Источник: https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017

**Безопасность при работе с компьютером 2017**

[Безопасность](https://losst.ru/security) Январь 11, 2017 [1](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#comments) [admin](https://losst.ru/author/admin)

Интернет — довольно агрессивная среда, где кроме полезной информации и нужных программ, есть вирусы и злоумышленники. И чем большую популярность набирают современные технологии, тем больше мошенников они привлекают. В 2016 году мы видели DDOS атаки, организованные с помощью целых сетей IoT устройств и камер видеонаблюдения, про безопасность которых никто не подумал.

Методы вымогателей становятся более изощренными. В прошлом году было захвачено много компьютеров с целью требования выкупа за расшифровку файлов. В том числе это были и серверы под Linux. Осенью лаборатория Касперского выпустила бюллетень по безопасности. В нем были обозначены угрозы, которые могут поджидать нас в 2017. Возможно, они пока не существуют, но мы уже можем предпринять действия по защите. В этой статье мы рассмотрим как сохранять безопасность при работе с компьютером 2017.

Содержание статьи:

* [1. Обновление, обновление и еще раз обновление](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#1_1054107310851086107410831077108510801077_1086107310851086107410831077108510801077_1080_107710971077_108810721079_1086107310851086107410831077108510801077)
* [2. Подключение к интернету](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#2_10551086107610821083110210951077108510801077_1082_108010851090107710881085107710901091)
* [3. Резервное копирование](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#3_105610771079107710881074108510861077_10821086108710801088108610741072108510801077)
* [4. Защитите IoT устройства](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#4_10471072109710801090108010901077_IoT_1091108910901088108610811089109010741072)
* [5. Используйте правильный брандмауэр](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#5_10481089108710861083110010791091108110901077_1087108810721074108010831100108510991081_1073108810721085107610841072109111011088)
* [6. Системы обнаружения вторжений](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#6_1057108010891090107710841099_10861073108510721088109110781077108510801103_107410901086108810781077108510801081)
* [7. Отключите отслеживание](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#7_105410901082108311021095108010901077_108610901089108310771078108010741072108510801077)
* [8. Аккуратность в социальных сетях](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#8_104010821082109110881072109010851086108910901100_1074_1089108610941080107210831100108510991093_10891077109011031093)
* [9. Используйте двухэтапную аутентификацию](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#9_10481089108710861083110010791091108110901077_10761074109110931101109010721087108510911102_10721091109010771085109010801092108010821072109410801102)
* [Выводы](https://losst.ru/bezopasnost-pri-rabote-s-kompyuterom-2017#104210991074108610761099)

**1. Обновление, обновление и еще раз обновление**



В 2016 году компания Касперского обнаружила несколько вирусов, собирающих информацию о пользователях. Среди них одним из самых опасных был ProjectSauron. Это платформа, которая пыталась собирать сведения из правительственных организаций, провайдеров и научно-исследовательских станций.

Такие программы часто используют уязвимости в различном программном обеспечении. Обычно эти уязвимости уже закрыты разработчиком, но не все получили обновление. Далеко не все пользователи устанавливают обновления сразу после того, как они становятся доступны. Настройте автоматическую установку обновлений безопасности в Linux, Windows или Mac чтобы безопасность персонального компьютера или сервера оставалась на высоком уровне.

**2. Подключение к интернету**



Будьте аккуратны при работе компьютера в сети. Если вы используете публичное беспроводное подключение в одном из общественных мест, то ваши данные могут быть очень просто перехвачены злоумышленниками. Это касается любой операционной системы.

Во-вторых, на ваш компьютер могут попасть вирусы, которые управляются из сети. Например, в декабре 2015 компания Juniper Networks сделала шокирующее заявление, что в коде брандмауэров был обнаружен сторонний код, который потенциально мог дать доступ злоумышленнику к системам.

Невозможно проверить каждую строку кода операционной системы, даже если она имеет открытый исходный код. Любые действительно конфиденциальные данные лучше хранить на устройстве, которое не подключено к интернету. Это самая надежная защита.

**3. Резервное копирование**



Согласно сообщению Kaspesky количество атак вымогателей увеличилось в три раза в течение 2016 года. В среднем, одна атака на 40 секунд. По тому же отчету компании Касперского видно, что один из пяти человек, которые заплатили выкуп, не получил свои данные обратно.

Использование резервного копирования поможет свести к минимуму ущерб от вымогателей. Для резервного копирования лучше использовать внешний носитель или облако. Все можно настроить в любой операционной системе, например. в Linux можно использовать Rsync. Также можно настроить безопасность компьютера в WIndows и MacOS.

**4. Защитите IoT устройства**



В октябре 2016 года более 80 крупных веб-сайтов подверглись DDOS атаке, которая была организована с помощью тысяч взломанных IoT устройств. Китайская компания, производитель электронных компонентов призналась, что ее камеры видеонаблюдения были взломаны. Такие устройства, как смарт холодильники Samsung тоже были взломаны чтобы получить пароли Gmail их владельцев.

Всегда изменяйте пароли по умолчанию на свои, потому что во многих случая они могут очень просто использоваться злоумышленниками, а на многих устройствах пароль вообще не установлен. Для связи между устройствам лучше использовать более безопасную технологию — WPA PSK (AES).

**5. Используйте правильный брандмауэр**



Не только Juniper Networks пострадала от брандмауэра. В январе разработчики FortiOS тоже обнаружили сторонний код в используемом брандмауэре. Скорее всего, в 2017 году производители брандмауэров продолжат находить бэкдоры в своих продуктах.

Рассмотрите возможность установки свободного брандмауэра с открытым исходным кодом IPFire в своей организации. Вы можете использовать брандмауэр и дома, например, на компьютере Raspberry Pi, чтобы быть уверенным, что там точно нет никаких сюрпризов. IPFire разработан для людей, у которых нет опыта работы в сети и позволяет разделить вашу сеть на безопасные зоны.

**6. Системы обнаружения вторжений**



Антивирусы могут обнаружить далеко не все новые угрозы. В августе 2015 группа хакеров Sofacy запустила кибер атаку с помощью собственного инструмента Azzy. Kaspersky обновили свои базы данных, добавив туда эту программу. А хакеры выпустили новую версию в течение 90 минут, которая уже не обнаруживалась антивирусом.

В 2017 году антивирусы, которые работают на основе баз данных не смогут быстро выявить новые угрозы. Выбирайте программное обеспечение, которое использует обнаружение аномалий и блокирует любые необычные действия программ.

К таким продуктам можно отнести ClamAV. Также в Linux можно настроить SELinux и Apparrmor для противодействия вторжениям и добавления еще одной степени защиты. Это основные правила безопасности за компьютером.

**7. Отключите отслеживание**



Kaspersky предполагает, что в 2017 году рекламодатели и шпионы будут продолжать собирать конфиденциальную информацию о вас с помощью отслеживающих Cookie. Это означает что если, например, вы посетите сайт страхования жизни, они могут узнать, что вы купили книгу о болезнях сердца на Amazon.

Пользователи Google Chrome, Chromium, Firefox могут настроить браузер таким образом, чтобы их не отслеживали. Можно установить специальное расширение, чтобы блокировать весь код отслеживания и тем самым улучшить обеспечение безопасности компьютера.

**8. Аккуратность в социальных сетях**



Злоумышленники продолжат свои действия в социальных сетях в 2017 году. В июле 2016 года было взломано несколько учетных записей известных людей. В том числе и Марка Цукерберга.

Вы не можете контролировать серверы, на которых размещены ваши любимые веб-сайты социальных сетей. Но подумайте что вы размещаете в интернете и убедитесь что настройки конфиденциальности выставлены правильно.

**9. Используйте двухэтапную аутентификацию**



В июле 2016 года ряд аккаунтов знаменитостей были скомпрометированы, что привело к слухам, о том что Джей Блэк мертв. Некоторые пароли были получены из дампа данных сайта Likedin, который утек в сеть. Многие пользователи имели одинаковые пароли для разных сайтов.

Было бы замечательно, если бы все использовали сложный пароль для каждого нового сайта. Но это не очень практично. Тем не менее, популярные сайты, такие как Twitter, Likedin, Facebook поддерживают проверку в два этапа, когда вам на телефон должно прийти СМС с кодом активации при входе в систему с нового местоположения.

**Выводы**

Конфиденциальность и безопасность вашей личной информации на компьютере и в сети имеют очень важное значение. В этой статье мы рассмотрели как поддерживать безопасность при работе с компьютером 2017 на достаточно высоком уровне и уберечь себя от взлома.