Содержание:

ВВЕДЕНИЕ

Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление "первой ласточки", наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (Win95.CIH), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того.

В литературе весьма настойчиво пропагандируется, что избавиться от вирусов можно лишь при помощи сложных (и дорогостоящих) антивирусных программ, и якобы только под их защитой вы можете чувствовать себя в полной безопасности. Это не совсем так - знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной программы.

Актуальность выбранной темы обусловлена тем, что с каждым днем вирусы становятся все более изощренными, что приводит к существенному изменению профиля угроз. Но и рынок антивирусного программного обеспечения не стоит на месте, предлагая множество, казалось бы, идентичных продуктов. Их пользователи, представляя проблему лишь в общих чертах, нередко упускают важные нюансы и в итоге получают иллюзию защиты вместо самой защиты.

Цель работы - выявить наиболее популярную антивирусную программу у пользователей ПК.

Поставленная цель обусловила решение следующих **задач:**

1. Рассмотреть наиболее распространненые способы защиты информации.
2. Провести анкетирование, выявляющее популярные антивирусные программы.
3. Разработать памятку пользователю «Как уберечься от вирусов».

Объектом данного исследования являются современные антивирусные программы, которые представляют собой многофункциональные продукты, сочетающие в себе как профилактические средства, так и средства лечения вирусов и восстановления данных.

Предметом данного исследования является проблема выбора антивирусной программы.

Гипотеза: большинство пользователей используют антивирусные программы как метод защиты от вирусов, однако предпочитают их бесплатные версии.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ВИРУСОВ

Понятие компьютерный вирус

Компьютерным вирусам уделяется гораздо больше внимания, чем они того заслуживают. С содержательной точки зрения в подавляющем большинстве компьютерных программ, называемых вирусами, нет ничего выдающегося, требующего высокой квалификации или специальных знаний от их создателей. Тем не менее нельзя не признать, что вокруг самого понятия "компьютерный вирус" сложился некий ореол таинства и мистики, который оказывает определенное влияние на вирусный и антивирусный рынки.

Строго определенного понятия "компьютерный вирус" пока не придумано, и имеются определенные сомнения в том, что оно может быть дано. Если не ставить перед собой цель дать именно формальное определение, то можно вполне удовлетворительно объяснить, что представляют собой компьютерные вирусы. Прежде всего следует четко понимать, что компьютерные вирусы являются разновидностью компьютерных программ и ничем более. Программы этой разновидности обладают важным характеристическим свойством: они способны производить свои копии, обладающие способностью к дальнейшему воспроизведению .

То, что именно способность вирусов к самовоспроизведению является их характеристическим свойством, много лет назад проиллюстрировал один из самых известных российских вирусологов Д.Н. Лозинский в своем классическом "Объяснении для домохозяек".[3]

Представим себе организацию, в которой работают пунктуальные, исполнительные чиновники. Каждый такой чиновник каждое утро приходит на работу и обнаруживает на своем рабочем столе стопку листов бумаги с разнообразными поручениями. Чиновники последовательно извлекают листы из стопок и выполняют указания руководства. Допустим, некий злоумышленник (а может быть, просто неумный начальник) положил в стопку одного из чиновников лист, на котором написано следующее: "размножить этот лист в N экземплярах и каждый из них положить в стопку одного из сослуживцев". Легко понять, что через непродолжительное время столы чиновников окажутся заваленными бумагой, а сами чиновники будут только и заниматься тем, что размножать очередные экземпляры глупой инструкции. В этом описании чиновники представляют собой компьютеры, а идиотская инструкция - компьютерный вирус.

Надо отметить, что Д.Н. Лозинский фактически описал механизм, который много лет используется для распространения так называемых "писем счастья" и прочей ерунды. В последнее время по этой же схеме распространяются многочисленные

(практически всегда не имеющие никаких оснований) предупреждения о "страшных вирусах, вчера обнаруженных Microsoft, от которых нет никакого противоядия".

Никакими другими характеристическими свойствами, кроме способности к самовоспроизведению, компьютерные вирусы не обладают. В частности, вопреки распространенному мнению, вирусы вовсе не обязаны быть "злобными" (деструктивными), что-то удалять, форматировать, осыпать буковки на экране, выводить забавные или устрашающие сообщения и вообще как-то обнаруживать свое присутствие.

Понятие "компьютерный вирус" никак не привязано к какой-либо конкретной системе, среде, языку программирования и т.д. Это, разумеется, не означает, что вирус, написанный для одной системы, обязательно будет работоспособен в другой, напротив, как правило, это не так. Мы имеем в виду, что само понятие "компьютерный вирус" не является принадлежностью какой-либо конкретной операционной системы - DOS, Windows, Novell Netware, Linux или другой и основное характеристическое свойство вирусов не зависит от языка, на котором они написаны.

Дать определение троянской программы оказывается еще сложнее, чем определение компьютерного вируса. Да, конечно, можно считать, что троянская программа проникает на компьютер без санкции пользователя. Но на любом компьютере установлены и функционируют множество программ, о которых пользователи и знать не знают.

Наличие сознательно заложенной деструктивной функции можно считать характеристическим свойством троянских программ.

Деструктивные функции, заложенные в троянских программах, бывают различными. Троянские программы могут разрушать или воровать данные, изменять (например, тормозить) работу операционной системы или просто глупо шутить. [4]

Троянские программы часто маскируются под обычное программное обеспечение, а иногда троянские компоненты являются "довеском" к вполне мирным программам. В любом случае защиту от троянцев, наряду с антивирусными программами, может обеспечить элементарная осторожность: не следует брать что попало откуда попало и уж тем более не следует запускать на своем компьютере программы, полученные из ненадежных источников и не прошедшие тщательную проверку.

1.2 Классификация вирусов и вредоносных программ

Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные «настольные» операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.

Если операционная система существует в единичных экземплярах, то вероятность ее злонамеренного использования близка к нулю. Если же производитель системы добился ее массового распространения, то очевидно, что рано или поздно хакеры и вирусо- писатели попытаются использовать ее в своих интересах. Чем популярнее операционная система или приложение, тем чаще она. [1]

Рис. 1 Классификация вирусов по среде обитания и степени воздействия

Безвредные уменьшают свободную область на диске за счет своего размножения.

Неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках.

Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах. Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера.

Очень опасные, воздействие которых может привести к безвозвратной потере программ, уничтожению данных, стиранию информации в системных областях диска.

В настоящее время известны тысячи компьютерных вирусов, которые можно классифицировать по следующим признакам (рис. 2).

Рис. 2 Классификация вирусов

Сетевые вирусы распространяются по различным компьютерным сетям. Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE, и активируются при их запуске. Находятся в оперативной памяти до выключения компьютера.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). При загрузке операционной системы с зараженного диска внедряются в

оперативную память и ведут себя как файловый вирусы.

Макровирусы — являются макрокомандами, которые заражают файлы документов Word, Excel, находятся в оперативной памяти до закрытия приложения.

Драйверные вирусы — заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.

Вирус не может содержаться в ASCII-текстах, графических или звуковых файлах, т. к. он является программой и требует исполнения своего кода.

ГЛАВА 2 АНАЛИЗ ПРОБЛЕМ И МЕТОДОВ ЗАЩИТЫ ОТ ВИРУСОВ

2.1 Защита информации от компьютерных вирусов

Однако не всякая могущая саморазмножаться программа является компьютерным вирусом. С программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к другим программам ("заражать" их). При запуске последних вирус может выполнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), модификацию и уничтожение данных, переполнение машинной памяти, создание помех в работе ЭВМ и т.п. Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий.

После того как вирус выполнит нужные ему действия, он передает управление той зараженной программе, в которой он находится в момент ее запуска, и она работает также как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Вирусы всегда наносят ущерб - они препятствуют нормальной работе ПК, разрушают файловую структуру и т.д., поэтому их относят к разряду так называемых вредоносных программ. Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус *о*стается резидентно в оперативной памяти, вследствие чего до перезагрузки операционной системы он время от времени заражает программы и выполняет вредные действия на компьютере.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Многие резидентные вирусы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают сведения о них в исходном (неискаженном) виде. Разумеется, этот эффект наблюдается только на зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью программ- дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, затрудняет нахождение таких вирусов программами-детекторами.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по локальной сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере.

А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации - страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации необходимы не только для защиты от вирусов. Имеются две основные разновидности этих средств:

- средства резервного копирования информации - создание копий файлов и системных областей дисков;
- средства разграничения доступа - предотвращают несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами, а также ошибочные действия пользователей.

В настоящие время имеется большое количество антивирусных средств. Однако все они не обладают свойствами универсальности: каждое рассчитано на конкретные вирусы, либо перекрывает некоторые каналы заражения ПК или распространения вирусов. В связи с этим перспективной областью исследований можно считать применение методов искусственного интеллекта к проблеме создания антивирусных средств.

Антивирусным средством называют программный продукт, выполняющий одну или несколько из следующих функций:

-
  - защиту файловой структуры от разрушения;
  - обнаружение вирусов;
  - нейтрализацию вирусов.

Антивирусные программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Детектором называется программа, осуществляющая поиск вирусов как на внешних носителях информации, так и в ОЗУ. Результатом работы детектора является список инфицированных файлов и/или областей, возможно, с указанием конкретных вирусов, их заразивших.

Детекторы делятся на универсальные и специализированные. Универсальные детекторы проверяют целостность файлов путем подсчета их контрольной суммы и ее сравнения с эталоном. Эталон либо указывается в документации на программный продукт, либо может быть определен в самом начале его эксплуатации.

Специализированные детекторы настроены на конкретные вирусы, один или несколько. Если детектор способен обнаруживать несколько различных вирусов, то его называют полидетектором. Работа специализированного детектора основывается на поиске строки кода, принадлежащей тому или иному вирусу, возможно заданной регулярным выражением. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение.

Детектор не способен обнаружить все возможные вирусы. Следует особо подчеркнуть, что программы-детекторы могут выявлять только те вирусы, которые им известны. Некоторые программы-детекторы могут настраиваться на новые типы вирусов, для этого им лишь необходимо указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Большинство программ-детекторов имеют функцию "доктора" или фага, т.е. они пытаются вернуть зараженные файлы или области диска в их **исходное состояние.**

Дезинфектором (доктором, фагом) называется программа, осуществляющая удаление вируса как с восстановлением, так и без восстановления среды обитания.

Наиболее известными полидетекторами-фагами являются программные пакеты Antiviral Toolkit Pro Евгения Касперского и DrWeb фирмы "ДиалогНаука". Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам

лечения новых вирусов. К таким программам относится, например, AVSP фирмы "ДиалогНаука".

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков. Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Но некоторые программы-ревизоры, например ADinf фирмы "ДиалогНаука", все же умеют делать и это, не используя вызовы операционной системы для чтения диска (правда, она работают не на всех дисководах). Другие программы часто используют различные полумеры - пытаются обнаружить вирус в оперативной памяти, требуют вызова из первой строки файла AUTOEXEC.BAT, надеясь работать на "чистом" компьютере, и т.д. Увы, против некоторых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы- ревизоры проверяют длину файла. Но одна такая проверка недостаточна - некоторые вирусы не изменяют длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. доктора-ревизоры. Это такие программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Что позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но даже такие программы, как доктора-ревизоры, могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Вирус-фильтром (монитором, сторожем) называется резидентная программа, обеспечивающая контроль выполнения характерных для вирусов действий и требующая от пользователя подтверждения на производство действий. Контроль осуществляется путем подмены обработчиков соответствующих прерываний. В качестве контролируемых действий могут выступать:

- обновление программных файлов;
- прямая запись на диск (по физическому адресу);
- форматирование диска;
- резидентное размещение программы в ОЗУ.

Программы-фильтры располагаются резидентно в оперативной памяти компьютера, перехватывают обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-мониторы не отслеживают подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера. Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Иммунизатором (вакциной) называют программу, предотвращающую заражение среды обитания или памяти конкретными вирусами. Иммунизаторы решают проблему нейтрализации вируса не посредством его уничтожения, а путем блокирования его способности к размножению.

Программы-вакцины или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы малоэффективны, поэтому в настоящее время практически не используются.

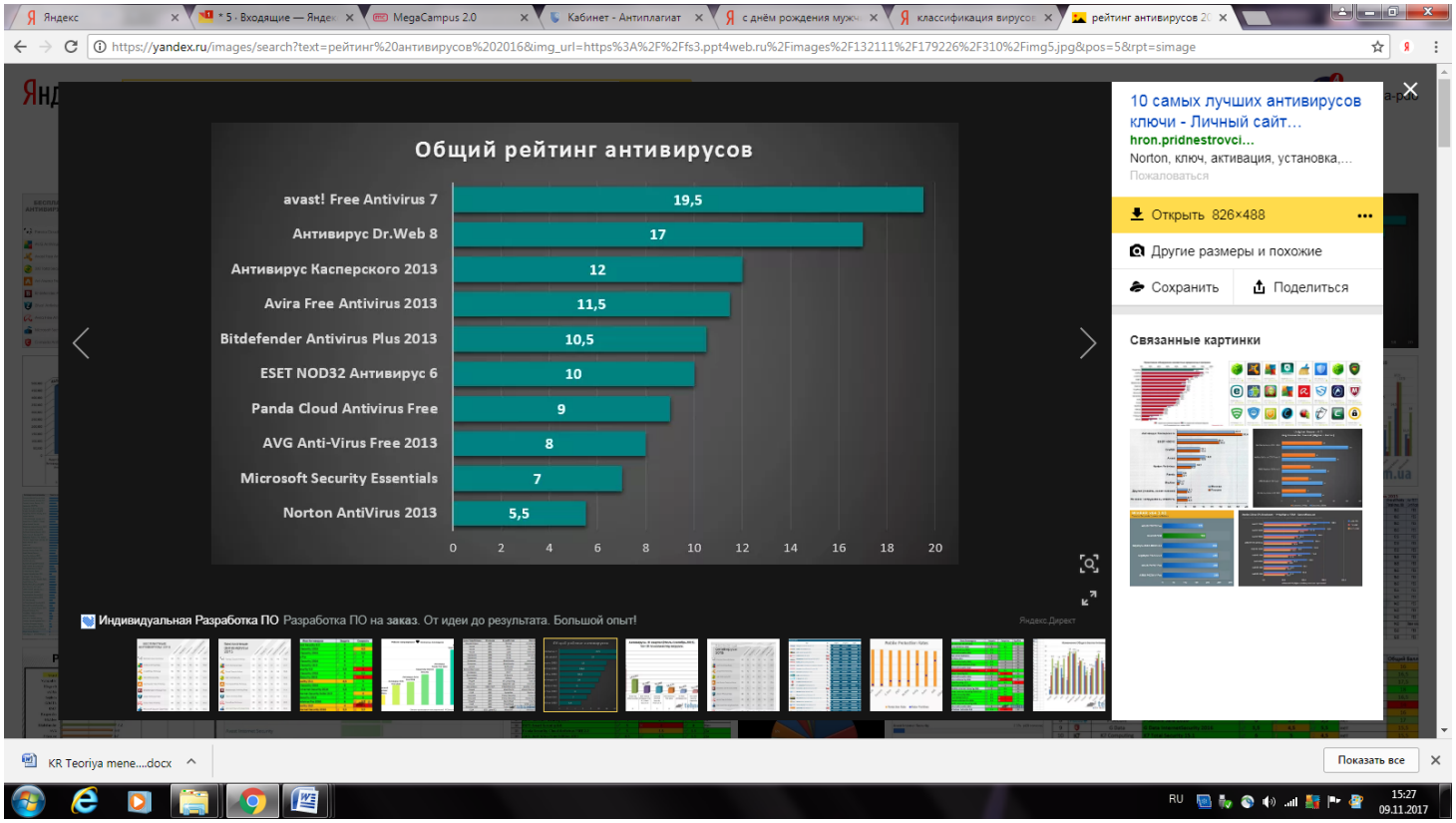
При заражении компьютера вирусом (или при подозрении на это) важно соблюдать четыре правила:

1. Прежде всего не надо торопиться и принимать опрометчивых решений. Непродуманные действия могут привести не только к потере части файлов, но к повторному заражению компьютера.
2. Надо немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.
3. Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС (обязательное правило).
4. Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь более опытных коллег.

Защита от компьютерных вирусов должна стать частью комплекса мер по защите информации как в отдельных компьютерах, так и автоматизированных информационных системах в целом.

2.2 Антивирусные программы

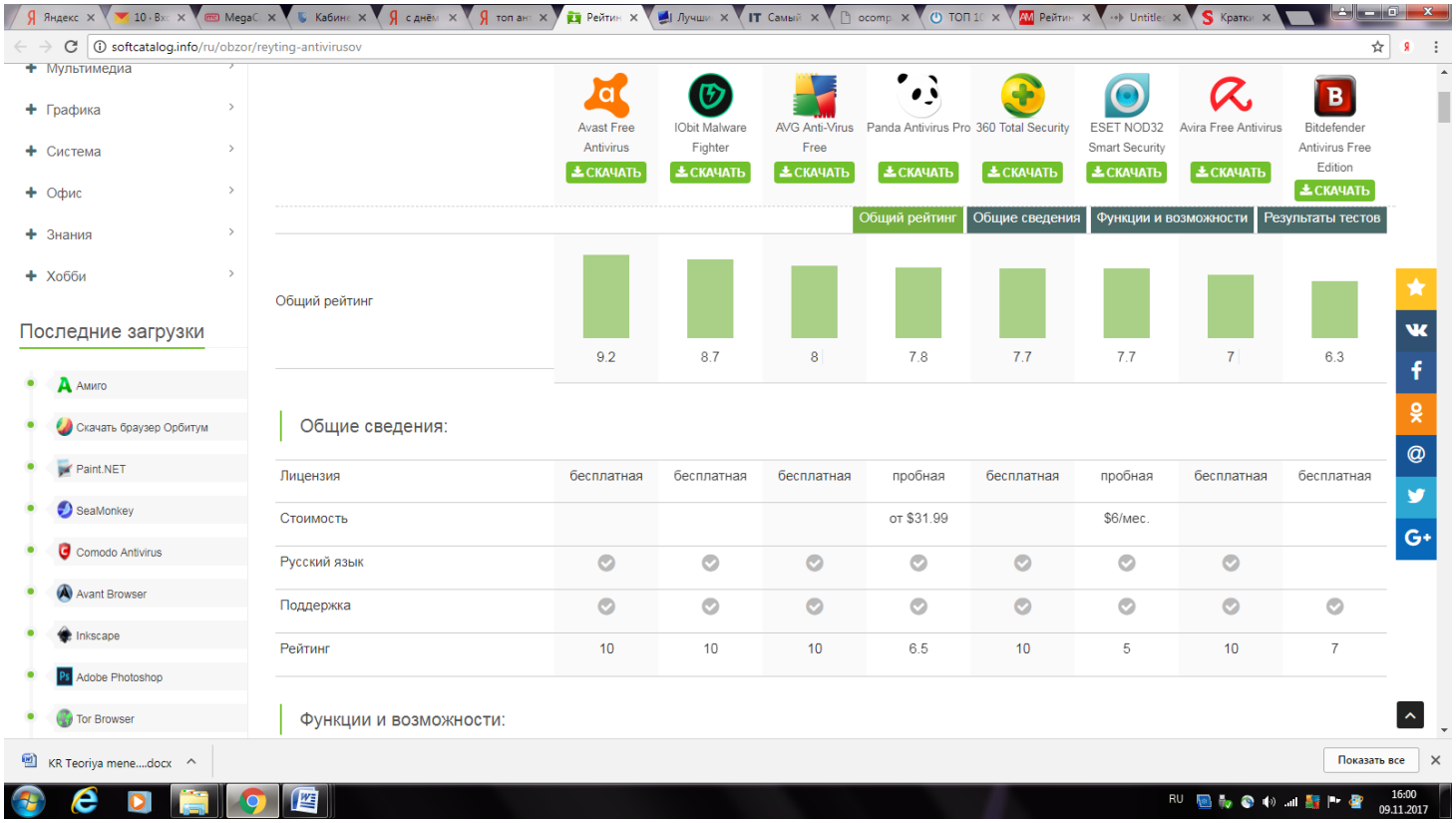
Антивирусная защита – это один из наиболее необходимых элементов в компьютере, так как он защищает ваши данные и операционную систему от различных вредоносных программ, которых в интернете огромное количество. Если на компьютере хранится важная информация, то к выбору антивируса стоит отнестись с особой ответственностью.



Рейтинг антивирусов 2017 - Выбираем лучший антивирус

На сегодняшний день выбор надежного антивируса - дело первоочередной важности для любого пользователя, ведь что может защитить компьютер лучше, чем полноценное комплексное решение, направленное на сохранность данных и стабильную работу? Эта статья посвящена лучшим антивирусным программам, которые дадут пользователю все необходимые инструменты для защиты от троянов и вирусов, предотвратят заражение компьютера, заблокируют вредоносный сайт и будут не сильно загружать систему.

Мы уже провели общий анализ самых популярных антивирусов 2017 года, выяснив все их плюсы и минусы. Результаты этой проверки вы можете посмотреть в сравнительной таблице. Ну а чтобы понять, кто из них - самый лучший бесплатный антивирус, давайте рассмотрим их более детально. Итак, приступим!



Avast Free Antivirus Скачать Avast Free Antivirus

Avast Free Antivirus - отличный бесплатный антивирус, который заслужил признание миллионов пользователей по всему миру благодаря надежной защите от троянов и вирусов в реальном времени. Последняя версия Avast может похвастаться обновленным интуитивно понятным интерфейсом, несколькими уникальными функциями (AutoSandbox, Intelligent Scanner и т.д.), улучшенным быстродействием и, главное, одной из самых широких баз вирусов в мире (она ежедневно пополняется).

Ключевые особенности Avast Free Antivirus:

- Огромная, постоянно обновляемая база сигнатур;
- Отличная защита от руткитов в реальном времени;
- Сетевой экран, защищающий компьютер во время интернет-сёрфинга;
- Современный движок, обеспечивающий завидное быстродействие программы;
- Автоматический и игровой режимы работы;

- Удобный виджет на рабочий стол;
- Интуитивный, приятный глазу интерфейс;
- Бесплатная версия дает полный функционал!

Avast Free Antivirus представляет пользователю новую функцию AutoSandbox, которая позволяет автоматизировать процесс помещения подозрительных файлов в "песочницу", где можно будет провести полный анализ файла и, при необходимости, вылечить его. Эта функция позволяет спасти от мгновенного стирания достаточно большой процент файлов, избежать системных ошибок, связанных с удалением важных системных файлов и тп. Приложение обращается с объектами аккуратнее аналогов!

Также новая версия Аваста включает в себя встроенную функцию удаленной поддержки. Пользователь может подключиться к компьютеру другого пользователя (только с разрешения) и оказать ему техническую поддержку или помощь, что довольно удобно, так как избавляет о необходимости иметь на компьютере настроенную программу для удаленного доступа. В целом, Avast Free Antivirus является отличным выбором для среднестатистического пользователя, предоставляя ему все необходимое для содержания системы в чистоте.

IObit Malware Fighter Скачать IObit Malware Fighter

IObit Malware Fighter не является классическим продуктом, как, например, «Антивирус Касперского», но гарантируют большую степень защиты, чем dr.web cureit и другие сканнеры, рассчитанные на обычную проверку ПК на вирусы. Также он может быть установлен в комплекте с программным обеспечением Advanced SystemCare – набором утилит, которые очищают систему, повышают производительность компьютера, восстанавливают случайно удаленную информацию и т.д. Найдется средство для решения чуть ли не любой проблемы. Ключевые особенности IObit Malware Fighter:

- Потребляет мало аппаратных ресурсов, имеет понятный интерфейс;
- Включает сигнатуры обнаружения троянских программ от Bitdefender;

- Содержит сразу несколько модулей для защиты пользователя во время работы в Сети;
- Анти-вымогатель помогает сохранить конфиденциальные данные и документы в недоступности для вредоносов;
- Позволяет применять действия к инфицированным объектам в ручном и автоматическом режиме;
- Предлагает также установить неплохой набор компонентов для очистки и настройки ОС Windows;
- В сравнении с платными аналогами, в базовой комплектации, имеет довольно неплохой уровень, достаточный для бытового использования.

Приложение попало к нам в обзор, поскольку отлично работает на слабых компьютерах, не требует платы за использования, однако, предоставляет должный уровень защиты подключения к интернету. Другие похожие продукты действуют иначе: делают упор на сканирование диска, забывая о возможности заражения из-за потенциально опасных сайтов и различных шпионских модулей. В качестве домашнего антивирусника, Malware Fighter справится с задачей, но для защиты массивов архи-важных данных лучше использовать серьезные продукты от западных разработчиков.

AVG Anti-Virus Free Скачать AVG Anti-Virus Free

AVG Anti-Virus Free - популярный антивирус основной характерной чертой которого является глубокая интеграция в систему и которомы можно абсолютно бесплатно пользоваться. Программа автоматически сканирует файлы и программы при их запуске, что позволяет избежать заражения вирусами, троянами и шпионскими программами. Также программа предоставляет пользователю сканер, настраиваемый по расписанию. Благодаря этой функции вы сами сможете контролировать как процесс проверки компьютера на зараженные файлы, так и процесс их лечения. В новой версии AVG полностью обновлен интерфейс, который теперь может похвастать приятным внешним видом и удобными меню.

Ключевые особенности AVG Anti-Virus Free:

- Быстрое и качественное сканирование системы;
- Автоматическое сканирование файла при его первом запуске;
- Сканер по требованию/по расписанию;
- Постоянные обновления;
- Полезные модули защиты (Link Scanner, e-Mail Scanner);
- Интуитивный интерфейс;

AVG Anti-Virus Free может похвастаться отличными показателями защиты системы и довольно малым потреблением системных ресурсов. В отличие от платной версии, которая, конечно, содержит в себе больше инструментов и функций, версия для бесплатного использования работает гораздо стабильнее, получая при этом ту же самую техническую поддержку в виде обновлений. Скорость работы программы поражает, а сканер электронной почты избавит вас от необходимости устанавливать специализированные приложения, так как справляется он на все 100%. Новая уникальная функция - Link Scanner позволяет пользователю использовать антивирус чтобы просканировать сайт не заходя на него, что может быть очень удобно. Именно AVG Anti-Virus Free является выбором "по-умолчанию" для более чем 5 миллионов пользователей по всему миру, а нам остается лишь подметить, что это вполне заслуженно.

Panda Antivirus Pro Скачать Panda Antivirus Pro

Panda Antivirus Pro служит одной единственной цели - она защищает компьютер пользователя от наиболее известных видов виртуальных угроз. И можно с уверенностью сказать, что справляется она с этим замечательно. Установив Панду пользователь получает в свое распоряжение крайне простой, но достаточно эффективный щит от любой виртуальной угрозы. Достаточно большая база вирусов Панды постоянно пополняется как разработчиками, так и пользователям, которым "везет" находить новые разновидности вирусов. Ну а в элементарном интерфейсе этого бесплатного антивируса разберется даже ребенок!

Ключевые особенности Panda Antivirus Pro:

- Автоматически обнаруживает вредоносное программное обеспечение;

- Блокирует вредоносные сайты;
- Обновляет базу вирусов практически каждый день;
- Специальные режимы работы для игр и воспроизведения мультимедиа;
- Антируткит фаерволл;
- Автоматически сканирует подключаемые USB устройства;
- Интуитивно-понятный интерфейс;
- Бесплатная версия антивируса!

Panda Antivirus Pro отличный выбор для пользователей, которые хотят получить качественную защиту от вирусов при минимуме усилий. Большинство функций Панды автоматизированы, программа постоянно сканирует оперативную память и жесткий диск на наличие угроз и подозрительных файлов. Новый движок приложения позволяет снизить потребление программой системных ресурсов до минимума. Антивирусный загрузочный диск Panda Cloud Cleaner дает возможность вылечить зараженную систему, которая не может сама загрузиться. Может немного напрягать количество ложных срабатываний, но ведь это не так и плохо - программа заботится о Вас! В общем, если Вам нужен отличный антивирус, который превосходно справляется с поддержкой системы в хорошем состоянии даже без участия пользователя в этом процессе, Panda Antivirus Pro - лучший выбор!

360 Total Security Скачать 360 Total Security

360 Total Security - мощный набор инструментов для поддержания операционной системы в порядке, который включает в себя современный антивирус, твикер для оптимизации и инструмент для очистки системы от мусора. Это бесплатное антивирусное решение, которое способно не только качественно защитить компьютер от внешних угроз, но также и оптимизировать его работу, помочь правильно распределить системные ресурсы, чтобы увеличить скорость процессов. Само приложение базируется на пяти активных движках, четыре из которых отвечают за защиту систему, поэтому можете быть уверены, качество 360 Total Security полностью соответствует его названию!

Ключевые особенности 360 Total Security:

- Отличная защита от вирусов как в реальном времени, так и при сканированиях;
- Использование нескольких отдельных модулей для защиты;
- Автоматическая проверка подключаемых носителей информации;
- Удобная интеграция в браузеры;
- Очистка системы от мусорных и временных файлов;
- Превосходная оптимизация системы;
- Абсолютно бесплатная версия!

360 Total Security является отличным выбором как для начинающих пользователей ПК, так и для продвинутых. Первые получают в свое распоряжение надежную систему с множеством автоматизированных функций, что позволит защищать компьютер без прямого участия пользователя. Вторые же по достоинству оценят гибкие настройки приложения, возможность менять профили, сохраняя в них разные настройки, функции по оптимизации работы системы и многие другие интересные опции. Оформление приложения не вызывает никаких вопросов и позволяет использовать все ее аспекты без лишних вопросов и помощи справки. Защитите свой компьютер вместе с 360 Total Security!

ESET NOD32 Smart Security Скачать ESET NOD32 Smart Security

ESET NOD32 Smart Security - замечательное комплексное решение для защиты вашего компьютера от различного рода виртуальных угроз. Вирусы, трояны, руткиты, рекламное ПО, спам - все это легко забывается после установки этого замечательного антивируса. "Лучшая защита - это нападение", - вероятно считают программисты ESET, так как по умолчанию на Нод32 выставлены довольно агрессивные настройки по сканированию и уничтожению угрозы. Но пока это дает такие результаты - а почему бы и нет?

Ключевые особенности ESET NOD32 Smart Security:

- Тотальная многоуровневая защита от вирусов, malware и adware приложений;
- Персональный файервол;
- Защита от ботнетов и улучшенный блокировщик эксплойтов;

- Функция Anti-Theft, которая позволяет найти и вернуть утерянный ноутбук;
- Smart Mode, автоматизирующий процессы сканирования и выявления подозрительных файлов;
- Возможность создания загрузочного диска для поврежденной системы;
- Минимальный процент ложных срабатываний;
- Симпатичный минималистичный интерфейс;
- 30 дней полной рабочей версии!

ESET NOD32 Smart Security имеет в своем арсенале всё необходимое для защиты вашего ПК: несколько ступеней защиты от любого типа нежелательного ПО или вируса, персональный кастомизируемый фаервол для шифровки соединения, родительский контроль, контроль и скан подключаемых устройств, бесплатная круглосуточная техподдержка и тд. Если ам необходим антивирус для установки на ноутбук, НОД32 будет практически идеальным решением, так как он имеет специальные профили для работы на портативных ПК, которые позволяют снизить расход энергии. Но за все приходится платить, и у ESET NOD 32 помимо огромного набора качественных инструментов также довольно высокое потребление системных ресурсов, что частично компенсируется профилями, где можно настроить каждый аспект. К слову, на официальном сайте антивируса есть много полезной информации по оптимизации работы приложения. Но в целом, ESET NOD32 Smart Security по праву является одной из самых популярных и надежных антивирусных программ на современном рынке.

Avira Free Antivirus Скачать Avira Free Antivirus

Avira Free Antivirus - простой антивирус, который может похвастаться довольно эффективной защитой от вирусов, троянов и рекламного ПО. Основным его преимуществом над конкурентами является уход в облачную технологию, которая позволяет защищать компьютер от самых новых, появившихся совсем недавно, угроз. Сам антивирус предоставляет лишь базовую защиту от угроз, но может быть расширен специальными модулями-плагинами, которые можно скачать абсолютно бесплатно с сайта производителя. Таким образом каждый пользователь может "построить" персональную и уникальную систему защиты.

Ключевые особенности Avira Free Antivirus:

- Постоянно пополняемая антивирусная база;
- Использование облачных технологий для экономии системных ресурсов;
- Умеет бороться с макровирусами и лечить зараженные им файлы;
- Возможность настраивания сканирования по расписанию;
- Автоматическое сканирование исполняемых файлов;
- Возможность подгружать модули, чтобы расширить функционал;
- Не конфликтует с другими антивирусными приложениями;
- Абсолютно бесплатный дистрибутив!

Avira Free Antivirus идет в комплекте с модулем Virus Guard, который автоматически сканирует файлы, которые открывает пользователь, что повышает уровень безопасности системы. В целом, Авира - одно из лучших решений для борьбы с так называемыми "полиморфными" вирусами, которые могут подражать обычным программам. Также Вы можете установить модуль сканирования электронной почты, защиту от спама и от программ с автодозвоном. Иными словами, Авира - хороший антивирус, который готов долго и надежно защищать ваш компьютер, что бы вы ни делали. Скачайте Avira Free Antivirus бесплатно и убедитесь в этом!

Bitdefender Antivirus Free Edition Скачать Bitdefender Antivirus Free Edition

Bitdefender Antivirus Free Edition - бесплатная версия популярного антивируса Bitdefender, которая, хоть слегка и подрастеряла инструментал, все еще может конкурировать с лидерами рынка антивирусных приложений, так как с легкостью отлавливает все существующие вирусы. В бесплатную версию вошел современный сканер с календарным модулем, дающим возможность планировать проверки системы наперед, карантинный модуль для наблюдения за подозрительными файлами, журнал отчетов о проверке и огромная база вирусов, которая содержит на сегодняшний день около 500 000 сигнатур. Бытует мнение, что бесплатная версия никогда не предоставит того же качества, которое есть в платных антивирусных программах, и Битдефендер с легкостью рушит все подобные стереотипы.

Ключевые особенности Bitdefender Antivirus Free Edition:

- Надежная защита от вирусов и троянов;

- Простой в использовании;
- Удобная блокировка вредоносных сайтов;
- Использует рекордно мало системных ресурсов;
- Не тормозит систему;
- Запускается на Windows XP, Windows 7, Windows 8 и Vista.

Bitdefender Antivirus Free Edition идеально подходит для домашнего использования, так как не нагружает систему лишними процессами, обеспечивая при этом высокий уровень защиты. В отличие от многих других антивирусов, Битдефендер не напрягает постоянно выскакивающими окнами и не требует участия пользователя в своей работе. Огромная база вирусов обеспечивает высочайший уровень защиты, а интуитивный интерфейс позволяет использовать его даже пользователям, которые никогда прежде не сталкивались с антивирусными программами. Попробуйте этот замечательный антивирус в действии и убедитесь, что это один из лучших представителей на рынке!

Comodo Antivirus Скачать Comodo Antivirus

Comodo Antivirus - мощный бесплатный антивирус для комплексной защиты компьютера от вирусов, троянов, хакерских атак и другого вредоносного ПО. Благодаря расширенному эвристическому анализу файлов, Комодо превосходно справляется с выявлением зараженных файлов, позволяя вылечить их быстрее, чем они нанесут вред системе. Установить антивирус еще проще, чем им пользоваться - по ходу установки Вам будет предложено выбрать множество настроек, чтобы облегчить работу с программой после установки.

Ключевые особенности Comodo Antivirus:

- Большая база вирусов;
- Встроенный календарь для автоматизации сканирования;
- Лучшие показатели эвристического анализа среди конкурентов;
- Удобная изоляция подозрительных файлов в карантин;
- Быстрая и качественная техподдержка;
- Практически идеальная проактивная защита;
- Симпатичный дизайн приложения.

Comodo Antivirus отлично подойдет как новичкам, так и продвинутым пользователям, так как удачно сочетает в себе богатый инструментал, удобные настройки по автоматизации процессов и имеет приятный интерфейс. Новейший движок Comodo позволяет практически не загружать системы во время работы, а также сокращает стандартно длинное время ожидания во время, к примеру, процесса сканирования компьютера на угрозы. В итоге мы имеем прекрасный кастомизированный антивирус, который будет верно служить многие годы.

Dr.Web Antivirus Скачать Dr.Web Antivirus

Dr.Web Antivirus - бесплатное антивирусное решение для обнаружения и уничтожения вирусов и другого вредоносного ПО. Благодаря эффективному эвристическому анализатору, Доктор Вэб легко обнаруживает новые неизветные виды виртуальных угроз даже в социальных сетях, а проактивная многоступенчатая защита ограждает систему от любой опасности во время интернет сёрфинга или использования непроверенных носителей информации. Составлением база занимаются независимые лаборатории что повышает качество базы вирусов.

Ключевые особенности Dr.Web Antivirus:

- Многоступенчатая система защиты;
- Модули для сканирования USB-носителей, электронной почты и тд;
- Защита пользовательских данных от повреждения;
- Высокая скорость противовирусного сканирования;
- Персональный сетевой экран для защиты от хакеров;
- Не замедляет работу компьютера;
- Максимально упрощенный интерфейс с симпатичным дизайном;
- Бесплатная пробная версия!

Dr.Web Antivirus способен удовлетворить запросы даже самого придирчивого пользователя: высокое быстродействие приложения позволяет ему сканировать компьютер за считанные минуты, активный сетевой фильтр заставляет забыть о любой опасности на просторах Сети, а удобный и интуитивно-понятный интерфейс изобилирует удобными меню, кнопками быстрого доступа и легко кастомизируется.

В целом, антивирус Доктор Веб имеет все шансы стать Вашим незаменимым помощником в деле содержания Вашего Пк в порядке.

Стоит отметить, что существует еще много других антивирусных программ, но, к сожалению, формат курсовой работы не позволяет охватить их все, поэтому такие интересные антивирусы, как Kaspersky Internet Security, Norton Internet Security, Dr. Web CureIt, Trend Micro, Microsoft Security Essentials, G Data и многие другие не попали в рассмотрение этой работы. Что до представленных в списке антивирусов - каждый из них способен поймать вредоносную программу, обнаружить рекламное ПО, и вылечить зараженный файл, поэтому какой из них выбрать - судить уже Вам.

2.3 Проблемы борьбы с вирусами

В настоящее время компьютер прочно вошел в повседневную жизнь. Его возможности используются на работе, при проведении досуга, в быту и других сферах жизни человека. В связи с этим, особенно обострилась проблема защиты информации.

Сегодня невозможно встретить пользователя персонального компьютера, который не слышал бы о компьютерных вирусах. В Интернете такие вредоносные программы существуют в огромном количестве.

Вирус - это вредоносная программа, проникающая на компьютер без ведома пользователя (хотя, возможно, при невольном его участии) и выполняющая определенные действия деструктивной направленности. Эти программы подобно биологическим вирусам размножаются, записываясь в системные области диска или приписываясь к файлам производят различные нежелательные действия, которые, зачастую, имеют катастрофические последствия.

Известные вирусы можно разделить на следующие группы: файловые вирусы, сетевые вирусы («черви»), загрузочные вирусы, макровирусы, троянские кони. Сегодня самой распространенной группой вирусов стали макровирусы, заражающие не программы, а документы, созданные в Microsoft Word и Microsoft Excel.

Основными путями проникновения вирусов в компьютер являются съемные диски, носители, а также компьютерные сети.

Сегодня на отечественном рынке представлено достаточное количество различных антивирусных программ. Некоторые из антивирусных программ распространяются бесплатно, другие на платной основе. Следует отметить, что эффективность платных антивирусных программ существенно выше, чем бесплатных, поэтому для надежной защиты компьютера (особенно при частом использовании Интернета, а также при работе в локальной сети) рекомендуется установить платную антивирусную программу.

Самыми популярными антивирусными программами среди пользователей, являются «Kaspersky» (17%), «Avast» (14%), Dr.Web (11%) и «Avira» (10%). Значительно реже пользуются AVG (7%), Microsoft Security Essentials (5%) и «Nod 32» (2%). Большинство пользователей предпочитают бесплатный способ защиты информации (57%), и лишь 43% респондентов готовы платить за информационную безопасность.

Подводя итоги исследования, можно сделать вывод, что соблюдение элементарных правил безопасности при работе в Интернете убережет пользователей от возможности заражения (не следует открывать письма от неизвестных адресатов с непонятными вложениями, переходить по присланным неизвестными интригующим ссылкам, т.п.). Необходимо сразу же проверять принесенную кем-то флешку или иной носитель информации, а уже затем открывать ее и работать с ее содержимым.

Если компьютер в локальной сети, то предпочтительно не давать без острой необходимости в общий доступ папки с полными правами на них. Туда очень легко могут проникнуть вирусы.

Каким бы хорошим и надежным не был антивирус, вероятность того, что он пропустит вирус, есть всегда.

В заключении хотелось бы дать несколько советов по обеспечению безопасности компьютера:

- установка лицензионного антивирусного программного обеспечения (платного или бесплатного) от надежного и авторитетного производителя;
- регулярное обновление антивирусных баз;
- проведение хотя бы раз в месяц полную проверку вашего компьютера антивирусом с актуальными базами.

Этих элементарных мер вполне хватит для того, чтобы знакомство с компьютерными вирусами было максимально коротким и безболезненным для компьютера.

ЗАКЛЮЧЕНИЕ

На сегодняшний день очень популярными являются вирусы, которые называют червями.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код. Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения, например, содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы. Троянские программы осуществляют различные не санкционированные пользователем действия, например, сбор информации и передачу ее злоумышленнику, разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Сведения о самых распространенных угрозах и потенциально нежелательных программах можно всегда найти на портале Центра Microsoft по защите от нежелательных программ (http://www. microsoft.com/rus/protect/products/computer/malwareprotectioncenter .mspx). А также специалисты «Лаборатории Касперского» постоянно информируют о новых угрозах, новых появившихся вирусах (http://www.securelist.com/ru/descriptions).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Безруков Н.Н. "Классификация компьютерных вирусов MS-DOS и методы защиты от них", Москва, СП "ICE", 2010 г.
2. Безруков Н.Н. "Компьютерные вирусы", Москва, Наука, 2010.

3. Денисов Т.В. "Антивирусная защита"//Мой Компьютер-№4-2009г.
4. Ершов Ф. И. Антивирусные препараты; ГЭОТАР-Медиа - Москва, 2006. - 312 с.
5. Компьютерные вирусы (Russian Edition); Подвиг - Москва, 2011. - 132 с.
6. Касперский, Е. Компьютерные вирусы в MS-DOS; М.: Русская редакция - Москва, 2011. - 176 с.
7. Леонтьев, В.П. Как защитить компьютер (вирусы, хакеры, реклама) / В.П. Леонтьев. - М.: Олма-пресс, 2015**. -** 538 с.
8. Никулин, Е.А. Компьютерная геометрия и алгоритмы машинной графики / Е.А. Никулин. - М.: СПб: BHV, 2016. - 576 с.
9. Мостовой Д.Ю. "Современные технологии борьбы с вирусами" // Мир ПК. - №8. - 2008.
10. Петров, М.Н. Компьютерная графика. Учебник (+ CD-ROM) / М.Н. Петров, В.П. Молочков. - М.: СПб: Питер, 2017. - 812 с.
11. Тимофеев, А.В. Информатика и компьютерный интеллект / А.В. Тимофеев. - М.: Педагогика, 2017. - 128 с.
12. Ф.Файтс, П.Джонстон, М.Кратц "Компьютерный вирус: проблемы и прогноз", Москва, "Мир", 2008 г.
13. http://www.symantec.ru/region/ru/product/navbrochure/index.htm
14. http://www.symantec.ru
15. http://www.dials.ru/
16. http://www.avp.ru/
17. http://www.dialognauka.ru/
18. http://www.apl.ru/isvwsolaris.htm