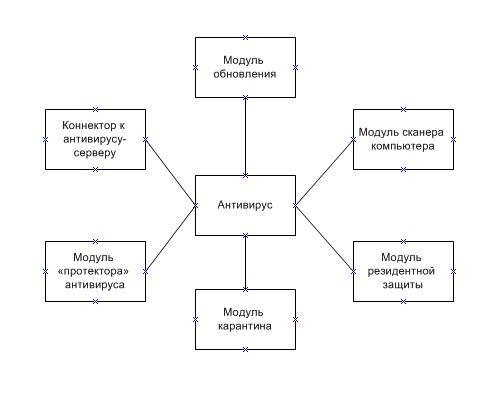
**Механизм работы современных антивирусов**

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:



**Рис. 3.1.**Схема антивируса

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

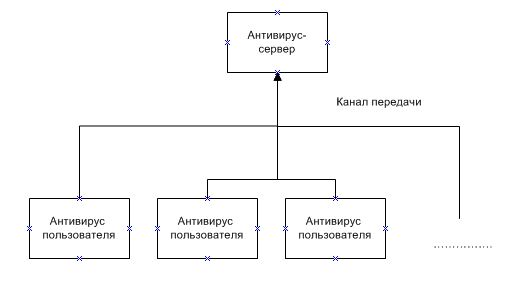
1. Модуль резидентной защиты
2. Модуль карантина
3. Модуль "протектора" *антивируса*
4. *Коннектор* к *антивирусу*-серверу
5. Модуль обновления
6. Модуль сканера компьютера

*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:



**Рис. 3.2.**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.

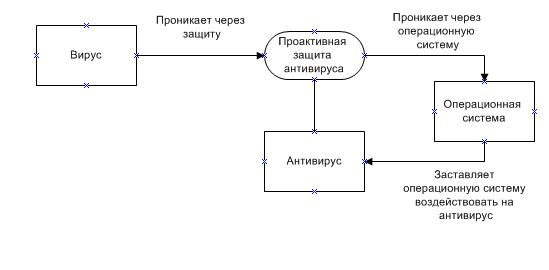
*Модуль* обновления отвечает за то, чтобы обновление *антивируса*, его отдельных частей, а также его антивирусных баз прошло правильно. В современной практике создания антивирусов стала применяться следующая идея: *модуль* обновления также должен определять подлинные или нет антивирусные базы скачивает 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.

**Надежность современных антивирусных программ**

Прежде всего, необходимо уяснить то, что абсолютно надежных антивирусных программ не бывает в принципе из-за изменчивой природы вирусов. Если говорят, что какой-либо *антивирус* является лучшим и защищает абсолютно от всех существующих вирусов, то это с большей долей вероятностью является рекламным ходом антивирусной компании, либо *антивирус* защищает от всех вирусов только в короткий промежуток времени, так как вирусы *по* всему миру выходят постоянно и неизвестно, какой именно *вирус* завтра будет бушевать на просторах сети *Интернет*. Причина такой непостоянной защищенности, которую предоставляют антивирусы проста - сначала должен появиться *вирус*, а только потом уже защита от него. И хотя в современных условиях антивирусы достаточно быстро реагируют на появление вирусов и уже в течение часа могут предоставить сигнатурную базу с описанием вируса и его лечением, все равно остается определенный промежуток времени, когда неизвестно, как лечить этот новый *вирус*. Частично проблема решается путем эвристического подхода, который позволяет блокировать вирусы, не попавшие в сигнатурные базы, но и он не всегда позволяет противостоять новым вирусам. Зачастую бывает так, что вирусописатели специально для *кражи* определенного типа данных с определенного места (например,*кража* всех логинов и паролей к *онлайн*-сервису) пишут определенный специально направленный *вирус*, который не сможет обнаружить*антивирус*. В этом случае такой *вирус* может ходить от *онлайн*-сервиса к *онлайн*-сервису до тех пор, пока он не попадет в руки антивирусной лаборатории, которая исследует *вирус* и занесет его в сигнатурную базу. Также вирусописатели изменяют свой подход к написанию вирусов в сторону улучшения их внедрения на *компьютер* пользователя. Это делается с помощью тех самых каналов связи, через которые *антивирус* получает сигнатурные базы, либо инструкции к некоторым действиям. *Вирус* просто блокирует эти каналы, и*антивирус* остается рабочим, но без обновлений и правильных сигнатурных баз. Это является благодатной почвой для вирусов, и в результате иногда случаются вирусные эпидемии на компьютерах пользователей. Во избежание этого антивирусные компании стараются максимально защищать каналы связи различными шифровальными методами, а также другими методами, которые позволили бы защитить*антивирус* от постороннего вмешательства вирусов в свою работу. Но, как бы ни старались максимально улучшить свое детище антивирусные компании, еще ни один *антивирус* не может уничтожать 100% угроз на протяжении долгого промежутка времени. Об этом говорит практика, а также различные аналитические центры. В среднем, самый лучший *антивирус* может сохранить свое преимущество перед остальными антивирусами недолгий промежуток времени, а также он будет справляться только с 70-80% от всех вирусных угроз, которые существуют (при этом во внимание берутся только распространенные угрозы. Вирусы, которые пишутся для определенной атаки на *компьютер* и фактически являющиеся одноразовыми, в этой статистике обычно не учитываются). В теории решением такой проблемы было бы использование одновременно нескольких антивирусов на одном компьютере, но это зачастую невозможно сделать из-за того, что антивирусы в этом случае будут конфликтовать между собой, усугубляя тем самым положение самого компьютера в свете защиты от вирусов. Однако существуют некоторые независимые лаборатории, в которых стоит сразу же большое количество антивирусов. Такие лаборатории могут выполнять *анализ* одного файла сразу многими антивирусами. Результат от такого анализа будет более точен, если тот же *файл* отправить на *анализ* только одному *антивирусу*. Но, несмотря на существование таких лабораторий, проблема 100% защиты от вирусов все же остается, так как лаборатория не может обеспечить постоянный надзор над компьютером, ей можно отсылать только файлы, которые вызывают подозрение у пользователя.

Существует также мнение, которое гласит, что *антивирус* никогда не сможет на 100% справляться с вирусами, потому что он является компонентом операционной системы (ее прикладной программой, хотя антивирусы и относят к системному программному обеспечению), а не ее непосредственной частью. Раньше эта проблема выглядела особенно остро, когда антивирусы и операционные системы постоянно конфликтовали между собой, причем, если *пользователь* хотел удалить *антивирус*, ему приходилось в большинстве случаев переустанавливать операционную систему, так как в ней начинались постоянные сбои и значительное снижение скорости работы. В современном периоде этот *конфликт* частично исправлен, но далеко не всегда получается так, что *антивирус* интегрируется в операционную систему без последствий. К тому же остается та проблема, что *операционная система* все равно остается "королем" (выражаясь абстрактно), а *антивирус* ее "слугой". Другими словами, если *операционная система* вынесет какие-либо действия *по*отношению к *антивирусу*, то *антивирус* не сможет отказать операционной системе. Этим непременно пытаются воспользоваться вирусописатели при написании своих детищ. Они пишут *вирус* так, чтобы он, прежде всего, воздействовал на операционную систему, которая может произвести воздействие на *антивирус*, чтобы отключить или удалить его. Схематически это может выглядеть следующим образом:



**Рис. 3.3.**Схема проникновения вируса

Из данной схемы можно увидеть следующее: *Вирус* проникает через проактивную защиту *антивируса*, далее он проникает через операционную систему и завладевает ею, заставляя операционную систему воздействовать на *антивирус*. Контролируя операционную систему, *вирус* может отдать ей любой приказ относительно *антивируса*, при этом *антивирус* не сможет противиться действиям операционной системы. Расширенной версией такой схемы является версия с попаданием и контролированием вируса системы *BIOS* (*BIOS*(англ. *basic* input/output *system* — "*базовая* система ввода-вывода") — реализованная в виде *микропрограмм* часть системного программного обеспечения, которая предназначается для обеспечения операционной системы *API* доступом к аппаратуре компьютера и подключенным к нему устройствам). В этом случае *вирус* будет контролировать абсолютно все действия, которые выполняются на компьютере, а также на любом компьютере, где есть *BIOS*. Впрочем, такие вирусы уже стали редкостью и практически не применяются в современной практике, так как проактивные защиты антивирусов не дают настолько глубоко проникнуть вирусу в *компьютер* пользователя.

Частыми случаями отказа в правильной работе антивирусов бывает недостаточно хорошая работа "протектора" *антивируса*. Обычно это происходит потому, что при написании протектора невозможно предусмотреть абсолютно все случаи возможного стороннего вмешательства в работу *антивируса*. Как показывают различные аналитические источники, современные протекторы не всегда могут обеспечить защиту *антивируса* даже в таком простом случае, когда *вирус* выдает свое действие *по* прекращению работы *антивируса* за действие пользователя. Этот факт должен напоминать пользователям о том, что необходимо быть внимательными к неожиданному прекращению работы *антивируса* и активировать его работу вручную.

**Основные моменты использования современных антивирусных программ**

Безусловно, антивирусные программы предоставляют защиту от вредоносных программ достаточно хорошо, но это не значит, что*пользователь* ничего не должен делать для поддержания этой работы и совершенно не должен следить за работой *антивируса*.*Пользователь* должен делать следующие действия, чтобы поддерживать работу *антивируса*, а также сделать ее максимально эффективной:

1. Обращать внимание на результаты работы сканера
2. Регулярно делать обновления *антивируса*
3. Периодически проверять работу резидентной защиты
4. Регулярно проверять сканером свой компьютер
5. В случае неполадок обязательно сообщать о них в службу поддержки *антивируса*
6. Регулярно просматривать отчеты *антивируса*
7. Настроить *антивирус* должным образом

Рассмотрим данные пункты более подробно:

*Пункт* №1 (обращать внимание на результаты работы сканера). Несмотря на то, что большинство современных сканеров *антивируса* сами находят вирусы и решают, что с ними делать, *пользователь* должен обращать внимание на результаты работы сканера. Это необходимо делать потому, что иногда *сканер* может допустить ошибку и поместить в карантин абсолютно безвредный *файл* (например, *файл* одного из свежеустановленных драйверов). Если *пользователь* уверен в том, что *антивирус* поместил в карантин *файл* *по* ошибке, то его необходимо изъять из карантина, так как в карантине *файл* не может совершать каких-либо действий, и от этого может пострадать работа компьютера в целом. Чтобы уверенность была объективной, необходимо проверить действительную принадлежность файла к лицензионному программному средству, либо к операционной системе (обычно на сайте производителя программного обеспечения можно узнать такую информацию) и если *программа* является свеже установленной, то можно изъять такой *файл* из карантина. Правда, в некоторых случаях необходимо помнить, что это делается на страх и риск пользователя, и до конца быть уверенным, что *файл* является безопасным, все равно нельзя. Также бывают случаи, когда *пользователь* мог набирать код программного средства в текстовом редакторе, а при проверке сканером такой документ может быть помещен в карантин, если код содержит какие-либо опасные с точки зрения безопасности вставки, не считая того, что это *файл* документа, который не может быть исполняемым файлом *по* определению.

*Пункт* №2 (регулярно делать обновления *антивируса*). От соблюдения этого пункта фактически зависит *безопасность* персональных данных пользователя, а также эффективность работы *антивируса* в целом. Стоит отметить, что обновления *антивируса* предусмотрены самим антивирусом, то есть *антивирус* регулярно проверяет себе обновления, но бывает и так, что *планировщик* обновлений сбивается, и приходится обновлять *антивирус* вручную. *Пользователь* должен помнить этот факт и внимательно следить за обновлениями *антивируса*, потому что без актуальных баз *антивирус* не сможет качественно выполнять свои функции *по* защите компьютера от вирусов.

*Пункт* №3 (периодически проверять работу резидентной защиты). Обычно резидентная защита включена *по* умолчанию постоянно и не должна быть выключена в какой-либо промежуток времени. Но известны случаи, когда при установке программного обеспечения резидентная защита *антивируса* временно отключается с целью обеспечить плавную установку нового программного обеспечения. При этом после установки программного обеспечения необходимо проверить, была ли включена снова резидентная защита *антивируса*, так как бывают случаи, когда она не активируется снова. Также целесообразно периодически проверять правильность самой работы резидентной защиты в целях профилактики работы *антивируса*. В этом могут помочь специальные лжевирусы, которые сами *по* себе не приносят вреда компьютеру, но создаются специально для того, чтобы проверить правильность работы резидентной защиты. Обычно такие лжевирусы выпускают различные аналитические компании, а также независимые пользователи, которые заинтересованы в регулярной проверке резидентной защиты *антивируса*. Такие "вирусы" можно скачать из сети *Интернет* (обычно они предоставляются открыто). Все эти меры помогут поддерживать правильность работы резидентной защиты. Если же в результате подобных проверок будет обнаружено, что резидентная защита не справляется полностью со своими функциями, необходимо связаться с создателями *антивируса* и описать проблему, либо вообще сменить антивирусную программу.

*Пункт* №4 (регулярно проверять сканером свой *компьютер*). Данный *пункт* является профилактикой заражения компьютера различными вирусами. *Пользователь* должен помнить, что не всегда резидентная защита *антивируса* может остановить абсолютно все угрозы, связанные с вирусами, и поэтому необходимо периодически устраивать проверки сканером *антивируса*. Такие проверки исключат возможность нахождения различных вирусов на компьютере. Проверки необходимо делать хотя бы раз в месяц и проверять *компьютер*необходимо полностью.

*Пункт* №5 (в случае неполадок обязательно сообщать о них в службу поддержки *антивируса*). Многие пользователи, обнаруживая какие-либо неполадки в работе антивирусной программы, пытаются сами исправить эти неполадки, даже если не совсем понимают, как именно это надо делать. А вместе с тем любая неполадка, даже самая незначительная на первый взгляд, может нести в себе элементы опасности для безопасной работы компьютера. Ведь зачастую остается неизвестной причина самой неполадки. Может быть, неполадка вызвана конфликтом операционной системы с антивирусом, может, программным обеспечением компьютера, а может и зловредной программой, которая хочет полностью отключить защиту *антивируса*. Поэтому при любых неполадках, даже самых незначительных, *пользователь*должен обращаться в службу поддержки *антивируса* с четким и понятным описанием проблемы, которая возникла в работе *антивируса*. Создатели *антивируса* гораздо более быстро выяснят причину неполадок и зачастую смогут дать полезные советы *по* обращению с их детищем. Необходимо помнить, что даже, казалось бы, безобидное временное прекращение работы резидентной защиты или кратковременное отключение обновлений *антивируса* может говорить о том, что на компьютере присутствует *вирус*, который надо как можно скорее обезвреживать.

*Пункт* №6 (регулярно просматривать отчеты *антивируса*). Это действие, которое является больше профилактическим, а также позволит лучше понять, что именно происходит на компьютере пользователя. Отчеты *антивируса* предназначены, в первую *очередь*, для самих пользователей, чтобы пользователи могли наглядно увидеть работу *антивируса*, узнать, какие файлы заблокировала резидентная защита, определить, когда было совершено последнее обновление *антивируса* (и удачно ли оно было совершено). Именно на основе отчетов можно понять, правильно ли *антивирус* выполняет свои функции, либо в его работе начались какие-либо неполадки, сбои. Увидеть это можно простым путем - если в отчетах стали появляться сообщения о неудачах работы *антивируса*, о его частых ошибках, либо отказе в каких-либо действиях, то можно быть уверенным, что были постоянные сбои в работе *антивируса*, и что он работает неправильно. Соответственно, в таком случае необходимо обязательно сообщить об этом в службу поддержки *антивируса*.

*Пункт* №7 (настроить *антивирус* должным образом). От правильной настройки *антивируса* зависит общая защищенность компьютера. Казалось бы, это очевидный факт, но многие пользователи забывают должным образом настроить свою антивирусную программу, а используют ее так, как она поставляется ему с сайта производителя. Это неверный подход, так как настройки современного *антивируса*достаточно богаты и можно "подогнать" антивирусное средство именно под свой *компьютер*, а также не упустить различные моменты в контролировании антивирусным средством компьютера. Настройки современных антивирусов позволяют задать четкое количество полных проверок компьютера, различные исключения для файлов (чтоб нужный *файл* нужной программы не попал в карантин *антивируса*), а также сделать так, чтобы *антивирус* полностью удовлетворял потребностям пользователя. Основной настройке подлежит *планировщик*заданий *антивируса* – важный *компонент*, который позволяет делать действия (проверять обновления, проверять *компьютер*) в определенные отрезки времени. Настроив его, *пользователь* может не беспокоиться о том, что может забыть проверить *компьютер* или скачать обновления для *антивируса*. Хотя стоит упомянуть о том, что периодически необходимо все же проверять правильность работы планировщика, чтобы неожиданно не обнаружить, что антивирусная *программа* не обновлена или полная проверка компьютера не была произведена.