1) Как и всегда, начнём с определения. «Компьютерный вирус — разновидность компьютерной программы, способной создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам». В отличие от червей (сетевых червей), вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере:
    - при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
    - вирус скопировал себя на съёмный носитель или заразил файлы на нем;
    - пользователь отослал электронное письмо с зараженным вложением.

   Разнообразие компьютерных вирусов выявило признаки, по которым они классифицируются. Какие же?

2) **По способу заражения вирусы бывают резидентные и нерезидентные.**

   Резидентные вирусы, получив управление, так или иначе остается в памяти и производят поиск жертв непрерывно, до завершения работы среды, в которой он выполняется. С переходом на Windows проблема остаться в памяти перестала быть актуальной: практически все вирусы, исполняемые в среде Windows, равно как и в среде приложений Microsoft Office, являются резидентными вирусами. Соответственно, атрибут резидентный применим только к файловым DOS вирусам. Существование нерезидентных Windows вирусов возможно, но на практике они являются редким исключением.

   Получив управление, нерезидентный вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту). К такому типу вирусов можно отнести скрипт-вирусы.

   **По степени воздействия вирусы подразделяются на безвредные, вредные и опасные.**

   Безвредные вирусы никак не влияют на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).

   Неопасные вирусы не мешают работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

   Опасные вирусы могут привести к различным нарушениям в работе компьютера, к потере программ, уничтожению данных, стиранию информации в системных областях диска.

   **Классификация вирусов по способу маскировки разбивает их на шифрованные, шифровальщики и полиморфные.**

   Обычно при создании копий для маскировки могут применяться следующие технологии:

   Шифрование — вирус состоит из двух функциональных кусков: собственно, вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

Метаморфизм — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

Шифрованный вирус использует простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора.

Полиморфный вирус использует метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

Вирус-шифровальщик в большинстве случаев приходит по электронной почте в виде вложения от незнакомого пользователю человека, а возможно, и от имени известного банка или действующей крупной организации. Письма приходят с заголовком вида: «Акт сверки…», «Ваша задолженность перед банком…», «Проверка регистрационных данных», «Резюме», «Блокировка расчетного счета» и прочее. В письме содержится вложение с документами, якобы подтверждающими факт, указанный в заголовке или теле письма. При открытии этого вложения происходит моментальный запуск вируса-шифровальщика, который незаметно и мгновенно зашифрует все документы. Пользователь обнаружит заражение, увидев, что все файлы, имевшие до этого знакомые значки, станут отображаться иконками неизвестного типа. За расшифровку преступником будут затребованы деньги. Но, зачастую, даже заплатив злоумышленнику, шансы восстановить данные ничтожно малы.

Вложения вредоносных писем чаще всего бывают в архивах .zip, .rar, .7z. И если в настройках системы компьютера отключена функция отображения расширения файлов, то пользователь (получатель письма) увидит лишь файлы вида «Документ.doc», «Акт.xls» и тому подобные. Другими словами, файлы будут казаться совершенно безобидными. Но если включить отображение расширения файлов, то сразу станет видно, что это не документы, а исполняемые программы или скрипты, имена файлов приобретут иной вид, например, «Документ.doc.exe» или «Акт.xls.js». При открытии таких файлов происходит не открытие документа, а запуск вируса-шифровальщика. Вот лишь краткий список самых популярных «опасных» расширений файлов: .exe, .com, .js, .wbs, .hta, .bat, .cmd. Поэтому, если пользователю не известно, что ему прислали во вложении, или отправитель не знаком, то, вероятнее всего, в письме – вирус-шифровальщик.

На практике встречаются случаи получения по электронной почте обычного `вордовского` (с расширением .doc) файла, внутри которого, помимо текста, есть изображение, гиперссылка (на неизвестный сайт в Интернете) или встроенный OLE-объект. При нажатии на такой объект происходит незамедлительное заражение.

Вирусы-шифровальщики стали набирать большую популярность начиная с 2013 года. В июне 2013 известная компания McAfee обнародовала данные, показывающие что они собрали 250 000 уникальных примеров вирусов шифровальщиков в первом квартале 2013 года, что более чем вдвое превосходит количество обнаруженных вирусов в первом квартале 2012 года.

В 2016 году данные вирусы вышли на новый уровень, изменив принцип работы. В апреле 2016 г. в сети появилась информация о новом виде вируса-шифровальщика Петя (Petya), который вместо шифрования отдельных файлов, шифрует таблицу MFT файловой

системы, что приводит к тому что операционная система не может обнаружить файлы на диске и весь диск по факту оказывается зашифрован.

**В классификации вирусов по среде обитания под «средой обитания» понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса. По среде обитания вирусы можно разделить на загрузочные, файловые, макровирусы и скрипт-вирусы.**

В эпоху вирусов для DOS часто встречались гибридные файлово-загрузочные вирусы. После массового перехода на операционные системы семейства Windows практически исчезли как сами загрузочные вирусы, так и упомянутые гибриды. Отдельно стоит отметить тот факт, что вирусы, рассчитанные для работы в среде определенной ОС или приложения, оказываются неработоспособными в среде других ОС и приложений. Поэтому как отдельный атрибут вируса выделяется среда, в которой он способен выполняться. Для файловых вирусов это DOS, Windows, Linux, MacOS, OS/2. Для макровирусов — Word, Excel, PowerPoint, Office. Иногда вирусу требуется для корректной работы какая-то определенная версия ОС или приложения, тогда атрибут указывается более узко: Win9x, Excel97.

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они:

- различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);
- создают файлы-двойники (компаньон-вирусы);
- создают свои копии в различных каталогах;
- используют особенности организации файловой системы (link-вирусы).

Все, что подключено к Интернету – нуждается в антивирусной защите: 82% обнаруженных вирусов «прятались» в файлах с расширением PHP, HTML и EXE.

Число вредоносных программ неуклонно растет и уже в скором будущем может достичь масштабов эпидемии. Распространение вирусов в цифровом мире не имеет границ, и даже при всех имеющихся возможностях нейтрализовать деятельность преступного киберсообщества сегодня уже невозможно. Бороться с хакерами и вирусописателями, которые неустанно совершенствуют свое мастерство, становится все сложнее. Так, злоумышленники научились успешно скрывать цифровые каналы распространения угроз, что значительно затрудняет отслеживание и анализ их онлайн-движения. Меняются и пути распространения, если раньше киберпреступники предпочитали электронную почту для распространения вирусов, то сегодня лидерские позиции занимают атаки в режиме реального времени. Также наблюдается рост вредоносных веб-приложений, которые оказались более чем пригодны для атак злоумышленников. Как заявил Говинд Раммурти, генеральный и управляющий директор компании eScan MicroWorld, сегодня хакеры научились успешно уклоняться от детектирования традиционными антивирусными сигнатурами, которые по ряду причин обречены на неудачу, когда дело доходит до обнаружения веб-угроз. Судя по образцам, исследованным в eScan, веб-угрозы превалируют среди вредоносных программ. 82% выявленных вредоносных программ - файлы с расширением PHP, HTML и EXE, а MP3, CSS и PNG - менее чем 1%.

Это явно говорит о том, что выбор хакеров – это Интернет, а не атаки с использованием уязвимостей программного обеспечения. Угрозы имеют полиморфный характер, это означает, что вредоносные программы могут быть эффективно перекодированы удаленно, что делает их трудно обнаружимыми. Поэтому высокая вероятность заражения связана, в том числе, и с посещениями сайтов. Согласно данным eScan MicroWorld, количество

перенаправляющих ссылок и скрытых загрузок (drive-by-download) на взломанных ресурсах увеличилось более чем на 20% за последние два месяца. Социальные сети также серьезно расширяют возможности доставки угроз.

Возьмем, к примеру, циркулировавший в Facebook баннер, предлагавший пользователю изменить цвет страницы на красный, синий, желтый и т.д. Заманчивый баннер содержал ссылку, направлявшую пользователя на мошеннический сайт. Там в руки злоумышленникам попадала конфиденциальная информация, которая использовалась или продавалась для получения незаконной прибыли различным интернет-организациям. Таким образом, антивирусы, основанные на традиционных сигнатурах, сегодня малоэффективны, так как они не могут надежно защитить от веб-угроз в режиме реального времени. Антивирус, который основан на облачных технологиях и получает информацию об угрозах из «облака», эти задачи под силу.

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией. Теоретически возможно появление загрузочных вирусов, заражающих CD-диски и USB-флешек, но на текущий момент такие вирусы не обнаружены.

Макровирусы являются программами на макроязыках, встроенных в такие системы обработки данных. Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макроязыки для автоматизации выполнения повторяющихся действий. Эти макроязыки часто имеют сложную структуру и развитый набор команд. Для своего размножения вирусы этого класса используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Скрипт-вирусы, также, как и макровирусы, являются подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

**Есть классификация вирусов по способу заражения файлов, где есть перезаписывающие и паразитические вирусы, вирусы-компаньоны, вирусы-ссылки, файловые черви, OBJ-, LIB-вирусы и вирусы в исходных текстах.**

Метод заражения перезаписью является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов

происходит различными методами — путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы).

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место. При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу.

Таким образом, при запуске зараженного файла первым управление получает код вируса. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т. е. дублируют работу ОС).

Есть несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется.

Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовок EXE-файла, в «дыры» между секциями EXE-файлов или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса. Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (EPO-вирусы — Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и выскочить на свободу только при некоторых ограниченных условиях.

Перед тем, как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле — иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например, поиск в файле последовательности

стандартного кода заголовков процедур языков программирования (C/Pascal), дизассемблирование кода файла или замена адресов импортируемых функций.

К категории вирусов-компаньонов относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD.

Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном катагоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Вирусы-ссылки или link-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Файловые черви никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии — например, INSTALL.EXE или WINSTART.BAT.

Некоторые файловые черви могут записывать свои копии в архивы (ARJ, ZIP, RAR). Другие записывают команду запуска зараженного файла в BAT-файлы.

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.

Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения. При этом вирус добавляет к исходным текстам свой исходный код (в этом случае вирус должен содержать его в своем теле) или свой шестнадцатеричный дамп (что технически легче). Зараженный файл способен на дальнейшее распространение вируса только после компиляции и линковки.

Специалисты «Лаборатории Касперского» подготовили летом 2012 года список из 15 наиболее заметных вредоносных программ, оставивших свой след в истории:

1986 Brian – первый компьютерный вирус; он распространялся за счет записи собственного кода в загрузочный сектор дискет.

1988 червь Морриса заразил примерно 10% компьютеров, подключенных к Интернету (т.е. около 600 компьютеров).

1992 Michelangelo – первый вирус, который привлек внимание СМИ.

1995 Concept – первый макровирус.

1999 Melissa ознаменовал наступление эры массовых рассылок вредоносного ПО, приводящих к глобальным эпидемиям.

26 апреля 1999 года произошла первая глобальная компьютерная катастрофа. Вирусом "Чернобыль" или CIH программисты, разве что, не пугали своих детей. По различным данным, пострадало около полумиллиона компьютеров по всему миру, и никогда еще до этого момента последствия вирусных эпидемий не были столь масштабными и не сопровождались такими серьезными убытками

2003 Slammer – бесфайловый червь, вызвавший широкомасштабную эпидемию по всему миру.

2004 Cabir – первый экспериментальный вирус для Symbian; распространялся через Bluetooth.

2006 Leap – первый вирус для платформы Mac OSX.

2007 Storm Worm [Zhelatin] – впервые использовал для управления зараженными компьютерами распределенные командные серверы.

2008 Koobface – первый вирус, целенаправленно атаковавший пользователей социальной сети Facebook.

2008 Conficker – компьютерный червь, вызвавший одну из крупнейших в истории эпидемий, в результате которой заражению подверглись компьютеры компаний, домашних пользователей и правительственных организаций в более чем 200 странах.

2010 FakePlayer – SMS-троянец для смартфонов на базе Android.

2010 Stuxnet – червь, с помощью которого была осуществлена целевая атака на системы SCADA (Supervisory Control And Data Acquisition – Диспетчерское управление и сбор данных), ознаменовавший начало эры кибервойн.

2011 Duqu – сложная троянская программа, которая собирает информацию промышленных объектах.

2012 Flame – сложная вредоносная программа, которая активно используется в ряде стран в качестве кибероружия. По сложности и функционалу вредоносная программа превосходит все ранее известные виды угроз.

2017 WannaCry - вредоносная программа, сетевой червь и программа-вымогатель денежных средств, поражающая только компьютеры под управлением операционной системы Microsoft Windows. Программа, используя уязвимость в порте SMB, шифрует почти все хранящиеся на компьютере файлы и требует денежный выкуп за их расшифровку. Её массовое распространение началось 12 мая 2017 года — одними из первых были атакованы компьютеры в Испании, а затем и в других странах. В этом же году произошла эпидемия нового подобного вируса под кодовым названием «Petya».
Учитывая эти эпидемии, возникает естественный вопрос: как защищаться?
И одним из элементов защиты компьютерной сети являются, конечно же, антивирусные программы.

3) **Антивирусная программа или антивирус — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики —**

**предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.**

**Наличие антивируса на современном компьютере или ноутбуке – вынужденная необходимость, которую никак нельзя обойти стороной при установке программного обеспечения на компьютер. Цель антивирусной программы, или антивируса, – обнаружение компьютерных вирусов, а также вредоносных программ, которые, как вариант, блокируют нормальною работу компьютера, а также антивирусы являются способом профилактики, защиты файлов и операционной системы от вредоносных кодов программ-вирусов.**

4) **Здесь также есть свои классификации: по способу воздействия и по способу защиты от вирусов.**

**В первой есть дискретные и поточные антивирусы, т.е. программы, которые непрерывно сканируют потоки данных, например, интернет-трафика, и принудительно запускаемые программы с целью сканирования определенных, указанных объектов.**

**Во второй различаются антивирусы так: детекторы, доктора, ревизоры, фильтры, вакцины, мониторы.**

Программы-детекторы позволяют обнаружить файлы, зараженные каким-либо известным вирусом. Данные программы проводят только проверку компьютера на наличие вирусов. Лечить данные программы не могут. Они находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса.

Программы-доктора позволяют не только обнаружить файлы, зараженные известным вирусом, но и произвести их лечение. При лечении зараженных файлов программа-доктор удаляет тело вируса из файла, т.е. восстанавливает файл в том состоянии, в котором он находился до заражения вирусом.

Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Они работают следующим образом. При своем первом запуске они запоминают сведения о состоянии программ и системных областей диска компьютера, в которые входят загрузочные секторы, таблицы размещения файлов, корневой каталог. Предполагается, что в этот момент программы и системные области дисков не заражены. Затем при последующих проверках компьютера программы-ревизоры сравнивают состояние файлов и системных областей диска с исходным. Если произошли изменения, характерные для действий вируса, то они сообщают об этом пользователю. Разновидностью данных программ являются доктора-ревизоры. Они представляют собой комбинацию ревизоров и докторов, т.е. они могут не только обнаруживать изменения в файлах и системных областях дисков, но и в случае изменений автоматически вернуть их в исходное состояние. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей.

Программы-фильтры, постоянно находясь в памяти компьютера, следят за действиями, которые выполняются на компьютере. При появлении действий, указывающих на наличие вирусов, они сообщают об этом пользователю. К этим действиям можно отнести изменение файлов с расширением COM и EXE, снятие с файлов атрибута "только для чтения", прямая запись на диск, форматирование диска, установка "резидентной"

(постоянно находящейся в оперативной памяти) программы. При появлении таких действий, на экран компьютера выводится сообщение о том, какое действие затребовано, и какая программа желает его выполнить. Пользователь может либо разрешить выполнение этого действия, либо запретить его. Программы-фильтры обладают одним большим преимуществом по сравнению с другими программами. Оно заключается в том, что данные программы 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. Программы-фильтры таким образом обнаруживают вирус на ранней стадии, пока он не начал размножаться. Это небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

Программы-вакцины – это программы, предотвращающие заражение файлов. Сущность действия данных программ заключается в том, что они изменяют файлы специальным образом. Причем это не отражается на работе, но вирус воспринимает эти файлы как зараженные и не внедряется в них. В настоящее время данный вид программ практически не используется.

Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас".

Классификация достаточно условна, поскольку многие антивирусы применяют различные способы обнаружения вирусов одновременно.

На текущий момент известно множество выпущенных антивирусных ПО…

5) **(перечислить). Теперь вопрос: по какому признаку пользователь должен выбрать себе антивирусное ПО?**

6) **Это признак является определяющим для ПК – производительность.**

Независимая лаборатория AV-Comparatives в апреле 2016 года провела сравнительное тестирование 19 антивирусов на быстродействие и использование системных ресурсов на платформе Windows 7 Pro SP1 64-Bit.

Здесь представлены характеристики влияния функционирования антивирусов на работу ПК.

Результаты, представленные AV-Comparatives в отчете данного сравнительного тестирования антивирусов на быстродействие, показывают лишь влияние на производительность системы (главным образом компонентов real-time/on-access защиты) различных антивирусных программ в данных конкретных тестах.

Пользователям предлагается попробовать антивирусную программу на их собственном компьютере и посмотреть, как антивирус работает на конкретной конфигурации системы.

Тестирование на быстродействие антивирусов проводились на ноутбуке Lenovo ThinkPad E560 с процессором Intel Core i5-6200 CPU, 8 ГБ (RAM) оперативной памяти и SSD дисками. Эксплуатационные испытания проводились на чистой и полностью обновленной системе Windows 7 Pro SP1 64-Bit (на английском языке), а затем с установленной антивирусной программой (с настройками по умолчанию). Тесты проводились при активном подключении к Интернету, чтобы обеспечить реальное влияние облачных сервисов и функций.

Специалисты лаборатории AV-Comparatives использовали самые последние версии продуктов, доступные на момент тестирования (апрель 2016 год). Обратим внимание, что в отличие от тестов производительности, проводимых в предыдущие годы, данный тест включает продукты как категории “Антивирус”, так и категории и “Internet Security”. Лаборатория протестировала продукты, которые вендоры предоставляют для основной серии испытаний.

Были приняты меры для минимизации сторонних факторов, которые могли повлиять на результаты тестирования и / или на совместимость систем. Используемые в продуктах технологии оптимизации также были рассмотрены - это означает, что результаты представляют воздействие продукта на систему после некоторого периода использования продукта пользователем. Испытания проводились несколько раз (с включенной и отключенной технологией оптимизации) чтобы получить средние значения и исключить ошибки измерения. После каждого запуска, тестовый компьютер был дефрагметирован и перезагружен 6 раз. Исследователи симулировали различные виды файловых операций.

Антивирусы должны загружаться в системе на ранней стадии для обеспечения максимальной защиты - подобная загрузка влияет на время запуска компьютера. Точное измерение времени загрузки является сложной задачей. Самая главная проблема заключается в определение состояния полной готовности системы, потому что во многих средах стартовая активность продолжается некоторое время уже после того, как система стала полностью отзывчивой для пользователя. Важно также учитывать, когда защита антивируса является полностью активной, потому что это может быть важным критерием завершения процесса загрузки. Некоторые вендоры реализуют очень позднюю загрузку для своих продуктов - в этом случае система может быть медлительной некоторое время уже после того, как она полностью загрузилась. На самом деле продукт просто загружает свои службы и процессы с опозданием, оставляя систему уязвимой на некоторое время. Лаборатория считает, что данная ситуация может вводить в заблуждение, поэтому времена загрузки не публикуются в отчетах.

В итоге выявилось, что на тот момент лучшим антивирусом по характеристикам производительности был признан Avira Antivirus. Оно и понятно – его интерфейс максимально упрощён и приближен к базисному встроенному антивирусу «Защитник Windows», понимание регулирования его настроек не вызывает неудобств.

Современный компьютер требует наличия на компьютере нескольких видов защиты от вирусов, так как такой вариант позволит пользователю эффективно защищать компьютер от вредоносного кода. По своей сути, антивирусные программы – это программное обеспечение (ПО), которое может упредить вредоносное средство или заблокировать причину, но далеко не панацея. К тому же, современные антивирусные продукты часто запаздывают с решениями, а против новых вирусов старые сигнатуры не действуют. Поэтому помимо антивирусов надо обезопасить работу также и в загрузчике интернет-страниц, т.е. в браузере.