

**Антивирус** – это компьютерная программа, которая защищает устройство от нежелательных программ, зараженных файлов и различных вредоносных вирусов.

Наличие антивируса на современном компьютере или ноутбуке – вынужденная необходимость

### **Задачи антивируса**

Основными задачами, которые ставятся перед программным антивирусным обеспечением, являются:

- препятствие проникновения зараженной информации в компьютерную систему;
- минимизация последствий от вирусов; обнаружение источника вируса; удаление и нейтрализация вредоносных файлов.

**Виды антивирусов** в зависимости от условий эксплуатации антивирусы бывают:

- постоянного действия – это средства, сканирующие потоки различных данных в интернете, почтовые фильтры и т. д.;
- периодического действия – это средства, работающие по запросу, предназначенные для однократного сканирования рабочей системы.

Антивирусные программы различаются по виду (способу) защиты от вирусов.

Тут можно выделить следующие:

- Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса.
- Программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов NortonAntiVirus, DoctorWeb, KasperskyAntivirus.
- Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. 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-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".
- Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

Современный компьютер требует наличия на компьютере нескольких видов антивирусных программ, так как такой вариант позволит пользователю эффективно защищать компьютер от вредоносного кода. По своей сути, антивирусные программы – это программное обеспечение (ПО), с которым довольно сложно разобраться неподготовленному пользователю как в смысле выбора антивируса, так и в плане установки данного ПО на компьютер. К тому же, современные антивирусные продукты часто запаздывают с решениями, а против новых вирусов старые сигнатуры не действуют.

### **Обзор бесплатных антивирусов для эффективной защиты компьютера**

Антивирусы бывают бесплатные, частично-бесплатные и платные.

### **Обзор бесплатных антивирусов**

Естественно, обзор будет только тех антивирусов, которые умеют работать в режиме реального времени – то есть висят постоянно в процессах и постоянно следят за работой пользователя. Стоит обратить внимание всех пользователей, какой бы антивирус вы не выбрали, при установке с сайта разработчика, уделите внимание прочтению содержимого страницы или меню установщика перед нажатием кнопки «скачать» или «установить». Очень часто в подарок к скачиваемому антивирусу *прилагается ненужное программное обеспечение, которое будет тормозить работу вашего компьютера*. Перед началом установки, всегда можно *отказаться от «подарка»*, сняв галочки в специальном меню установщика. Будьте внимательны!

Обзор лучших бесплатных антивирусов

Самый дружелюбный и бесплатный **Avast**

Avast! FreeAntivirus. Самый популярный бесплатный антивирус для домашнего использования. Постоянно отслеживает почту, трафик, чаты, P2P сети на наличие вирусов, червей, шпионских программ и т.п. Может сканировать систему не только по запросу или планировщику, а и предоставляет возможность проверки до загрузки Windows. Есть «игровой режим», позволяющий в одно нажатие отключить всплывающие сообщения.

Приятные мелочи в виде инструмента обновления программ, установленных на ПК и «удаленный помощник» с возможностью полного управления компьютером, на котором установлен такой же антивирус. Недостатком этого антивируса является реклама, которая назойливо предлагает пользователю перейти на платную версию путем обновления. Часто непосвященный пользователь нажимает кнопку «обновить», думая, что обновит вирусные базы, обновляется до платной версии, которая по истечении пробного периода перестает работать, требуя ключ.

Начиная с 2014 года, разработчики «Avast! FreeAntivirus» требуют бесплатную регистрацию, которую необходимо сделать в течение 30 дней, с момента установки программы. Жирный плюс в этой регистрации, что введенные данные не проверяются, т.е. фамилию, имя и электронный адрес можно ввести «от фонаря». Если вы ищите хороший и эффективный бесплатный антивирус, то мы в первую очередь посоветовали бы вам «Avast! FreeAntivirus».

**Борец рекламой Antivirus+**

Ad-AwareFreeAntivirus+. Достойный бесплатный антивирус. Защищает персональный компьютер от вирусов, троянских программ, рекламы, сайтов-паразитов, мошеннических программ, программ-шпионов и т.п. Антивирус умеет сканировать процессы в оперативной памяти, а также выполнять выборочное или полное сканирование по запросу пользователя либо по планировщику заданий.

Через 30 дней работы антивирус выдает сообщение об окончании работы пробной версии. Зато предлагает купить платную версию либо, оставшись на бесплатной версии, лишиться некоторых возможностей. Таких как проверки почты, сканирования внешних носителей и ещё десятка приятных мелочей.

**Ещё один «последний русский»**

AviraFreeAntivirus. Отличный бесплатный антивирус по функционалу смахивает на «Avast! FreeAntivirus». Он отлично справляется с макровирусами и способен обновляться оффлайн. Однако, есть негатив от пользователей, что Avira определяет взломанные игры и программы как вирус, удаляя их. Поэтому устанавливать его рекомендуется на компьютеры для офиса и дома. Антивирус надежно их защитит совершенно бесплатно.

**Редчайший случай – получить что-то полезное от Microsoft совершенно бесплатно**

MicrosoftSecurityEssentials. 100% бесплатный антивирус от самой Microsoft. Антивирус сам обновляется, практически не потребляет системные ресурсы. По заявлению многих пользователей этого антивируса, он иногда пропускает рекламу, шпионские модули и вредоносные программы. Но исследовав иностранные

ресурсы, можно смело сделать выводы, что на «MicrosoftSecurityEssentials» русскоязычные пользователи просто наговаривают, не веря, что «бесплатный сыр» бывает ещё и вкусным.

Этот антивирус подойдет всем пользователям, у которых довольно старые компьютеры, имеющие процессор с одним ядром и малый объем оперативной памяти. Негатива к антивирусу от Microsoft всего два. Не работает с Windows XP и работает в системе незаметно. Эта незаметность настораживает пользователей, в отличие от других антивирусов, которые постоянно выводят сообщение о том, что в системе полный порядок, или обнаружена угроза. «MicrosoftSecurityEssentials» работает незаметно, чем и пугает. Но если открыть файл отчёта за месяц работы антивируса, можно увидеть, что в карантине много подозрительных файлов, что свидетельствует об активности антивируса.

### **Мишка Панда на страже**

PandaCloudAntivirus. Отличный антивирус, защищающий компьютер по принципу «облака» — создает виртуальный компьютер между Windows и интернет. Однако из-за этого «облака», при работе в сети интернет, заметно торможение загрузки больших интернет страниц. В бесплатной версии реализован эвристический анализ и сканирование.

Скромно потребляет системные ресурсы, благодаря чему получил широкую популярность среди программистов, работающих на очень старых компьютерах. Программисты очень любят животных — пингвинов, кошек, панд, чертиков с вилами....

### **Бесплатных антивирусов не счесть**

Существует много бесплатных антивирусов, таких как «ComodoAntivirus», «PC ToolsAntiVirusFree», «Zillya! AntivirusFree», «AVG AntiVirusFree», «360 TotalSecurity». Все, перечисленные антивирусы также работают в режиме реального времени, но к их работе есть много вопросов и проскакивают негативы относительно торможения систем, после установки. Огромный негатив, подрывающий работу антивируса — это невозможность программы своевременно распознать вирус или вредную программу, чем и провинились перечисленные антивирусы.

### **Чудо-звери**

Антивирус, который не желательно устанавливать на персональный компьютер. Есть известные «чудо-звери» от китайских разработчиков под названием «Baidu» и «360 InternetSecurity». А последнее время появляются всё новые и новые антивирусы от китайцев, узнать их можно по иероглифам. Китайские антивирусы очень сильно нагружают систему. Удалить их очень сложно. И до сих пор эффективность их на постсоветском пространстве не доказана!

### **Как не заразить компьютер вирусами?**

На сегодняшний день существуют (и активно делают гадости!) сотни и тысячи вредоносных программ. Все они способны «заразить» Ваш компьютер, нарушить его работу, представить данные с жестких дисков злоумышленникам. Существуют элементарные правила, соблюдая которые можно в разы уменьшить или даже свести к нулю риск заражения компьютера вирусами.

### **Правило 1. Установите антивирусное ПО.**

Антивирусное ПО или антивирус — важнейший элемент защиты. Предлагать какой — либо конкретный антивирус не имеет смысла, т.к. каждый из существующих ныне имеет свои преимущества. Дадим лишь совет: при покупке антивирусного ПО не скупитесь! В противном случае защиту компьютеру не обеспечите, а только «выкинете на ветер» свои деньги. Если Вам трудно определиться, какую программу лучше всего купить — «возьмите» пробник. Практически у каждой антивирусной компании существует сайт, на котором можно бесплатно скачать пробную версию программы (обычно на 30 дней). Загрузи такую, «убьете двух

зайцев»: обеспечите безопасность своих данных и определите – стоит ли такой антивирус своих денег и нужно ли его приобретать.

## **Правило 2. Гуляйте там, где безопасно!**

В наше время даже самый неопытный пользователь компьютера и Интернета не ограничивается только посещением Одноклассников и работой с документами Word. Гуляя по просторам Сети, многие из нас ищут фильмы, музыку, игры, торренты и т.п. А где мы все это ищем? Правильно. На различных сайтах – на знакомых уже нам с прошлого посещения и совсем новых, где не летал курсор мыши человека. Так вот сократить риск заражения компьютера можно посещением интернет – ресурсов, известных Вам, Вашим родственникам и друзьям. Купить антивирус – полдела. Даже самое дорогое антивирусное ПО способно ошибиться и пропустить вредоносный код с сайта. Это стоит учитывать!

## **Правило 3. Доверяй, но проверяй!**

Вирусы и вредоносные программы способны проникать в компьютер не только из Интернета, но и со съемных носителей – дисков, флеш – карт и т.д. Получается, хоть и не умышленно, но Вы сами можете «заразить» свой компьютер, просто принеся «игрушку» от друга. При чем «заразой» может служить не только игра, но и программа, картинка, трек или неизвестного расширения файл. Перед тем, как нести свой или чужой диск или флешку к себе домой (и не только к себе!), нужно удостовериться, что на другом компьютере установлен антивирус. Убедившись в наличии антивирусного ПО, проверьте свой съемный накопитель на «инфекцию» и только после этого можете его использовать у себя на компьютере.

## **Правило 4. Не поддавайся!**

Социальные сети в последнее время стали эффективным каналом распространения компьютерных угроз. Наверное, каждый из нас сталкивался с тем, что к нему приходили письма от неизвестных людей, нередко даже с просьбами что – то скачать. Часто необходимость в том, что бы именно Вы загрузили, объяснялась необычными подарками, которые Вы получите. Так вот файлы, которые «необходимо» загрузить – вирусы. Получайте программы и другую информацию только от друзей и знакомых и все равно проверяйте загруженное антивирусом!

## **Правило 5. Профилактика.**

Регулярно проводите проверку собственного компьютера антивирусом. Бывает, программа не сразу заметит вредоносный файл, а после повторного сканирования обнаружит и удалит.

Ну вот и все! Соблюдайте приведенные правила, и будет Вам счастье!

## **Простые правила безопасности в интернете**

1. Никогда не сохраняйте пароли! Допустим, вы входите на этот сайт, и компьютер предлагает вам «Сохранить/запомнить пароль?» Нет, никогда! Все пароли сохраняются в специальном файле на компьютере, и какой-нибудь вирус-троян его прочитает и перешлет злоумышленникам. Пароль для почты и других аккаунтов должен быть сложным, тогда его будет нелегко или невозможно подобрать. Лучше всего, если пароль состоит из цифр и букв разного регистра, например, 27gtsy7T9GGI. Не стоит для пароля брать дату своего рождения и т.п. Самым распространенным в 2013 году признан такой пароль: 123456.

2. Не имейте один и тот же пароль для почты, для регистрации на сайтах (в одноклассниках, в контакте, еще где-то).

3. В наше время в интернете ОЧЕНЬ много вирусов! Поэтому на своем компьютере ОБЯЗАТЕЛЬНО нужно иметь антивирусную программу и файервол. Можно купить лицензионный антивирусник на год (это примерно стоит 1000-2000 рублей), тогда вы сможете все время обновлять свои антивирусные базы, ведь

новые вирусы появляются почти ежедневно. Можно скачать бесплатный антивирусник (но защита будет уже не совсем сильная, какие-то вирусы он может и не ловить), но это все равно лучше, чем ничего.

4. Конечно, если вы обмениваетесь с людьми информацией через диски, флешки, дискеты и другие носители, то вирусы могут проникнуть и оттуда. Не поленитесь проверить такой носитель на вирусы, прежде, чем начать загружать информацию с него.

5. Бывает, что вирусы приходят через почту. Получаете письмо, в нем прикрепленный файл. Если это письмо от вашего знакомого, и он не упоминает о прикрепленном файле, спросите его, прикреплял ли он этот самый файл. Если письмо от незнакомого человека, такое письмо лучше сразу удалить. Самые опасные файлы имеют расширение exe, com, bat (это программы).

6. Имейте в виду, что самая большая вероятность подцепить вирус в Интернете - это когда вы заходите на сайт, где можно скачать игры, картинки, видео, всякое бесплатное, порносайты. Посещайте только проверенные сайты, знакомые вам.

7. Если вы что-то ищете через поисковик Яндекс, то при выдаче результатов, там всегда пишут, если сайт заражен. Что-то типа: «Этот сайт может угрожать безопасности вашего компьютера». Обращайте на это свое внимание! Конечно, заходить на такой сайт не стоит.

8. Как бы вы не берегли свой компьютер, а нежелательные файлы все равно в него попадут. Поэтому один из верных способов обезопаситься – форматировать его почаще (хотя бы 1-2 раза в год). Вы можете сохранять свои письма из Аутлука, ссылки Избранное, другие файлы на внешнем диске или на флешках, диски, компьютер форматировать и устанавливать на него все заново.