 «А» класса МАОУ «СОШ №54»
Мариевского Дмитрия

# Вирусы

- **Компьютерные вирусы** – программы, которые создают программисты специально для нанесения ущерба пользователям ПК. Их создание и распространение является преступлением.
- Вирусы могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков и документы. Активизация вируса может вызвать уничтожение программ и данных.. Первая эпидемия произошла в 1986г (вирус «Brain» - мозг по англ.) Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000г, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

# Вирусы по месту их обитания

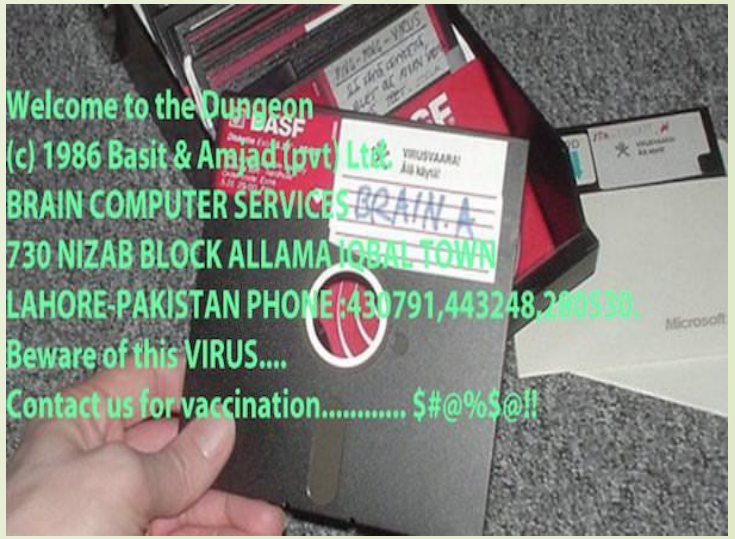
- ***Файловые вирусы*** способны внедряться в программы и активизируются при их запуске
- Из ОП вирусы заражают другие программные файлы (com, exe, sys) меняя их код вплоть до момента выключения ПК. Передаются с нелегальными копиями популярных программ, особенно компьютерных игр. Но не могут заражать файлы данных (изображения, звук)
- * ***Загрузочные вирусы*** передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы. Правила защиты:1)Не рекомендуется запускать файлы сомнительного источника (например, перед загрузкой с диска А – проверить антивирусными программами); 2) установить в BIOS ПК (Setup) защиту загрузочного сектора от изменений
- * ***Макровирусы*** - заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия приложения. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их
- загрузку. Выбор запрета на макросы предотвратит загрузку от зараженных, но и отключит возможность использования полезных макросов в документе
- * **Сетевые вирусы** – распространяются по компьютерной сети.
- При открытии почтового сообщения обращайте внимание на вложенные файлы!

# Первые вирусы

- Отцом первого компьютерного вируса стал американский студент Фред Коэн, который во время своей учебы в Университете Южной Калифорнии написал опытную программку в целях эксперимента. Запустив вирус на компьютере VAX, он убедился, что его творение размножается невероятно быстро и, в зависимости от условий, может заразить всю систему за время от 5 минут до часа. Испугавшись, студент прекратил эксперимент – на календаре было 11 ноября 1983 года. А в следующем году Фред Коэн написал научную работу по данной тематике, дав определение самому понятию компьютерного вируса. И детально описав механизмы заражения систем, предугадав, как именно зловредные программы через сети станут распространяться по планете.

# Brain - самый  первый вирус в мире

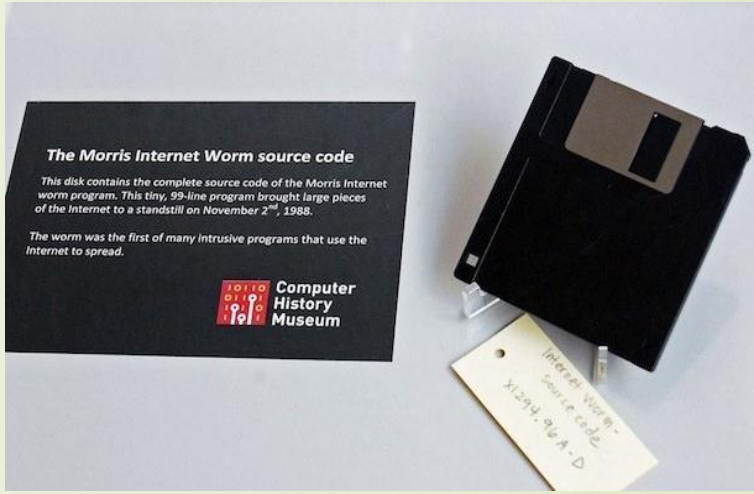
- Brain (1986 годс) оздавался как оружие возмездия против местных пиратов, ворующих созданное братьями ПО. Однако, как это нередко бывает, опасная сила вырвалась на свободу и причинила немало вреда, только в одних США было заражено порядка 18 тыс. Вирус распространялся, записывая свое тело в загрузочные сектора дискет. Если их пытались сканировать, он выставлял на обозрение вместо зараженного сектора его специально созданную нейтральную копию.



# Jerusalem


Создан в Израиле и выпущен на свободу 13 мая 1988 года, вирус «Jerusalem» напугал очень многих пользователей на Ближнем Востоке, в Европе и США. Просто потому, что антивирусы тогда были диковинкой и никто толком не знал, как с ним бороться. А вреда «Jerusalem» приносил много, например, при попытке запуска зараженного файла он сразу удалял его. А если приход пятницы совпадал с наступлением 13-го числа, что случается не так уж редко, в университетских сетях и офисах крупных компаний начиналась настоящая паника – зловред попросту форматировал жесткие диски, стирая все данные без разбора.

# «Червь Морриса» «сломал» весь тогдашний Интернет




- Стоит отметить, что в 1988 году размеры всемирной паутины были куда как меньше современных. И поэтому быстро и бесконтрольно размножающемуся червю Морриса не составило особого труда за короткий срок захватить его целиком. Ноябрь 1988 года запомнился как месяц, когда один вирус парализовал работу всего Интернета, что обернулось прямыми и косвенными убытками на общую сумму в 96 млн. долларов.

# «Michelangelo», известен тем, что стал стимулом для развития антивирусного ПО

- Сравнительно безобидный вирус «Michelangelo» (1992 год), проникавший через дискеты в загрузочные сектора ПК, где он и находился, бездействуя. И лишь 6 марта (день рождения Микеланджело), зловред активизировался и стирал все данные на компьютере. В реальности количество зараженных систем не превысило 10 тыс., но мир уже был наслышан об опасности компьютерных вирусов, поэтому охотно поддался на пропаганду разработчиков антивирусных программ. Как следствие, последние неплохо заработали и сделали отличный задел на будущее, тогда как реальный ущерб от «Michelangelo» оказался не особо велик.


YOUR LEISURE READING

Michelangelo virus attacks P.C. data worldwide

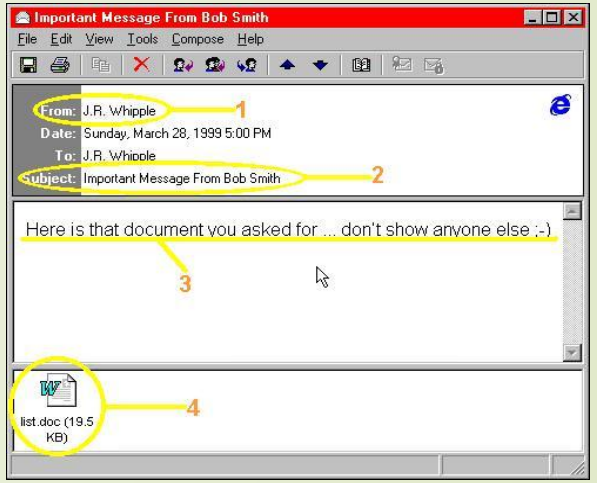
Gambling fever takes its toll in Australia

# «Win95.CIH» стирал BIOS и вывел из строя до 500 000 компьютеров

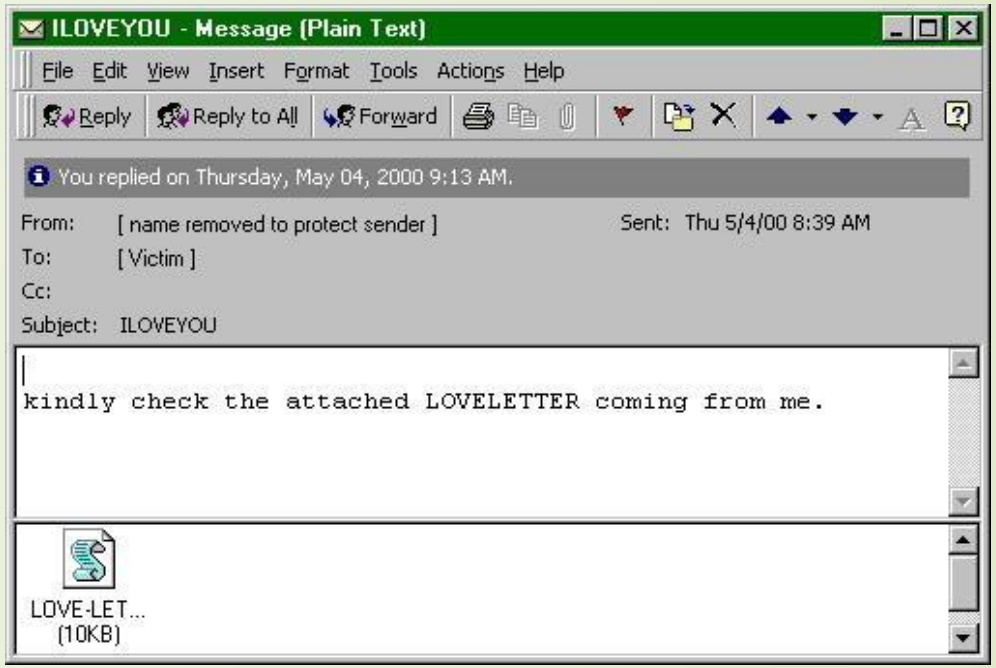
- Скандально известный и очень опасный вирус, разработанный неким тайванским студентом в 1998 году, CIH – это его инициалы. Для проникновения на компьютеры использовал все способы, включая распространение по электронной почте, на сменных носителях данных, просто через Интернет. При этом довольно умело прятался среди файлов других программ и никак себя не проявлял. Часом «Х» было 26 апреля, дата аварии на ЧАЭС, за что в Рунете вирус прозвали «Чернобылем». Проснувшийся CIH не просто форматировал данные, но и стирал содержимое BIOS, нанося уже физический вред – после этого компьютер просто не включался.
- Больше всего «Чернобыль» свирепствовал в апреле 1999 года, достоверно известно о 300 тыс. зараженных компьютеров, преимущественно в странах Восточной Азии. Бороться с вирусом, в страхе ожидая приближение очередной даты 26 апреля, пришлось еще несколько лет. По некоторым оценкам, за это время он успел проникнуть на более чем полумиллиона систем во всем мире.

# . Melissa, 1999 год, забивал спамом электронную почту

- 26 марта 1999 года мир познакомился с массовой атакой почтовых сервисов. Проникнув на очередной компьютер, Melissa разыскивала файлы приложения MS Outlook и самовольно отсылала первым 50-ти адресатам из списка контактов себя саму. Скорость распространения зловреда оказалась невероятно высокой, он за считанные дни поразил сети многих крупных компаний, включая таких IT-гигантов, как Intel и Microsoft. Рассылка велась от имени владельца зараженного компьютера, но сам он об этом и не подозревал – чтобы не допустить хаоса, многим организациям пришлось вовсе отключить свою почту. Суммарный ущерб от Melissa потом оценили в $100 млн.



# I Love You» колоссальный ущерб и повод задуматься о психологии




Также известен как «Loveletter», «The Love Bug» (2000 год) или просто «романтик», данный вирус создавался опытными злоумышленниками, которые использовали слабости человеческой природы. Очень немногие офисные работники, получив по электронной почте письмо с текстом «I Love You» и неким вложением, настораживались и включали антивирус. Большинство тут же открывали прикрепленный файл, выпуская монстра на свободу – в дальнейшем «романтик» вел себя также, как и его предшественник Melissa.

Кроме того, что он очень быстро заражал компьютеры, «I Love You» еще и крал секретные пароли, что увеличивало наносимый ущерб.

Специфическая особенность вируса позволила ему расползтись по всему

# «Nimda» - вирус с правами администратора

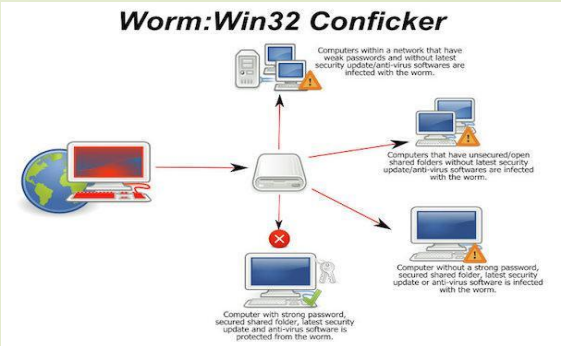
- Разработан в Китае, выпушен в Интернет 18 сентября 2001, всего через 22 минуты стал самым распространенным зловредом в Сети. Nimda был спроектирован очень грамотно, а принцип его действия основан на том, что вирус первым делом получал права администратора на зараженных компьютерах, после чего ему не составляло труда влезть в любые настройки. Собственно, название «Nimda» это «admin», но написанное наоборот и вел себя вирус именно как системный администратор, перешедший на темную сторону силы – не созидал, а разрушал компьютерные системы.

# «My Doom» - лидер по скорости заражения Сети

- «My Doom» (2004 год) - сравнительно простой вирус, который генерировал огромное количество спама и физически забивал каналы передачи данных. Каждый из свежезараженных компьютеров отсылал еще больше информационного мусора с вредоносным кодом, количество источников угрозы увеличивалось лавинообразно. Остановить это нашествие было сложно еще и потому, что вирус блокировал доступ с зараженных систем на сайты разработчиков антивирусного ПО, а также сервисы обновлений Microsoft. Более того, в итоге «My Doom» даже устроил DDoS-атаку на сайт самой компании из Редмонда.

# Conficker

- Весьма коварный вирус, написанный специально для действия в системе Microsoft Windows. Используя уязвимости ОС, Conficker (2008 год) оставался незамеченным для антивирусных программ, сам же он первым делом блокировал доступ к обновлениям их баз. Затем отключались апдейты для самой ОС, подменялись названия служб и вирус прописывался по разным закоулкам системы, так что найти и уничтожить все его фрагменты становилось почти невозможно. 12 млн. зараженных компьютеров в мире и слава одного из самых опасных зловредов в истории.

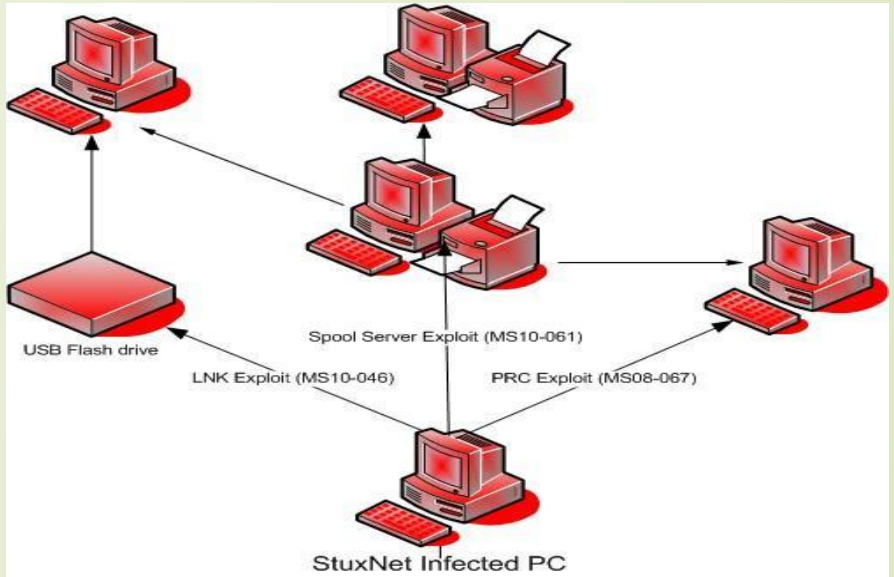


# «Win32/Stuxnet» - первый вирус, созданный для промышленных систем

Впервые обнаружен 17 июня 2010 года Сергеем Уласенем, специалистом по информационной безопасности из белорусской компании «ВирусБлокАда», который сегодня работает в «Лаборатории Касперского». Отличительная черта «Win32/Stuxnet» состоит в том, что хоть он и написан для OS Windows, этот червь заражал не только пользовательские ПК, но и промышленные автоматизированные системы. Данный вирус стал настоящей сенсацией и породил массу вопросов, спровоцировав несколько скандалов на международном уровне.

Win32/Stuxnet умеет обнаруживать и перехватывать потоки данных между контроллерами Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC, разработанными компанией Siemens

Вирус, по сути, предназначен для диверсий и шпионажа, а при необходимости он без труда разрушает зараженную систему.



# История возникновения антивирусных программ

- История развития антивирусов – это смена поколений программ, когда устаревшие методы борьбы заменяются более эффективными технологиями.
- Еще в 1975 году через *сеть* Telenet разошелся и самый первый сетевой *вирус* "TheCreeper", и впервые была создана *программа - антивирус* "Reeper
- Так *по* этому принципу вирусы распространились и в наше время через глобальную *сеть*.
- История развития антивирусов – это смена поколений программ, когда устаревшие методы борьбы заменяются более эффективными технологиями.

# Обнаружение и борьба с вирусами

- Пользователь часто может сам обнаружить присутствие вируса на компьютере.
- Обнаружение  вирусов лучше поручить специализированным программам, тем более что иногда признаки, которые пользователь расценивает как результат действия вируса, могут характеризовать системные или аппаратные сбои.
- Для борьбы с компьютерными вирусами применяются антивирусные программы.

# THE BRAIN

- Также в 86 г два брата Амджад в Пакистане открыли неизвестный доселе *вирус*. 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.

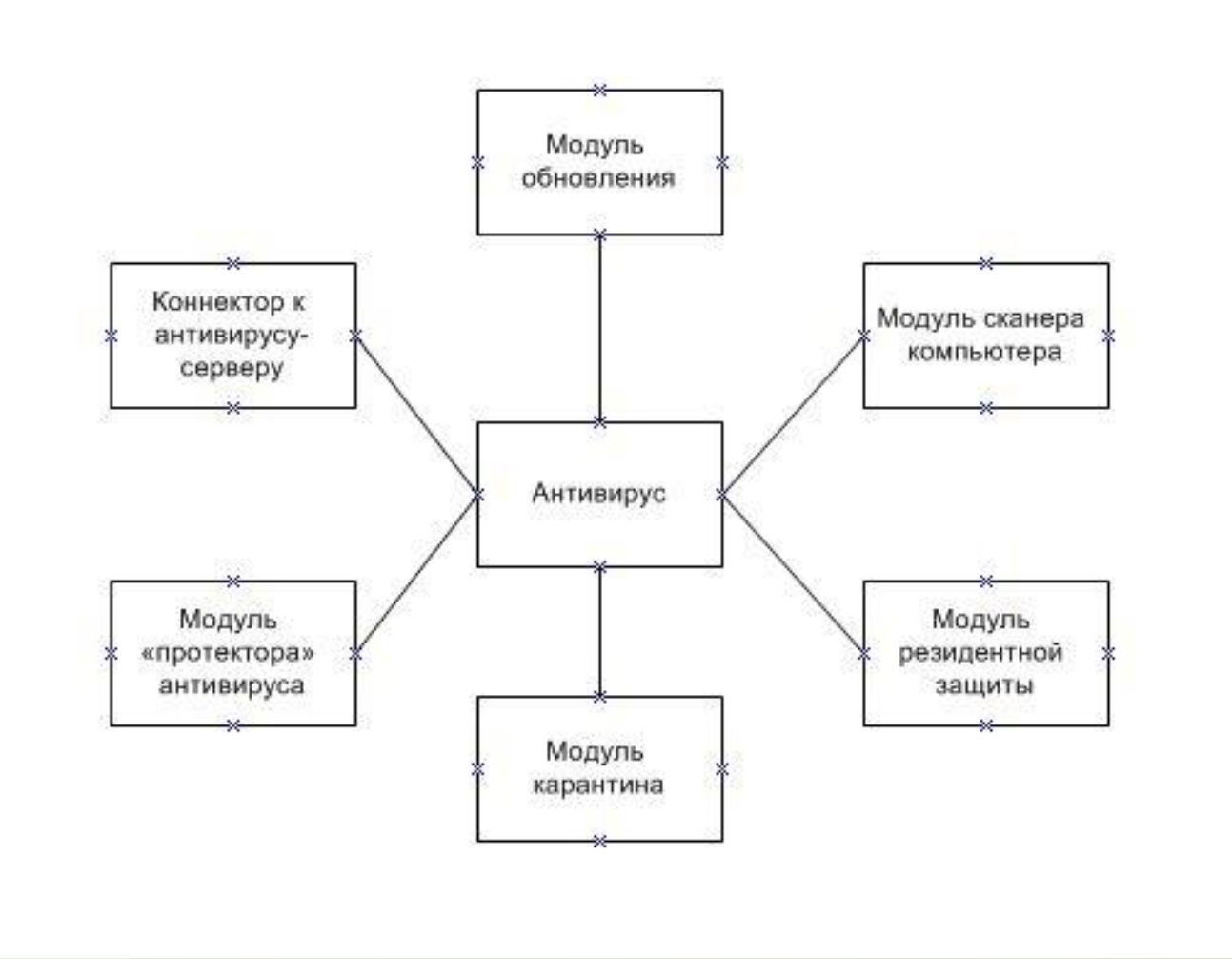
# Первая литература

- 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".

# Схема антивируса

***Антивирус* состоит из следующих частей:**

- Модуль резидентной защиты
- Модуль карантина
- Модуль "протектора" *антивируса*
- *Коннектор к антивирусу-серверу*
- Модуль обновления
- Модуль сканера компьютера



# Модуль резидентной защиты

- *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

*Модуль* карантина *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. Обычно карантин создается в особой папке антивирусной программы, которая изолирована от каких-либо действий, кроме действий со стороны *антивируса*.

# Модуль протектора

- *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*.

# *Коннектор* к *антивирусу*-серверу

*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:

# Модуль обновления

- *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

- 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 требоватьпользователь 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 пообезвреживанию 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 промежуточноговремени от проверки до проверки хватит, чтобы украсть персональные данные пользователя

# Вооружен, значит защищен!