**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ**

**ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»**

**(БГТУ им. В.Г. Шухова)**

Кафедра программного обеспечения вычислительной техники и

автоматизированныхсистем

Расчетно-графическое задание

дисциплина: Информатика

тема: **«Компьютерные вирусы, их свойства и классификация»**

Выполнил ст. группы ВТ-12

Воскобойников Илья Сергеевич

Белгород 2018

**Оглавление**

Введение3

Сетевой червь4

Способы распространения4

Признаки заражения 4

Способы защиты 5

Троянская программа6

Способы распространения6

Признаки заражения 6

Способы защиты 7

Эксплойт8

Способы распространения8

Признаки заражения 8

Способы защиты 8

Руткит9

Способы распространения9

Признаки заражения 10

Способы защиты 10

Кейлогеры11

Способы распространения11

Признаки заражения 11

Способы защиты 11

Бэкдор13

Способы распространения13

Признаки заражения 14

Способы защиты 14

Заключение15

**Список используемой литературы16**

**Введение**

Данная тема затрагивает каждого пользователя компьютера. Каждый когда-то сталкивался с вирусами. К тому же с каждым годом их количество и сложность растет. Поэтому данная тема будет актуальна всегда. И что бы постараться себя обезопасить и не заразить совой компьютер вирусами нужно разбираться в вирусах их классификациях, принципах работы, знать, как они могут попасть на компьютер и что на нем могут сделать. Зная это, вы будете максимально подготовлены к встрече с вирусами.

**Сетевой червь**

**Сетевой червь** — разновидность [вредоносной программы](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), самостоятельно распространяющейся через локальные и глобальные [Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) компьютерные сети.

**Способы распространения**

* Использование [уязвимостей](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) и ошибок администрирования в программном обеспечении, установленном на компьютере. [Червь Морриса](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D1%80%D0%B2%D1%8C_%D0%9C%D0%BE%D1%80%D1%80%D0%B8%D1%81%D0%B0) использовал известные на тот момент уязвимости в программном обеспечении, а именно в почтовом сервере [sendmail](https://ru.wikipedia.org/wiki/Sendmail), сервисе finger и подбирал пароль по словарю. Такие черви способны распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.
* Используя средства так называемой [социальной инженерии](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F), провоцируется запуск вредоносной программы самим пользователем. Чтобы убедить пользователя в том, что файл безопасен, могут подключаться недостатки пользовательского интерфейса программы — например, червь [VBS.LoveLetter](https://ru.wikipedia.org/wiki/VBS.LoveLetter) использовал тот факт, что [Outlook Express](https://ru.wikipedia.org/wiki/Outlook_Express) скрывает расширения файлов. Данный метод широко применяется в спам-рассылках, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы, и даже [эксплойтов](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82) под различные [операционные системы](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0).

**Признаки наличия**

Повышенная сетевая активность с резким взлётом исходящего трафика – явный признак того, что в компьютере орудует сетевой червь. Блокировка антивируса – также признак наличия сетевого червя. Помимо этого, вирусы, в частности, сетевые черви, любят блокировать доступ к официальным сайтам разработчиков антивирусного ПО.

**Способы защиты**

Антивирус с базовым функционалом защитой от сетевых червей можно назвать лишь условно. Антивирусные модули могут выявить факт заражения компьютера, заблокировать угрозу, но они не решают проблему с проникновением сетевых червей. Последние могут снова и снова настырно лезть через сеть, сколько бы их антивирус не блокировал. Тем не менее, хороший антивирус - обязательное условие работы на компьютере, если тот подключён к локальной сети или к Интернету. Подобрать для себя оптимальную антивирусную защиту вам поможет статья на нашем сайте [Какой антивирус самый лучший](http://remontcompa.ru/238-kakoy-antivirus-samyy-luchshiy.html).

В числе штатного функционала Windows инструментами для снижения рисков заражения системы сетевыми червями являются предустановленные настройки автоматического обновления системы и активированный брандмауэр (другое его название - файервол). В некоторых [пиратских сборках Windows](http://remontcompa.ru/507-piratskie-sborki-windows-za-i-protiv.html) обновления и брандмауэр могут быть отключены. Это не самый лучший способ выделить сборку среди массы аналогичных, если она рассчитана на обычных пользователей, а не профи. Так, с помощью обновлений компания Microsoft постоянно устраняет бреши системы и защищает её от новых опасностей, появляющихся в Интернете с каждым днём. Штатный брандмауэр (файервол) – это внедрённый в Windows, начиная с версии ХР, инструмент для защиты компьютера, в частности, как раз таки от сетевых червей. Брандмауэр проверяет данные, которые поступают по сети, и только после проверки разрешает или запрещает их дальнейшую передачу на компьютер.

**Троянская программа**

**Троя́нская программа** — разновидность [вредоносной программы](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), проникающая в компьютер под видом легального программного обеспечения, в отличие от [вирусов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81) и [червей](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%87%D0%B5%D1%80%D0%B2%D1%8C), которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

**Способы распространения**

Троянские программы распространяются людьми — как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах.

Для достижения последнего троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы ([файл-серверы](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80) и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, [электронной почтой](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0)), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы (в том числе, третьи).

**Признаки наличия**

Троянские программы обычно имеют следующие расширения:

* .exe, .com (под видом игр, офисных приложений и других легальных программ, расширение может быть не видно, если в Windows отключено отображение расширений, возможны файлы с «двойным» расширением, например, image.jpg.exe);
* .js, .vbs, .jse, .vbe, .bat, .cmd, .sh (скрипты; расширение может быть не видно, иногда файлы этих форматов можно прочитать в редакторе кода);
* .html, .htm, .shtml, .shtm, .xhtml, .xht, .hta (HTML документы; могут скачивать вирусы и другие вредоносные программы из Интернета, перенаправлять на вирусные и ложные сайты; файлы .hta работают вне браузера и может выполнять опасные действия непосредственно на компьютере);
* .pif (ярлык с возможностью выполнения вредоносных действий);
* .docm, .xlsm и т.п. (в электронных документах могут быть опасные макросы, обычно расширение заканчивается на «m»);
* .xml, .xsl, .svg, .xaml (XML-документы, аналогично HTML);
* .scr (программа, работающая зачастую скрытно);
* некоторые другие.

**Способы защиты**

В целом, троянские программы обнаруживаются и удаляются антивирусным и антишпионским ПО точно так же, как и остальные вредоносные программы.

Троянские программы хуже обнаруживаются контекстными методами антивирусов (основанных на поиске известных программ), потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бо́льшей задержкой, нежели самопроизвольно распространяемые вредоносные программы. Однако эвристические (поиск алгоритмов) и проактивные (слежение) методы для них столь же эффективны.

**Эксплойт**

**Экспл*о́*ит** — [компьютерная программа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), фрагмент [программного кода](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4) или последовательность [команд](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), использующие [уязвимости](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) в [программном обеспечении](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) и применяемые для проведения [атаки](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) на вычислительную систему. Целью атаки может быть как захват контроля над системой ([повышение привилегий](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B2%D1%8B%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D1%80%D0%B8%D0%B2%D0%B8%D0%BB%D0%B5%D0%B3%D0%B8%D0%B9)), так и нарушение её функционирования ([DoS-атака](https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0)).

**Способ распространения**

Эксплоит может распространяться в виде [исходных текстов](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D1%82%D0%B5%D0%BA%D1%81%D1%82), [исполняемых модулей](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D0%BF%D0%BE%D0%BB%D0%BD%D1%8F%D0%B5%D0%BC%D1%8B%D0%B9_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C) или словесного описания использования уязвимости. Он может быть написан на любом языке программирования (наиболее часто использующиеся: [C](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8_(%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F))/[C++](https://ru.wikipedia.org/wiki/C%2B%2B), [Perl](https://ru.wikipedia.org/wiki/Perl), [Python](https://ru.wikipedia.org/wiki/Python), [PHP](https://ru.wikipedia.org/wiki/PHP), [HTML](https://ru.wikipedia.org/wiki/HTML)+[JavaScript](https://ru.wikipedia.org/wiki/JavaScript))[[1]](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82#cite_note-1).

Эксплоиты могут быть классифицированы также по типу используемой ими уязвимости, такой как: [переполнение буфера](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BF%D0%BE%D0%BB%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B1%D1%83%D1%84%D0%B5%D1%80%D0%B0), [внедрение SQL-кода](https://ru.wikipedia.org/wiki/%D0%92%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D0%B5_SQL-%D0%BA%D0%BE%D0%B4%D0%B0), [межсайтовый скриптинг](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%B8%D0%BD%D0%B3), [подделка межсайтовых запросов](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0%B4%D0%B5%D0%BB%D0%BA%D0%B0_%D0%BC%D0%B5%D0%B6%D1%81%D0%B0%D0%B9%D1%82%D0%BE%D0%B2%D1%8B%D1%85_%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D1%81%D0%BE%D0%B2) и т. д.

**Признаки наличия**

Компьютер тормозит совершает операции без участия пользователя.

**Способы защиты**

Не скачивать и не отрывать файлы с [C](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8_(%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F))/[C++](https://ru.wikipedia.org/wiki/C%2B%2B), [Perl](https://ru.wikipedia.org/wiki/Perl), [Python](https://ru.wikipedia.org/wiki/Python), [PHP](https://ru.wikipedia.org/wiki/PHP), [HTML](https://ru.wikipedia.org/wiki/HTML)+[JavaScript](https://ru.wikipedia.org/wiki/JavaScript)

**Руткит**

**Руткит** — набор [программных средств](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих:

* маскировку объектов (процессов, файлов, каталогов, драйверов);
* управление (событиями, происходящими в системе);
* сбор данных (параметров системы).

Термин *Rootkit* исторически пришёл из мира [UNIX](https://ru.wikipedia.org/wiki/UNIX), и под этим термином понимается набор [утилит](https://ru.wikipedia.org/wiki/%D0%A3%D1%82%D0%B8%D0%BB%D0%B8%D1%82%D0%B0) или специальный [модуль ядра](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C_%D1%8F%D0%B4%D1%80%D0%B0), которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Этот набор, как правило, включает в себя разнообразные утилиты для «заметания следов» вторжения в систему, делает незаметными [снифферы](https://ru.wikipedia.org/wiki/%D0%A1%D0%BD%D0%B8%D1%84%D1%84%D0%B5%D1%80), сканеры, [кейлоггеры](https://ru.wikipedia.org/wiki/%D0%9A%D0%B5%D0%B9%D0%BB%D0%BE%D0%B3%D0%B3%D0%B5%D1%80), [троянские программы](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B), замещающие основные утилиты UNIX (в случае не ядерного руткита). Rootkit позволяет взломщику закрепиться во взломанной системе и скрыть следы своей деятельности путём скрытия файлов, процессов, а также самого присутствия руткита в системе.

В систему руткит может быть установлен различными способами: загрузка посредством эксплойта, после получения шелл-доступа (в таком случае, может использоваться средство типа wget или исходный [FTP-клиент](https://ru.wikipedia.org/wiki/FTP-%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82) для загрузки руткита с удаленного устройства), в исходном коде или ресурсах программного продукта.

### **Способы распространения**

 Самый популярный способ распространения: через программы обмена мгновенными сообщениями. Попав на компьютер, руткит рассылает сообщения, содержащие вредоносные вложения, всем, чьи адреса есть в списке контактов. Существует и более современный подход, который заключается во вставке вредоносного кода в файлы PDF. Для активизации достаточно просто открыть файл.

### **Признаки заражения**

  Как уже говорилось, обнаружить присутствие их в системе чрезвычайно сложно, но есть некоторые признаки, позволяющие предположить заражение:

* Компьютер не реагирует на действия мыши и клавиатуры.
* Настройки операционной системы меняются без участия пользователя - это один из способов руткита скрыть свои действия.
* Нестабильно работает доступ в сеть из-за значительно возросшего интернет-трафика.

 Стоит отметить, что правильно работающий руктит вполне способен не допустить появления всех этих симптомов, за исключением разве что последнего. Да и то только в случае, если компьютер выступает в роли ретранслятора спама или участвует в DDoS-атаках (объем трафика порой увеличивается так, что скрыть это не представляется возможным).

**Способы защиты**

Основная сложность борьбы с руткитами в том, что они активно противодействуют своему обнаружению, пряча свои файлы и ключи реестра от сканирующих программ, а также применяя другие методики. Существуют утилиты, специально созданные для поиска известных и неизвестных руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа. Удаление руткита – тоже сложный и многоэтапный процесс, который редко сводится к удалению пары файлов. Обычно приходится применять специальную программу, такую как [TDSSkiller](http://support.kaspersky.ru/5350), созданную для борьбы с руткитом TDSS. В некоторых случаях жертве даже приходится переустанавливать операционную систему, если в результате заражения компьютерные файлы повреждены слишком глубоко

**Кейлогеры**

**Кейло́гер** — [программное обеспечение](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) или [аппаратное устройство](https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BA%D0%BB%D0%B0%D0%B4%D0%BA%D0%B0), регистрирующее различные действия пользователя — нажатия клавиш на [клавиатуре компьютера](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BA%D0%BB%D0%B0%D0%B2%D0%B8%D0%B0%D1%82%D1%83%D1%80%D0%B0), движения и нажатия клавиш [мыши](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BC%D1%8B%D1%88%D1%8C) и т. д.

**Способы распространения**

Распространяется в интернете как exe файл иногда скачивает вместе с установочными файлами других программ.

**Признаки наличия**

Данный вирус сложно обнаружить но следуют обратить внимание на неизвестные запущенные службы и то чем они занимаются.

**Способы защиты**

Защита от «известных» несанкционированно установленных программных кейлоггеров:

* использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей с автоматическим обновлением сигнатурных баз.

Защита от «неизвестных» несанкционированно установленных программных кейлоггеров:

* использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют так называемые эвристические (поведенческие) анализаторы, то есть не требующие наличия сигнатурной базы.
* использование программ, шифрующих вводимые с клавиатуры данные, а также применение клавиатур, осуществляющих такое шифрование на аппаратном уровне;

Защита от «известных» и «неизвестных» несанкционированно установленных программных кейлоггеров включает в себя использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют:

* постоянно обновляемые сигнатурные базы шпионских программных продуктов;
* эвристические (поведенческие) анализаторы, не требующие наличия сигнатурной базы.

Защита от несанкционированно установленных аппаратных кейлоггеров:

* тщательные внешний и внутренний осмотры компьютерных систем;
* использование виртуальных клавиатур;

**Бэкдор**

**Бэкдор**— дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить [несанкционированный доступ](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF) к данным или удалённому управлению [операционной системой](https://ru.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) и [компьютером](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) в целом.

## **Способы распространения**

Бэкдоры не способны распространяться и заражать систему без ведома пользователя. Большинство таких паразитов нужно устанавливать вручную в связке с другим программным обеспечением. Существуют четыре основных способа, как эти угрозы попадают в систему.

* Неосознанные пользователи ПК могут случайно установить типичные бэкдоры на свои компьютеры. Они могут прийти прикрепленными к сообщениям электронной почты или программам обмена файлами. Авторы дают им неподозревающие имена и обманывают пользователя открыть или запустить такой файл.
* Бэкдоры часто устанавливаются другими паразитами такими, как вирусы, трояны или даже шпионские программы. Они попадают в систему без ведома и разрешения пользователя, который использует зараженный компьютер. Некоторые угрозы могут быть установлены вручную хакерами, которые имеют достаточно привилегий для установки программного обеспечения. Небольшая часть бэкдоров может распространяться за счет использования удаленных систем с некоторыми уязвимостями в системе безопасности.
* Несколько бэкдоров уже интегрированы в конкретные приложения. Даже законные программы могут быть подделаны удаленными функциями доступа. Атакующий файл должен связаться с компьютером через установку такой программы, чтобы мгновенно получить доступ к системе или взять на себя контроль над определенным программным обеспечением.
* Некоторые бэкдоры заражают компьютеры за счет использования определенных уязвимостей программного обеспечения. Они работают так же, как черви и автоматически распространяются без ведома пользователя. Пользователь не может заметить ничего подозрительного, так как угрозы не отображают никаких мастеров установок, диалоговых окон или предупреждений.

Широкое распространение бэкдоров в основном заражает компьютеры на операционной системе Microsoft Windows. Тем не менее, множество менее распространенных паразитов предназначены для работы в разных сферах, например для операционной системы Mac и других.

**Признаки наличия**

Компьютер ведет себя странно: перезагружается, создаются файлы, удаляются файлы,

меняются темы, появляются новые приложения.

## **Способы защиты**

Бэкдоры используют те же способы установки, что и другие [вирусы](http://profi-user.ru/virus/) (через ссылки, загружаемые файлы, при установке программ). Поэтому бороться с ними нужно так же, как и с любым вредоносным ПО:

* Не переходить на подозрительные сайты;
* Внимательно смотреть, какие файлы собираетесь качать;
* Не выполнять действия, предлагаемые спамом, который приходит на электронную почту;
* Использовать лицензионный антивирус и регулярно его обновлять;

**Заключение**

В настоящее время известно более 5000 программных вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Итак, можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают жизненно важную, ценную информацию, что может привести не только к финансовым потерям, но и к человеческим жертвам.

Стоит помнить, что все в наших руках и если быть осторожным и пользоваться антивирусом, то можно и не столкнуться с вирусами.

**Список используемой литературы**

[**https://mydiv.net/**](https://mydiv.net/)

[**https://www.kaspersky.ru/**](https://www.kaspersky.ru/)

[**https://ru.wikipedia.org/**](https://ru.wikipedia.org/)

[**http://profi-user.ru/**](http://profi-user.ru/)

[**https://www.securitylab.ru/**](https://www.securitylab.ru/)

[**https://habr.com/**](https://habr.com/)