КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

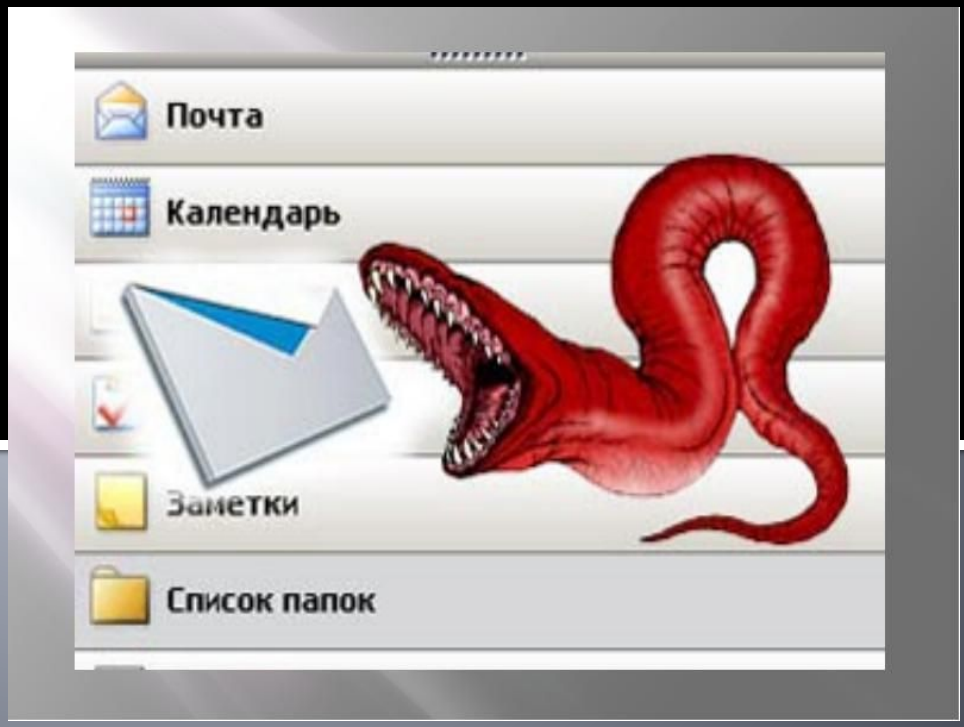
Компьютерный вирус – это программный код, встроенный в другую программу ,в документ или в определённые области носителя данных , предназначенный для выполнения несанкционированных действий на несущем компьютере.

ТИПЫ КОМПЬЮТЕРНЫХ ВИРУСОВ

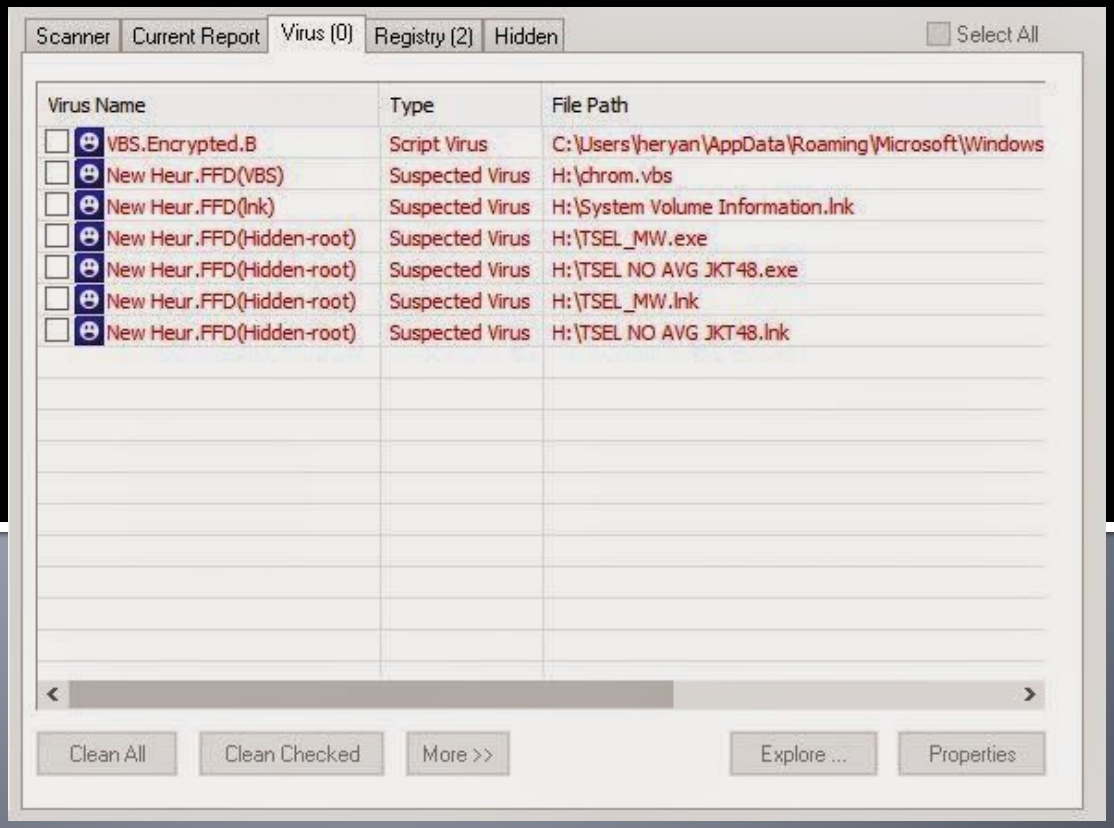
- Файловые вирусы
- Загрузочные вирусы
- Макровирусы
- Сетевые вирусы

ФАЙЛОВЫЕ ВИРУСЫ

Файловый вирус — компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной системы.



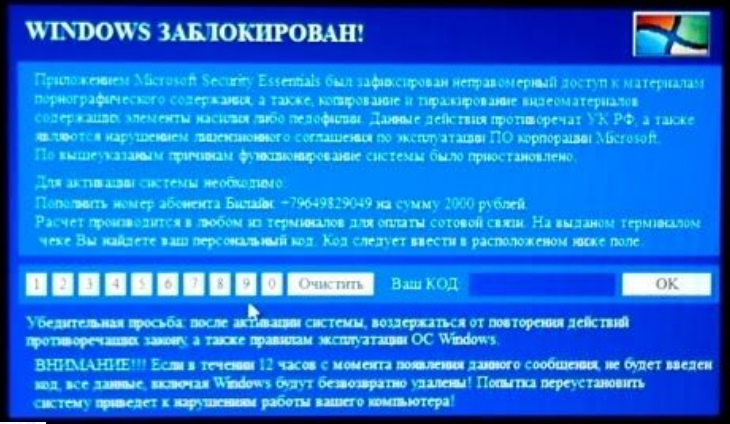
Собственно файловые вирусы — те, которые непосредственно работают с ресурсами операционной системы.
Пример: Virus.VBS.Sling) – вирус, который при запуске ищет файлы с расширениями .VBS или .VBE заражая их. 16-го июня или июля вирус при запуске удаляет все файлы с расширениями .VBS и .VBE, включая самого себя.



ЗАГРУЗОЧНЫЕ ВИРУСЫ

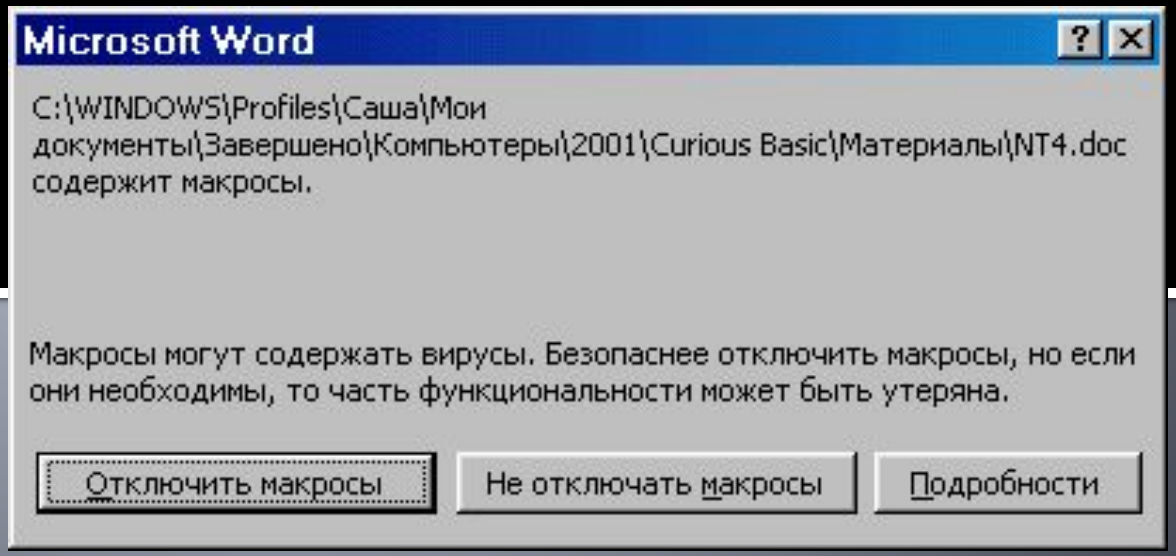
Загрузочный вирус – это блок программного кода, поражающий не программные файлы, а определённые системные области магнитных носителей.

Загрузочные вирусы внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска .



МАКРОВИРУСЫ

Макровирусы – это особая разновидность вирусов ,которая поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения макрокоманд.



Макровирусы — вирусы, написанные на языке макрокоманд и исполняемые в среде какого-либо приложения. Речь идет о макросах в документах Microsoft Office.
Пример: Macro.Word97.Thus - один из наиболее разрушительных макровирусов, который содержит три процедуры Document_Open, Document_Close и Document_New, для подмены стандартных макросов, выполняющихся при открытии, закрытии и создании документа, тем самым обеспечивая заражение других документов. 13 декабря срабатывает деструктивная функция вируса - он удаляет все файлы на диске C:, включая каталоги и подкаталоги. Macro.Word97.Thus.aa кроме указанных действий при открытии каждого зараженного документа выбирает на локальном диске случайный файл и шифрует первые 32 байта этого файла, постепенно приводя систему в неработоспособное состояние.

СЕТЕВЫЕ ВИРУСЫ

Сетевые вирусы -это вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Это, в первую очередь, конечно, электронная почта, различные интернет-мессенджеры, файлообменные и торрент-сети, локальные сети, сети обмена между мобильными устройствами.

АНТИВИРУС

Антивирус – это специализированная программа, которая предназначена для поиска и уничтожения компьютерных вирусов, а также для предохранения от заражения вирусом.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Для защиты от вирусов обычно используются: специализированные программы .
Выделяют:

- Полифаги
- Ревизоры
- Блокировщики

ПОЛИФАГИ

Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, Kaspersky Anti-Virus, Dr. Web). Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и операционной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.

Полифаги могут обеспечивать проверку файлов в процессе их загрузки в операционную память. Такие программы называются антивирусными мониторами.

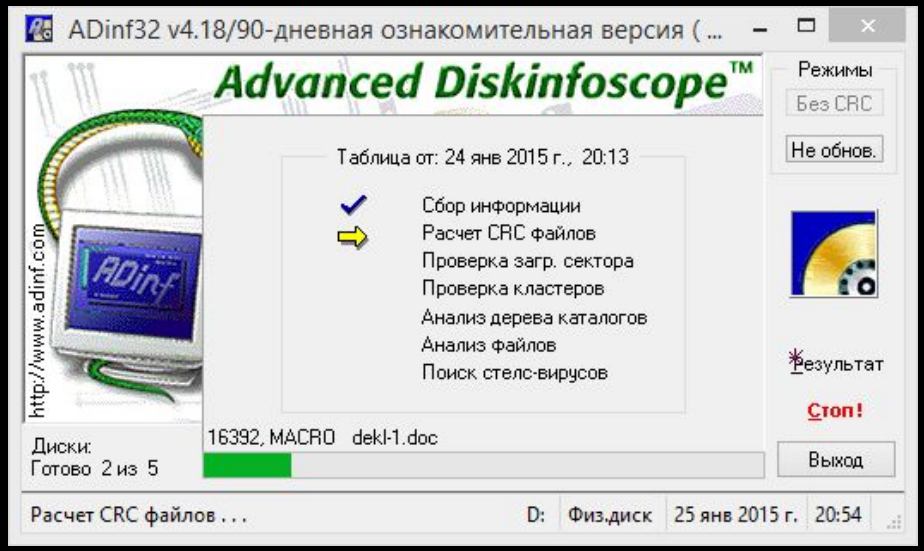
К достоинствам полифагов относится их универсальность. К недостаткам можно отнести большие размеры используемых ими антивирусных баз данных, которые должны содержать информацию о максимально возможном количестве вирусов, что, в свою очередь, приводит к относительно небольшой скорости поиска вирусов.

РЕВИЗОРЫ

Ревизоры. Принцип работы ревизоров (например, ADinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в база данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.

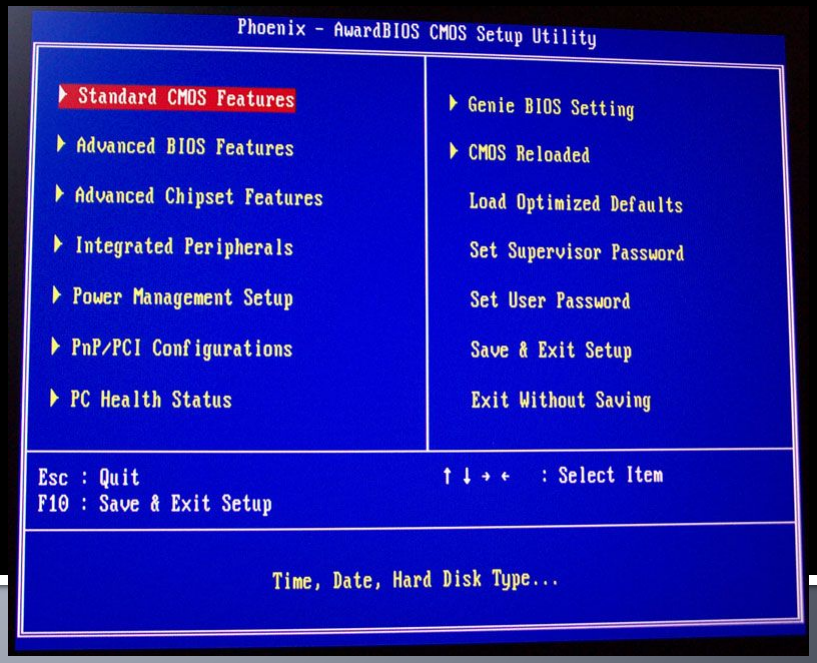
При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах, поскольку в их базах данных отсутствует информация об этих файлах.



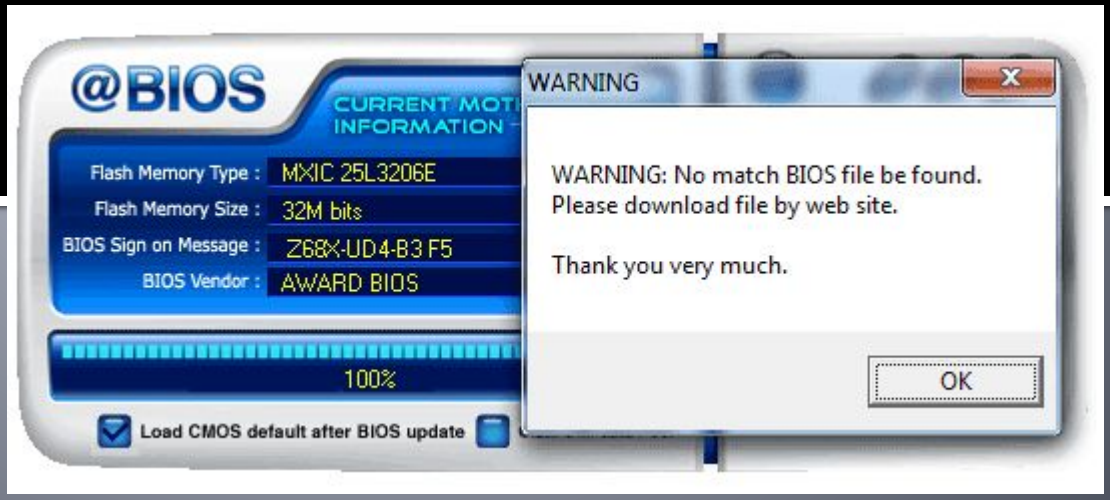
БЛОКИРОВЩИКИ

Антивирусные блокировщики – это программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К таким ситуациям относятся, например, запись в загрузочный файл сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.



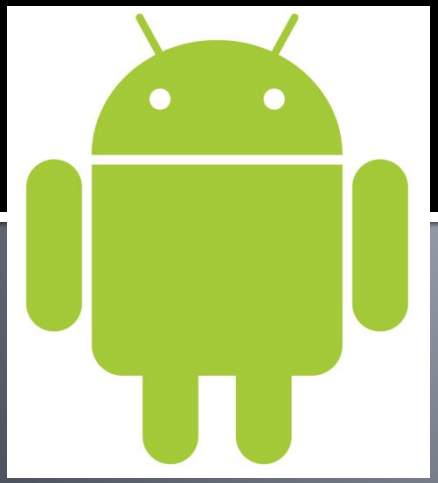
Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

К достоинствам блокировщиков относятся их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.

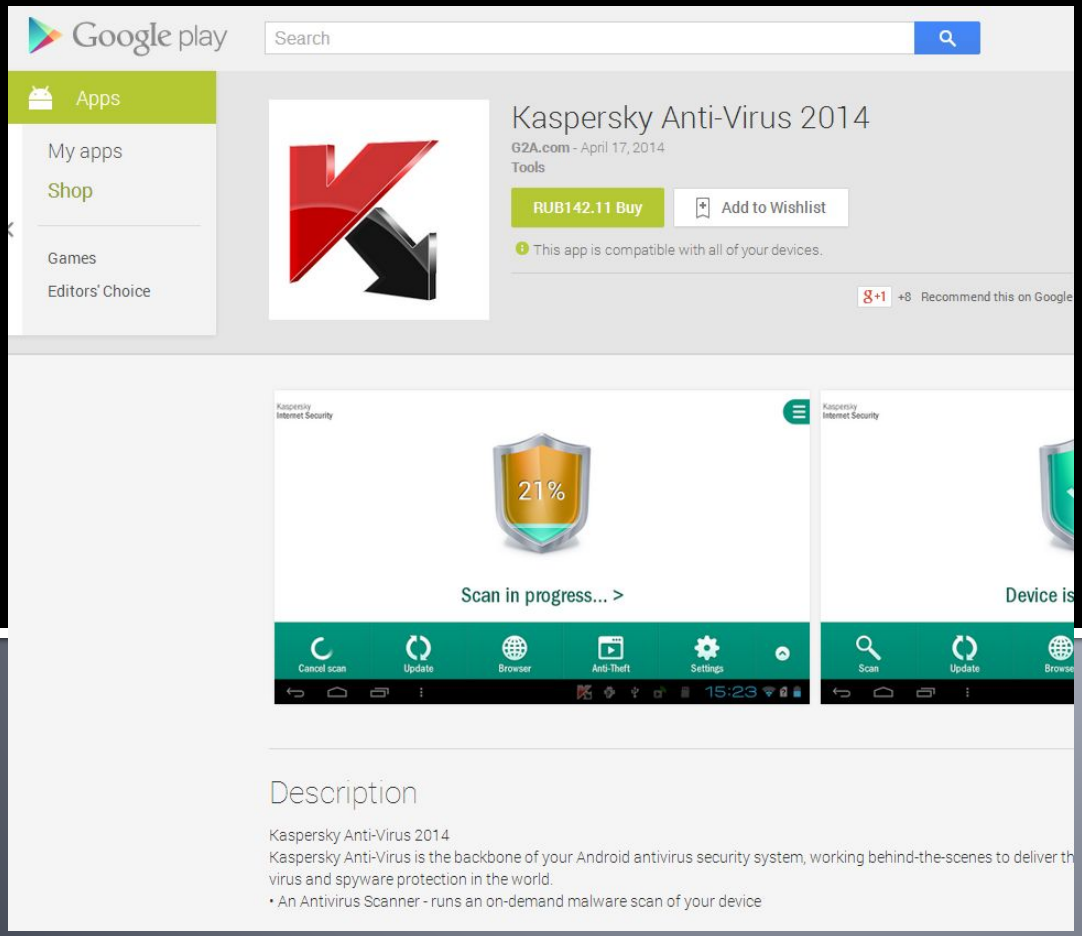


НУЖНЫ ЛИ АНТИВИРУСЫ ДЛЯ ANDROID?

Операционная система андроид имеет встроенные функции антивируса сама по себе. Приложения на Google Play проверяются на вирусы: при публикации приложений в магазине Google, они автоматически проверяются на вредоносный код с помощью сервиса Bouncer.
Google Play может удалять приложения : если Вы установили приложение, которое, как позже выяснилось, является вредоносным, Google может удалить его с Вашего телефона.



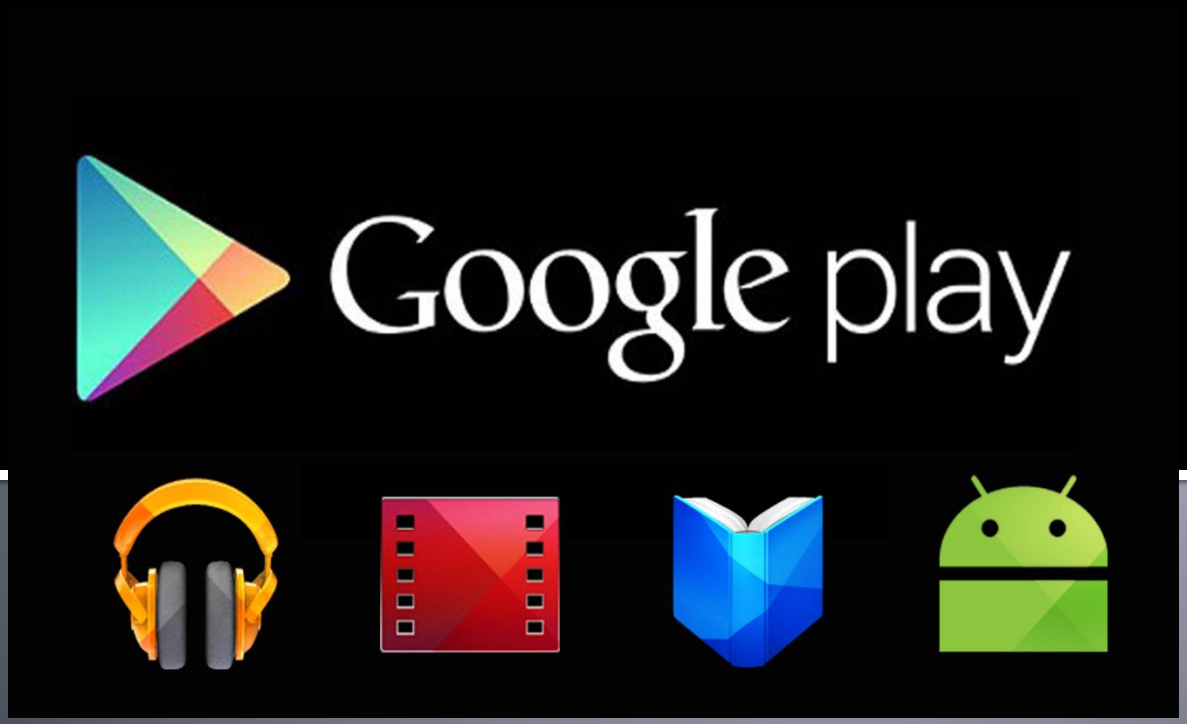
Android 4.2 проверяет сторонние приложения: как уже было написано выше, приложения на Google Play сканируются на вирусы, однако этого нельзя сказать про стороннее программное обеспечение из других источников.



- Android 4.2 блокирует отправку платных смс сообщений: в операционной системе запрещена фоновая отправка смс на короткие номера, которая часто используется в различных троянах, при попытке приложения отправить такое смс сообщение, вы будете об этом оповещены.

Android ограничивает доступ и работу приложений: система разрешений, реализованная в андроид, позволяет ограничить создание и распространение троянов, программ-шпионов и аналогичных приложений. Приложения на андроид не могут работать в фоновом режиме, записывая каждое ваше нажатие на экран или введенный символ. Кроме этого, при установке, Вы можете увидеть все разрешения, которые требуются программе.

Как показывает анализ, большая часть вирусов приходит из различного рода источников, где пользователи пробуют скачать платное приложение или игру бесплатно. Если для загрузки приложений Вы используете только Google Play — вы относительно защищены от троянов и вирусов. Кроме этого, собственная внимательность может вам помочь: например, не устанавливайте игр, которым требуется возможность отправки смс сообщений.



Однако, если вы часто загружаете приложения из сторонних источников, то антивирус может Вам понадобиться, особенно, если вы используете более старую, чем Android 4.2 версию операционной системы. Однако, даже с антивирусом, будьте готовы к тому, что скачав пиратскую версию игры для Андроид вы загрузите совсем не то, что ожидали.