Лекция №24. Защита от вредоносных программ и спама.

[1. Классификация вредоносных программ 1](#_Toc511786778)

[1.1. Компьютерные вирусы 1](#_Toc511786779)

[1.2. Сетевые черви 2](#_Toc511786780)

[1.3. Троянские программы 3](#_Toc511786781)

[1.5. Шпионское ПО (Spyware) 5](#_Toc511786782)

[1.6. Хакерские утилиты (RootKit) 5](#_Toc511786783)

[2. Основы работы антивирусных программ 6](#_Toc511786784)

[2.1. Сигнатурный анализ 6](#_Toc511786785)

[2.2. Проактивные методы обнаружения 7](#_Toc511786786)

[2.2.1. Эвристические анализаторы 7](#_Toc511786787)

[2.2.2. Поведенческие блокираторы 8](#_Toc511786788)

[2.3. Дополнительные модули 9](#_Toc511786789)

[2.4. Режимы работы антивирусов 10](#_Toc511786790)

[2.4.1. Проверка в режиме реального времени 10](#_Toc511786791)

[2.4.2. Проверка по требованию 10](#_Toc511786792)

[2.4.3. Тестирование работы антивируса 11](#_Toc511786793)

[2.5. Антивирусные комплексы 12](#_Toc511786794)

[2.6. Дополнительные средства защиты 13](#_Toc511786795)

# Классификация вредоносных программ

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.

В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на следующие типы: компьютерный вирус, червь, троян, шпионское ПО (spyware), хакерские утилиты (rootkit).

Следует отметить, что компьютерным вирусом часто называют любую вредоносную программу. Это обусловлено тем, что первые известные вредоносные программы были именно компьютерными вирусами, и в течение последующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем числе инцидентов с вредоносными программами за последние годы значительно сократилась.

В настоящее время вредоносные программы – это уже большей частью именно не вирусы, хотя такие термины, как «вирус» и «заражение вирусом», применяются по отношению ко всем вредоносным программам. Поэтому далее под термином «вирус» будет пониматься и вредоносная программа.

## Компьютерные вирусы

**Компьютерный вирус – это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.**

Основная цель любого компьютерного вируса – это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 25-го числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

* + 1. проникновение на чужой компьютер;
    2. активация;
    3. поиск объектов для заражения;
    4. подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения – фактически все каналы, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевых ресурсов – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

* + - *загрузочные вирусы* – заражают загрузочные сектора жестких дисков и мобильных носителей;
    - *файловые вирусы* – заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например, Linux, UNIX или macOS.

При подготовке своих копий вирусы могут применять для маскировки разные технологии:

* + - *шифрование* – в этом случае вирус состоит из двух частей: сам вирус и шифратор;
    - *метаморфизм* – при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно, в зависимости от используемых методов маскировки вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

## Сетевые черви

В отличие от вирусов, сетевые черви – это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему черви делятся на следующие типы:

* + 1. *сетевые черви* – используют для распространения локальные сети и Интернет;
    2. *почтовые черви* – распространяются с помощью почтовых программ;
    3. *IM-черви* – используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
    4. *P2P-черви* – распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer – равный с равным).

После проникновения на компьютер червь должен активироваться – иными словами, запуститься. По методу активации все черви можно разделить на две большие группы: на тех, которые требуют активного участия пользователя, и тех, кто его не требует.

Отличительная особенность червей из первой группы – это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий – такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые черви могут кооперироваться с вирусами – такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

## Троянские программы

Троянская программа (программа класса «троянский конь») имеет только одно назначение – нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются.

Жизненный цикл троянов состоит всего из трех этапов:

* + - проникновение в систему;
    - активация;
    - выполнение вредоносных действий.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем – то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя – либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель троянов – это выполнение несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

* + - *похитители паролей* предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат;
    - *утилиты скрытого удаленного управления* – это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных;
    - *логические бомбы* характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, в ответ на определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов;
    - *клавиатурные шпионы*, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры, с целью последующей их передачи своему автору;
    - *анонимные SMTP- и прокси-серверы* – такие трояны на зараженном компьютере организуют несанкционированную отправку электронной почты, что часто используется для рассылки спама;
    - *модификаторы настроек браузера* меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.

Отдельно отметим, что существуют программы из класса троянов, которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы – *организаторы DDoS-атак.*

* 1. Условно опасные программы

Условно (или потенциально) опасные программы не классифицируются как вирусы, но могут, тем не менее, нанести ущерб пользователю. Сами по себе они не являются вредоносными и не содержат в себе деструктивный код. Можно выделить следующие типы условно-опасных программ: adware и riskware.

Adware — это программы, которые предназначены для показа рекламы на вашем компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о вас (например, какого рода сайты вы посещаете), чтобы реклама соответствовала вашим интересам.

Adware-программы, которые собирают данные с вашего согласия, не следует путать с троянскими программами-шпионами, которые собирают информацию без вашего разрешения и ведома. Если Adware-программа не уведомляет о сборе информации, она считается вредоносной, например, вредоносная программа троянец-шпион (Trojan-Spy).

За исключением показа рекламы и сбора данных такие программы, как правило, не проявляют своего присутствия в системе. Обычно у такой программы отсутствует значок на панели задач, и в меню программ она тоже отсутствует.

Adware-программы могут попасть на ваш компьютер с бесплатным или условно-бесплатным программным обеспечением. Adware-программы могут входить на вполне законных основаниях в состав некоторых бесплатных или условно-бесплатных программ в качестве рекламной составляющей. Доходы от такой рекламы помогают финансировать их разработку.

Посещение зараженного веб-сайта может привести к несанкционированной установке Adware-программы на ваш компьютер. В этих целях часто используются хакерские технологии. Например, для проникновения на компьютер может использоваться уязвимость браузера и троянская программа, предназначенная для незаметной установки Adware. Действующие таким образом Adware-программы часто называют Browser Hijackers.

К категории Riskware относят легальные программы, которые могут причинить вред компьютеру, если используются злоумышленниками для удаления, блокирования, изменения или копирования данных, а также для нарушения работы компьютеров и сетей. В категорию Riskware входят следующие виды программ, которые широко используются в легальных целях: утилиты удаленного администрирования, программы для загрузки файлов, программное обеспечение для мониторинга активности компьютеров, утилиты управления паролями, серверные веб-службы, такие как FTP, Web, Proxy и Telnet.

По своему назначению это не вредоносные программы, но некоторые их функции могут быть использованы во вредоносных целях.

При таком большом количестве легальных программ, которые злоумышленники могут использовать в незаконных целях, нелегко решить, какие из программ представляют угрозу. Например, программы удаленного администрирования часто используются системными администраторами и службами поддержки клиентов для диагностики и устранения неполадок, возникающих на компьютерах пользователей. Однако если такая программа установлена на вашем компьютере злоумышленником (без вашего ведома), он получит удаленный доступ к вашему компьютеру. Полностью контролируя ваш компьютер, злоумышленник сможет использовать его практически в любых нужных ему целях.

Так как Riskware-программы могут присутствовать на компьютере на законных основаниях, антивирусы не всегда могут определить степень опасности конкретной Riskware-программы.

Существует много причин, чтобы подозревать обнаруженную антивирусной программой Riskware-программу в том, что она представляет собой угрозу. Например, если вы не давали согласия на установку программы и не знаете о ее происхождении.

## Шпионское ПО (Spyware)

*Шпионское ПО* (*Spyware*) – опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне – создателю или заказчику такой программы. Среди заказчиков шпионского ПО – спамеры, маркетинговые агентства, спам-агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы интересуются системными данными, типом браузера, посещаемыми веб- узлами, иногда и содержимым файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере – нестабильная работа браузера и замедление производительности системы;

## Хакерские утилиты (RootKit)

Первоначально термин rootkit означал набор вредоносных приложений, скрывающих свое присутствие на компьютере и позволяющих хакеру делать свои дела незаметно. Слово root в названии явно указывает, что слово зародилось в мире Unix-компьютеров, но сегодня, когда мы говорим о руткитах, как правило речь ведется о Windows-компьютерах, и в понятие «руткит» включаются не только средства обеспечения скрытности, но и весь набор функций вредоносного приложения. Оно обычно прячется глубоко в недрах операционной системы и специально написано таким образом, чтобы избегать обнаружения антивирусами и другими средствами безопасности. Руткит может содержать различные вредоносные инструменты, такие как клавиатурный шпион, вор сохраненных паролей, сканер данных о банковских карточках, дистанционно управляемый бот для осуществления DDoS-атак, а также функции для отключения антивирусов.

Руткит обычно имеет также функции бэкдора, то есть он позволяет атакующему дистанционно подключаться к зараженному компьютеру, устанавливать или удалять дополнительные модули и таким образом делать с машиной все, что подскажет фантазия. Некоторые примеры актуальных сегодня руткитов для Windows это TDSS, ZeroAccess, Alureon and Necurs.

Руткиты делятся на две категории: уровня пользователя и уровня ядра. Первые получают те же права, что обычное приложение, запущенное на компьютере. Они внедряются в другие запущенные процессы и используют их память. Это более распространенный вариант. Что касается руткитов уровня ядра, то они работают на самом глубинном уровне ОС, получая максимальный уровень доступа на компьютере. После инсталляции такого руткита, возможности атакующего практически безграничны. Руткиты уровня ядра обычно более сложны в создании, поэтому встречаются реже. Также их гораздо сложней обнаружить и удалить.

Есть и еще более экзотические вариации, такие как буткиты (bootkit), которые модифицируют загрузчик компьютера и получают управление еще даже до запуска операционной системы. В последние годы появились также мобильные руткиты, атакующие смартфоны под управлением Android.

Первично руткиты попадают на компьютер так же, как другие вредоносные приложения. Обычно используется уязвимость в браузере или плагине, также популярный способ заражения – через USB-флешки. Атакующие иногда даже оставляют зараженные флешки в общественных местах, где их может подобрать подходящая жертва. Затем руткит использует уязвимости ОС чтобы получить привилегированное положение в системе и устанавливает дополнительные компоненты, обеспечивающие удаленный доступ к компьютеру и другую вредоносную функциональность.

Основная сложность борьбы с руткитами в том, что они активно противодействуют своему обнаружению, пряча свои файлы и ключи реестра от сканирующих программ, а также применяя другие методики. Существуют утилиты, специально созданные для поиска известных и неизвестных руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа.

# Основы работы антивирусных программ

Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами, и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно. В современных антивирусных продуктах используются два основных подхода к обнаружению вредоносных программ: сигнатурный и проективный/эвристический.

*Сигнатурные методы* – точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

*Проактивные*/*эвристические методы* – приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

## Сигнатурный анализ

Термин «сигнатура» происходит от английского слова signature, означающего «подпись», или же в переносном смысле «характерная черта, нечто идентифицирующее».

Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиске вирусов путем сравнения файлов с выявленными чертами.

Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют *антивирусную базу*.

Эта технология предполагает непрерывное отслеживание новых экземпляров зловредов, их описание и включение в базу сигнатур. Задачу выделения сигнатур, как правило, решают люди – эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска. В наиболее простых случаях могут применяться специальные автоматизированные средства выделения сигнатур, например, для несложных по структуре троянов или червей, которые не заражают другие программы, а целиком являются вредоносными программами.

Практически в каждой компании, выпускающей антивирусы, есть своя группа экспертов, выполняющая анализ новых вирусов и пополняющая антивирусную базу новыми сигнатурами. По этой причине антивирусные базы в разных антивирусах отличаются. Тем не менее между антивирусными компаниями существует договоренность об обмене образцами вирусов, а значит, рано или поздно сигнатура нового вируса попадает в антивирусные базы практически всех антивирусов. Лучшим же антивирусом будет тот, для которого сигнатура нового вируса была выпущена раньше всех.

Часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому количество сигнатур не всегда равно количеству обнаруживаемых вирусов. Соотношение количества сигнатур и числа известных вирусов для каждой антивирусной базы свое. Если же учесть, что антивирусные компании обмениваются образцами вирусов, можно с высокой долей уверенности считать, что антивирусные базы наиболее известных антивирусов эквивалентны. Важное дополнительное свойство сигнатур – точное и гарантированное определение типа вируса. Это свойство позволяет занести в базу не только сами сигнатуры, но и способы лечения вируса.

Главные критерии эффективности сигнатурного метода – это скорость реакции на новые угрозы, частота обновлений, максимальное число обнаруженных угроз.

Главный недостаток сигнатурного метода – задержка при реакции на новые угрозы. Для получения сигнатуры необходимо иметь образец вируса. Создать его сигнатуру невозможно, пока вирус не попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления нового вируса. С момента появления вируса в сети Интернет до выпуска первых сигнатур обычно проходит несколько часов, и все это время вирус способен заражать компьютеры почти беспрепятственно. Именно поэтому традиционный сигнатурный метод непригоден для оперативной защиты от вновь появляющихся вирусов.

## Проактивные методы обнаружения

Проактивные методы обнаружения вирусов получают все большее распространение. В принципе, использование этой технологии позволяет обнаруживать еще неизвестные вредоносные программы. Существует несколько подходов к проактивной защите. Рассмотрим два наиболее популярных подхода: эвристические анализаторы и поведенческие блокираторы.

### Эвристические анализаторы

Слово «эвристика» происходит от греческого глагола «находить». Суть *эвристических методов* состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Такое определение звучит достаточно сложно, поэтому эвристический метод поясним далее на примерах.

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на предположении (весьма правдоподобном), что новые вирусы часто оказываются похожи на какие-либо из уже известных. Такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Этот эвристический метод часто называют *поиском вирусов, похожих на известные*, или *статическим анализом.*

*Эвристический анализатор* (*эвристик*) – это программа, которая анализирует программный код проверяемого объекта и по косвенным признакам определяет, является ли объект вредоносным. Работа эвристического анализатора, как правило, начинается с поиска в программном коде подозрительных признаков (команд), характерных для вредоносных программ.

Например, многие вредоносные коды ищут исполняемые программы, открывают найденные файлы и изменяют их. Эвристический анализатор просматривает код приложения и, встретив подозрительную команду, увеличивает некий «счетчик подозрительности» для данного приложения. Если после просмотра всего кода значение счетчика превышает заданное пороговое значение, то объект признается подозрительным.

Первые эвристические анализаторы появились в антивирусных продуктах довольно давно, и на сегодняшний день более или менее совершенные эвристики реализованы во всех антивирусных решениях. Достоинствами статического анализа являются простота реализации, высокая скорость работы, возможность обнаружения новых неизвестных вирусов еще до того, как для них будут выделены сигнатуры.

Однако уровень обнаружения новых вредоносных кодов остается довольно низким, а вероятность ложных срабатываний – высокой. Поэтому в современных антивирусах статический анализ используются в сочетании с динамическим.

Идея такого комбинированного подхода состоит в том, чтобы до того, как приложение будет запущено на компьютере пользователя, эмулировать его запуск в безопасном виртуальном окружении, которое называется также буфером эмуляции, или «песочницей».

Динамический эвристический анализатор читает часть кода приложения в буфер эмуляции антивируса и с помощью специальных приемов эмулирует его исполнение. Если в процессе этого псевдоисполнения обнаруживаются какие-либо подозрительные действия, объект признается вредоносным и его запуск на компьютере пользователя блокируется.

В отличие от статического метода, динамический более требователен к ресурсам ПК, так как для анализа приходится использовать безопасное виртуальное пространство, а запуск приложения на компьютере пользователя откладывается на время анализа. Однако и уровень обнаружения вредителей у динамического метода значительно выше статического, а вероятность ложных срабатываний существенно меньше.

Недостатки эвристических анализаторов:

* + - невозможность лечения – в силу потенциальных ложных срабатываний и возможного неточного определения типа вируса попытка лечения может привести к большим потерям информации, чем из-за самого вируса, а это недопустимо;
    - низкая эффективность против принципиально новых типов вирусов.

### Поведенческие блокираторы

Поведенческий блокиратор – это программа, которая анализирует поведение запущенного приложения и блокирует любые опасные действия.

К основным вредоносным действиям относят:

* + - удаление файла;
    - запись в файл;
    - запись в определенные области системного реестра;
    - открытие порта на прослушивание;
    - перехват данных, вводимых с клавиатуры;
    - рассылка писем и др.

Выполнение каждого такого действия по отдельности не дает повода считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например, перехватывает данные, вводимые с клавиатуры, и с определенной частотой пересылает их на какой-то адрес в Интернете, значит, эта программа по меньшей мере подозрительна.

В отличие от эвристических анализаторов, где подозрительные действия отслеживаются в режиме эмуляции (динамический эвристик), поведенческие блокираторы работают в реальных условиях.

Принцип действия первых поведенческих блокираторов был прост. При обнаружении потенциально опасного действия задавался вопрос пользователю: разрешить или запретить это действие. Во многих случаях такой подход работал, но «подозрительные» действия производили и легитимные программы (вплоть до операционной системы). Поэтому если пользователь не обладал должной квалификацией, вопросы антивируса вызывали непонимание.

Современные поведенческие блокираторы анализируют уже не отдельные действия, а последовательность операций. Другими словами, заключение об опасности того или иного приложения выносится на основе более сложного анализа. Таким образом, удается значительно сократить количество запросов к пользователю и повысить надежность детектирования.

Современные поведенческие блокираторы способны контролировать широкий спектр событий, происходящих в системе. Это прежде всего контроль опасной активности (анализ поведения всех процессов, запущенных в системе, сохранение всех изменений, производимых в файловой системе и реестре).

При выполнении некоторым приложением набора подозрительных действий выдается предупреждение пользователю об опасности данного процесса. Помимо этого, блокиратор позволяет перехватить все возможности внедрения программного кода в чужие процессы. Вдобавок блокиратор способен обнаружить руткиты, то есть программы, которые скрывают от пользователя работу вредоносного кода с файлами, папками и ключами реестра, а также прячут запущенные программы, системные службы, драйверы и сетевые соединения. Особо стоит выделить такую функциональность поведенческих блокираторов, как контроль целостности приложений и системного реестра Microsoft Windows. В последнем случае блокиратор контролирует изменения ключей реестра и позволяет задавать правила доступа к ним для различных приложений. Все вместе это позволяет осуществить откат изменений после определения опасной активности в системе. Таким образом, можно восстанавливать систему даже после вредоносных действий неизвестных программ, вернув ее к незараженному состоянию.

Любой поведенческий блокиратор на определенном этапе требует вмешательства пользователя, что предполагает наличие у последнего определенной квалификации. На практике пользователь часто не обладает необходимыми знаниями, поэтому информационная поддержка – фактически поддержка принятия решений – является обязательным атрибутом современных антивирусных решений.

Поведенческий блокиратор может предотвратить распространение как известного, так и неизвестного (написанного после создания блокиратора) вируса, что является неоспоримым достоинством такого подхода к защите.

Недостатком поведенческих блокираторов остается срабатывание на действия ряда легитимных программ. Для принятия окончательного решения о вредоносности приложения требуется вмешательство пользователя, что предполагает наличие у него достаточной квалификации.

Проактивный подход к борьбе с вредоносными программами стал ответом разработчиков антивирусов на все возрастающий поток новых вредителей и увеличивающуюся скорость их распространения. Существующие сегодня проактивные методы действительно позволяют бороться со многими новыми угрозами. Однако проактивные технологии не позволяют полностью отказаться от обновлений антивирусной защиты. Проактивные методы, так же, как и сигнатурные, требуют регулярных обновлений.

Для оптимальной антивирусной защиты необходимо сочетание проактивных и сигнатурных подходов. Максимального уровня обнаружения угроз можно достигнуть, только комбинируя эти методы.

Практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

## Дополнительные модули

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса – для того чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

***Модуль обновления***

Каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вирусов сегодня является сигнатурный анализ, который полагается на использование антивирусной базы.

Чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют образцы новых вирусов и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, применяющих соответствующую антивирусную программу. Именно эту задачу и решает модуль обновления.

После того как эксперты создали новые сигнатуры, файлы с сигнатурами размещаются на серверах компании – производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

***Модуль планирования***

Модуль планирования является вторым важным вспомогательным модулем. Существует ряд действий, которые антивирус должен выполнять регулярно: проверять весь компьютер на наличие вирусов и обновлять антивирусную базу.

В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур для обновления антивирусной базы буквально каждый час. Разумным расписанием для компьютера можно считать проверку раз в неделю. Модуль планирования позволяет настроить периодичность выполнения этих действий.

***Модуль управления***

По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. Основные требования к такому модулю – удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают антивирусы для домашнего использования.

Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами. Такие антивирусы оборудованы специальным модулем управления.

Основные свойства этого модуля управления:

* + - *поддержка удаленного управления и настройки* – администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места;
    - *защита настроек от изменений* – модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации.

***Карантин***

Во многих антивирусах среди вспомогательных средств имеется специальная технология – карантин, – которая защищает от возможной потери данных в результате действий антивируса.

Например, нетрудно представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса.

Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит, с определенной вероятностью антивирус мог удалить незараженный файл. Или же антивирус обнаруживает важный документ, зараженный вирусом, и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация.

От таких случаев желательно застраховаться. Это можно сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда, если окажется, что файл был удален ошибочно или потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

## Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты – ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер, и выключаться только после завершения работы всех программ.

Однако, с другой стороны, пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей прикладной задачи, и антивирусная защита не должна ему мешать это сделать. Оптимальный выход в этой ситуации – это введение двух различных режимов работы антивирусных средств:

* + - непрерывная проверка на наличие вирусов с небольшой функциональностью в режиме реального времени;
    - тщательная проверка на наличие вирусов по запросу пользователя.

### Проверка в режиме реального времени

Проверка в режиме реального времени обеспечивает непрерывность работы антивирусной защиты. Это реализуется с помощью обязательной проверки всех действий, совершаемых другими программами и самим пользователем, на предмет вредоносности вне зависимости от их исходного расположения – будь то свой жесткий диск, внешние носители информации, другие сетевые ресурсы или собственная оперативная память. Также проверке подвергаются все косвенные действия через третьи программы. Режим постоянной проверки защиты системы от заражения должен быть включен с момента начала загрузки операционной системы и выключаться только в последнюю очередь.

### Проверка по требованию

В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Допустим, что на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров, и, следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя – распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса – проверка по требованию.

Для такого режима пользователь обычно сам указывает, какие файлы, каталоги или области диска необходимо проверить, и время, когда нужно произвести такую проверку, – в виде расписания или разового запуска вручную. Рекомендуется проверять все чужие внешние носители информации, такие как дискеты, компакт-диски, флэш- накопители, каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.

### Тестирование работы антивируса

После того как антивирус установлен и настроен, необходимо убедиться, что все сделано правильно и антивирусная защита работает. Как проверить работу антивируса?

Использовать для тестирования настоящие вирусы крайне опасно. Если пользователь неправильно выполнил установку или настройку антивируса, то в процессе такого тестирования он может заразить свой компьютер, потеряв в результате данные или став источником заражения для других компьютеров.

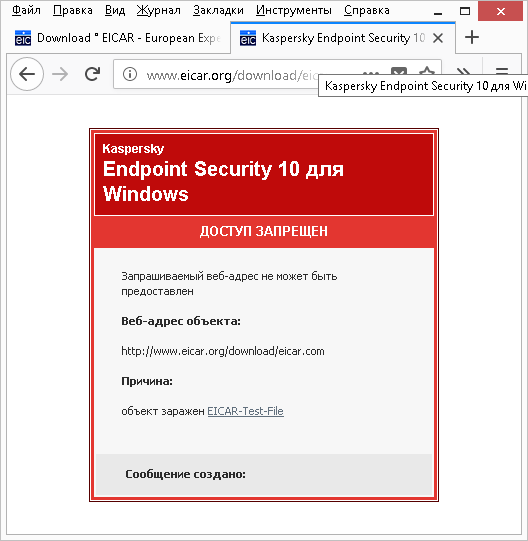
Нужен такой способ тестирования антивирусов, который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус.

Учитывая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, названный по имени организации – eicar.com.

Eicar.com – это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку «EICAR-STANDARD-ANTIVIRUS-TEST-FILE!».

Получить eicar.com можно на сайте организации EICAR по адресу <http://www.eicar.org/85-0-Download.html>.

Файл eicar.com позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами – большинством троянов, некоторыми червями. При попытке загрузить файл eicar.com антивирус блокирует доступ к файлу.



## Антивирусные комплексы

Второй способ оптимизации работы антивируса – это создание различных его версий для компьютеров, служащих разным целям. Зачастую они отличаются лишь наличием тех или иных специфических модулей и различием в интерфейсе, в то время как непосредственно антивирусная проверка осуществляется одной и той же подпрограммой, называемой антивирусным ядром.

*Антивирусный комплекс* – набор антивирусов, использующих одинаковое антивирусное ядро, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Всякая локальная сеть, как правило, содержит компьютеры двух типов: рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей. В соответствии с характером выполняемых функций серверы делятся на:

* + - *сетевые*, которые обеспечивают централизованное хранилище информации: файловые серверы, серверы приложений и др.;
    - *почтовые*, на которых работает программа, служащая для передачи электронных сообщений от одного компьютера к другому;
    - *шлюзы*, отвечающие за передачу информации из одной сети в другую. Например, шлюз необходим для соединения локальной сети с Интернетом.

Соответственно, различают четыре вида антивирусных комплексов – для защиты рабочих станций, файловых серверов, почтовых систем и шлюзов.

*Рабочие станции* – это компьютеры локальной сети, за которыми непосредственно работают пользователи. Главной задачей комплекса для защиты рабочих станций является обеспечение безопасной работы на рассматриваемом компьютере – для этого необходимы проверка в режиме реального времени, проверка по требованию и проверка локальной электронной почты.

*Сетевые серверы* – это компьютеры, специально выделенные для хранения или обработки информации. Они обычно не используются для непосредственной работы за ними, и поэтому, в отличие от рабочих станций, проверка электронной почты на наличие вирусов тут не нужна. Следовательно, антивирусный комплекс для файловых серверов должен производить проверку в режиме реального времени и проверку по требованию.

Антивирусный комплекс для защиты *почтовых систем* предназначен для проверки всех проходящих электронных писем на наличие в них вирусов. То есть проверять другие файлы, размещенные на этом компьютере, он не обязан (для этого существует комплекс защиты сетевых серверов). Поэтому к нему предъявляются требования по наличию собственно программы для проверки всей принимаемой и отправляемой почтовой корреспонденции в режиме реального времени и дополнительно механизма проверки по требованию почтовых баз данных.

Аналогично, в соответствии со своим назначением, антивирусный комплекс для *шлюза* осуществляет только проверку проходящих через шлюз данных.

Поскольку все вышеперечисленные комплексы используют сигнатурный анализ, то в обязательном порядке в них должно входить средство для поддержания антивирусных баз в актуальном состоянии, то есть механизм их обновления. Дополнительно часто оказывается полезным модуль для удаленного централизованного управления, который позволяет системному администратору со своего рабочего места настраивать параметры работы антивируса, запускать проверку по требованию и обновление антивирусных баз.

## Дополнительные средства защиты

Возможности антивирусных программ расширяют дополнительные средства защиты от вредоносных программ и нежелательной корреспонденции.

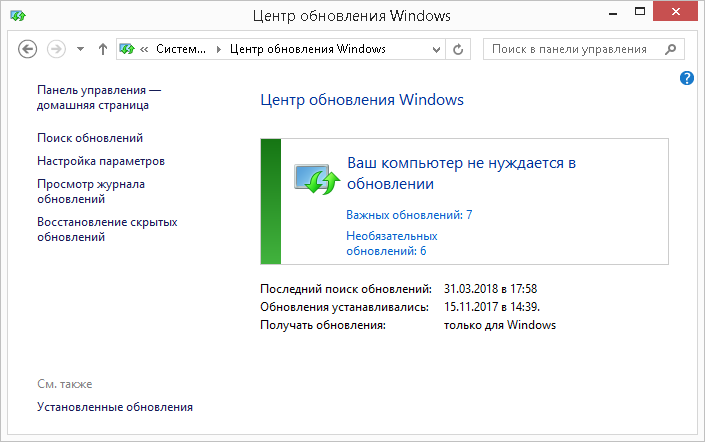
Такими средствами защиты являются:

* + - обновления, устраняющие уязвимости в операционной системе, через которые могут проникать вирусы;
    - брандмауэры – программы, защищающие от атак по сети;
    - средства борьбы со спамом.

***Обновления ПО***

Как известно, вирусы нередко проникают на компьютеры через уязвимости в операционной системе или установленных программах. Причем чаще всего вредоносными программами используются уязвимости операционной системы Microsoft Windows, пакета приложений Microsoft Office, браузера Internet Explorer.

Чтобы не дать вирусам возможности использовать уязвимость, операционную систему и программное обеспечение нужно обновлять. Производители, как правило, раньше вирусописателей узнают о дырах в своих программах и заблаговременно выпускают для них исправления.

Для загрузки и установки обновлений в большинстве программ и систем есть встроенные средства. Например, в операционных системах семейства Microsoft Windows имеется специальный компонента “Центр обновления Windows”**.**

В последнее время вредоносные программы, использующие уязвимости в Windows и прикладных программах, появляются вскоре после выхода исправлений к этим уязвимостям. В некоторых случаях вредоносные программы появляются даже раньше исправлений. Поэтому необходимо своевременно устанавливать исправления, используя для этого средства автоматической установки.

***Брандмауэры***

Для того чтобы удаленно воспользоваться уязвимостью в программном обеспечении или операционной системе, нужно установить соединение и передать специально сформированный пакет данных. От таких попыток проникновения и заражения можно защититься путем запрета определенных соединений. Задачу контроля соединений успешно решают программы-брандмауэры.

Брандмауэр – это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил.

Правило брандмауэра задается несколькими атрибутами:

* + - *приложение* – определяет программу, к которой относится правило, так что одни и те же действия могут быть разрешены одним программам и запрещены другим. Например, получать и отправлять почту разумно разрешить только почтовому клиенту;
    - *протокол* – определяет протокол, используемый для передачи данных. Обычно можно выбрать между двумя протоколами – TCP и UDP;
    - *адреса* – определяет, для соединений с каких адресов или на какие адреса будет действовать правило;
    - *порт* – задает номера портов, на которые распространяется правило;
    - *направление* – позволяет отдельно контролировать входящие и исходящие соединения;
    - *действие* – определяет реакцию на обнаружение соединения, соответствующего остальным параметрам. Реакция может быть следующей: разрешить, запретить или спросить у пользователя.

Необязательно задавать конкретные значения всем атрибутам правила. Можно создать правило, которое будет запрещать входящие соединения на TCP-порт 111 для всех приложений или разрешать любые исходящие соединения для программы Internet Explorer.

Для борьбы с вирусами брандмауэры могут применяться следующим образом.

Во-первых, брандмауэр можно успешно использовать для защиты от вредоносных программ, которые распространяются непосредственно по сети, используя уязвимости в операционной системе.

Второй способ применения брандмауэров для защиты от вредоносных программ состоит в контроле исходящих соединений. Многие троянские программы, да и черви, после выполнения вредоносной функции стремятся подать сигнал автору вируса. Например, троянская программа, ворующая пароли, будет пытаться переслать все найденные пароли на определенный сайт или почтовый адрес. Для того чтобы воспрепятствовать этому, можно настроить брандмауэр на блокирование всех неизвестных соединений: разрешить только соединения от доверенных программ, таких как используемый браузер, почтовый клиент, программа мгновенного обмена сообщений, а все остальные соединения запретить.

Некоторые вредоносные программы пассивно ожидают соединения на каком-то из портов. Если входящие соединения разрешены, то автор вредоносной программы сможет через некоторое время обратиться на этот порт и забрать нужную ему информацию или же передать вредоносной программе новые команды. Чтобы этого не произошло, брандмауэр должен быть настроен на запрет входящих соединений на все порты, кроме фиксированного перечня портов, используемых известными программами или операционной системой.

В последнее время широко распространены универсальные защитные программы, объединяющие возможности брандмауэра и антивируса, например Kaspersky Internet Security, Dr.Web Security Space, ESET NOD32 Internet Security, Norton Internet Security, McAfee Internet Security и прочие.

***Средства защиты от нежелательной корреспонденции***

Для решения проблемы защиты от спама (нежелательной корреспонденции рекламного характера) используются специальные спам-фильтры. Для фильтрации нежелательной почты в спам-фильтрах применяется несколько методов:

* черные и белые списки адресов. Черный список – это список тех адресов, письма с которых фильтр отбраковывает сразу, не применяя других методов. В этот список нужно заносить адреса, если с них постоянно приходят ненужные или, хуже того, зараженные письма. Белый список – это список адресов хорошо известных пользователю людей или организаций, которые передают только полезную информацию. Спам-фильтр можно настроить так, что будут приниматься только письма от адресатов из белого списка;
* базы данных образцов спама. Как и антивирус, спам-фильтр может использовать базу данных образцов нежелательных писем для удаления писем, соответствующих этим образцам;
* анализ служебных заголовков. В письме в относительно скрытой форме хранится служебная информация о том, с какого сервера было доставлено письмо, какой адресат является реальным отправителем и др. Используя эту информацию, спам- фильтр может решать, является письмо спамом или нет. Например, некоторые почтовые серверы, часто используемые для рассылки спама, заносятся в специальные общедоступные черные списки, и, если письмо было доставлено с такого сервера, вполне вероятно, что это спам. Другой вариант проверки – запросить у почтового сервера, действительно ли существует адресат, указанный в письме как отправитель. Если такого адресата не существует, значит, письмо, скорее всего, является нежелательным;
* самообучение. Спам-фильтры можно обучать, указывая вручную, какие письма являются нормальными, а какие нежелательными. Через некоторое время спам-фильтр начинает с большой достоверностью самостоятельно определять нежелательные письма по их похожести на предыдущий спам и непохожести на предыдущие нормальные письма.

Использование спам-фильтров помогает защититься и от некоторых почтовых червей. Самое очевидное применение – это при получении первого зараженного письма (в отсутствие антивируса это можно определить по косвенным признакам) отметить его как нежелательное – и в дальнейшем все другие зараженные письма будут заблокированы фильтром.

Более того, почтовые черви известны тем, что имеют большое количество модификаций, незначительно отличающихся друг от друга. Поэтому спам-фильтр может помочь и в борьбе с новыми модификациями известных вирусов с самого начала эпидемии.