ВЫЯВЛЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Вредоносная программа – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.

К вредоносному программному обеспечению относятся:

- сетевые черви;
- классические файловые вирусы;
- троянские программы;
- хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Разновидности вредоносных программ

- компьютерный вирус;
- троян;
- шпионское программное обеспечение (Spyware);
- сетевые черви;
- руткиты (Rootkit).

Признаки заражения компьютера вредоносной программой

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали.

Косвенные признаки заражения компьютера

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

Действия при обнаружении заражения

- отключить компьютер от интернета (от локальной сети);
- если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер;
- прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (CD-диск, флэш-накопитель и т.д.);
- установить антивирус, если на вашем компьютере не установлено никаких антивирусных программ;
- получить последние обновления антивирусных баз. Если это возможно, для их получения выходить в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.

Методы защиты от вредоносных программ

- использовать современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- своевременно устанавливать патчи; если существует режим автоматического обновления, включить его;
- постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
- использовать специализированные программные продукты, которые для противодействия вредоносным программам используют так называемые эвристические (поведенческие) анализаторы, то есть

Классификация антивирусных программ

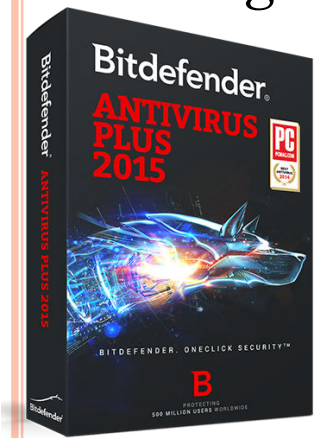
- сканеры;
- ревизоры;
- сторожа (мониторы);
- вакцины.

Современные антивирусные средства защиты и их основные функциональные особенности

- BitDefender Antivirus Plus;
- Eset NOD32;
- Kaspersky Antivirus;
- Dr. Web;
- McAfee VirusScan Plus.

BitDefender Antivirus Plus

- функция Heuristics in Virtual Environment – эмуляция виртуальной машины, с помощью которой проходят проверку потенциально опасные объекты с использованием эвристических алгоритмов;
- автоматическая проверка данных, передаваемых по протоколу POP3, поддержка наиболее популярных почтовых клиентов (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat и другие);

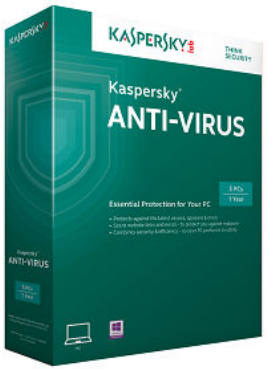


- защита от вирусов, распространяющихся через файлообменные Peer-2-Peer сети;
- формирование личного спам-листа пользователя.

Eset NOD32

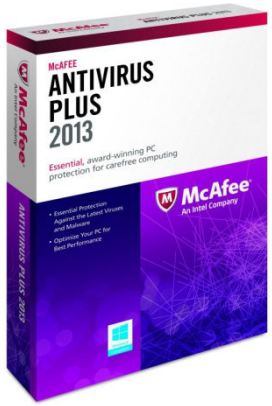
- эвристический анализ, позволяющий обнаруживать неизвестные угрозы;
- технология ThreatSense – анализ файлов для выявления вирусов, программ-шпионов (spyware), непрошенной рекламы (adware), phishing-атак и других угроз;
- проверка и удаление вирусов из заблокированных для записей файлов (к примеру, защищенные системой безопасности Windows библиотеки DLL);
- поверка протоколов HTTP, POP3 и PMTP.

Kaspersky Antivirus



- проверка трафика на уровне протоколов POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих, специальные плагины для Microsoft Outlook, Microsoft Outlook Express и The Bat!;
- предупреждение пользователя в случае обнаружения изменения как в нормальных процессах, так и при выявлении скрытых, опасных и подозрительных;
- контроль изменений, вносимых в системный реестр;
- блокирование опасных макросов Visual Basic for Applications в документах Microsoft Office.

McAfee VirusScan Plus



- защита от вирусов, макровирусов, троянов, Интернет-червей, spyware, adware, вредоносных элементов управления ActiveX и Java;
- автоматическая проверка входящей (POP3) и исходящей (SMTP) электронной почты;
- технологии ScriptStopper и WormStopper для блокирования вредоносной активности скриптов и червей.

Dr. Web

- защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;
- обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;
- проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);
- эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.