Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей Хабаровского края)»

ПАМЯТКА

«ЛЕЧЕНИЕ» КОМПЬЮТЕРА ПОСЛЕ ЗАРАЖЕНИЯ ВИРУСАМИ

г. Хабаровск, 2021 год

Памятка ««Лечение» компьютера после заражения вирусами» / Сост. Е.А. Фомина – г. Хабаровск: КГАОУ ДО РМЦ, 2021. – 4 с.

Ответственный за выпуск: О.В. Монахова

«ЛЕЧЕНИЕ» КОМПЬЮТЕРА ПОСЛЕ ЗАРАЖЕНИЯ ВИРУСАМИ

Переустановка компьютера после того, как он был взломан, может быть кропотливым процессом, но это лучший способ убедиться, что все, что оставил злоумышленник, было найдено.

Контрольный список перед выполнением переустановки

- Смена паролей - вам следует изменить пароли ко всем системам, к которым вы подключались со своего компьютера, в период, когда он мог быть взломан. Особенно обратите внимание на сайты банков и кредитных карт, электронную почту и интернет-магазины, поскольку злоумышленник мог установить «ловушку паролей» на ваш компьютер. НЕ меняйте пароль на взломанном компьютере. Если у вас нет доступа к другим компьютерам, измените пароль после завершения процесса переустановки.
- Убедитесь, что ваши файлы данных имеют резервную копию. НЕ создавайте резервные копии приложений, таких как Microsoft Office, iTunes и т. д., Поскольку злоумышленник мог изменить файлы программы.
- Убедитесь, что у вас есть установочный носитель для вашей операционной системы, а также все остальные необходимые приложения и руководства по установке. Некоторые компьютеры поставляются без установочного носителя операционной системы, но с методом «восстановления», либо в виде диска, либо в виде специального раздела на жестком диске компьютера, предназначенного для восстановления вашего компьютера до «заводской установки по умолчанию».

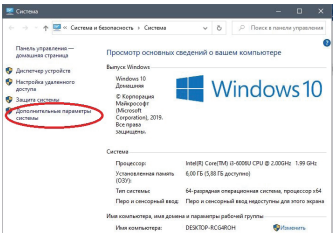
КАК «СПАСТИ» СВОЙ КОМПЬЮТЕР

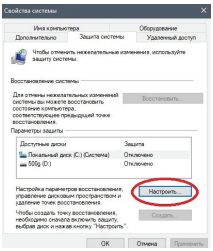
1. Убедитесь, что обновления вашего антивирусного программного обеспечения актуальны.

2. Используйте другую стороннюю утилиту для очистки от вирусов, троянских программ или червей. Возможно, ваше текущее антивирусное программное обеспечение не все обнаружит, поэтому использование нескольких утилит даст вам душевное спокойствие. Например, таких как Vipre Rescue, Vipre и Spybot.

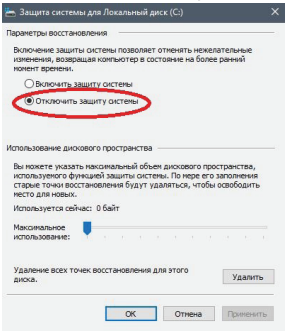
3 Выключите восстановление системы на ПК.

- Для этого щелкните правой кнопкой мыши значок «Мой компьютер».
- Выберите «Свойства».



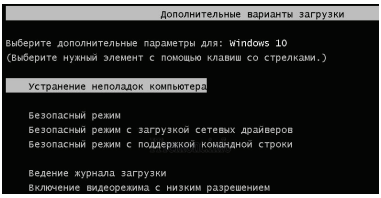


- Перейдите на вкладку «Восстановление системы»
- Установите флажок «Отключить восстановление системы»



4 Отсоедините сетевой кабель от компьютера, который вы планируете сканировать, если он подключен.

5 Перезагрузите компьютер в безопасном режиме. Большинство ПК используют F8 для перехода в безопасный режим. Итак, пока компьютер перезагружается, продолжайте нажимать F8.



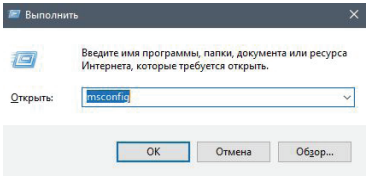
6 Вам будет предложено перейти в безопасный режим. Щелкните «Да».

7 В безопасном режиме перейдите в «Установка и удаление программ» в Панели управления и удалите приложения, с которыми вы не знакомы. Иногда установленное вредоносное программное обеспечение может быть указано здесь и может быть удалено.

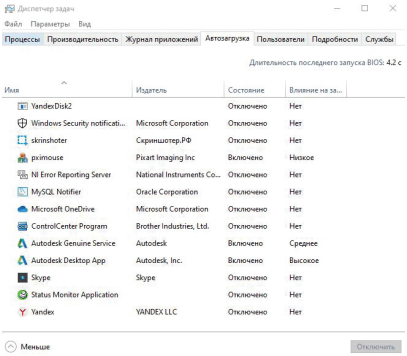
8 Запустите полное сканирование ПК с помощью Vipre Rescue, Vipre и Spybot. Запустите каждое приложение и сканируйте по одному в безопасном режиме.

9 Все еще в безопасном режиме

- Перейдите в Пуск > Выполнить, введите msconfig и нажмите Enter.



- Щелкните вкладку «Автозагрузка».



Снимите флажки с элементов, перечисленных в разделе «Автозагрузка» для тех приложений, которые не нужно запускать при запуске компьютера.

Если вы не знаете название, указанное в списке, «погуглите» его. Вы не хотите снимать отметку с системного процесса Windows, который необходим для запуска и работы системы. Но вы также должны убедиться, что сняли флажок с элемента автозагрузки, связанного с червем или вирусом, который может автоматически запускаться при запуске компьютера или запускать автоматическую репликацию при каждой перезагрузке.

10 Обратите внимание на то, что вы оставили отмеченными, а какие - не отмеченными (или отключенными при запуске).
Закройте окно, когда закончите.

11 Вам будет предложено перезагрузить компьютер. Перезагрузите компьютер и на этот раз запустите его в обычном режиме.

12 Теперь в нормальном режиме вам будет предложено внести изменения в конфигурацию. Просто поставьте галочку рядом, чтобы не показывать это снова, затем нажмите OK.

13 Щелкните правой кнопкой мыши на панели задач и выберите Диспетчер задач. Выберите вкладку процессов и сравните имена образов тех, которые вы записали в безопасном режиме. Завершите задачу тех процессов, которые вы не видели в безопасном режиме. По завершении закройте окно диспетчера задач.

14 Перейдите в Пуск > Выполнить, введите msconfig и нажмите Enter. Щелкните вкладку «Автозагрузка». Сравните элементы автозагрузки с теми, которые вы записали в безопасном режиме. Те, которые вы не отметили, остались снятыми? Был ли у них еще один элемент запуска, который выскочил и теперь проверяется? Если да, то найдите этот элемент автозагрузки в Google. Если он связан с вирусом, снимите флажок. Закройте окно, когда закончите, и перезапустите снова. Затем повторите с шага 11.

15 В обычном режиме запустите полное или глубокое сканирование ПК с помощью Vipre Rescue, Vipre и Spybot. Запускайте сканирование каждого приложения по одному. Повторяйте этот шаг до тех пор, пока компьютер не будет на 100% чист во всех 3 приложениях сканирования.

16 Включите восстановление системы на ПК.
- Для этого щелкните правой кнопкой мыши значок «Мой компьютер».
- Выберите «Свойства».
- Щелкните вкладку «Восстановление системы» и снимите флажок «Отключить восстановление системы».

17 Убедитесь, что ваше антивирусное приложение будет автоматически обновлять наличие вирусов и обеспечивает защиту в реальном времени.

18 Подключите сетевой кабель обратно и перезагрузите компьютер.

Обеспечение безопасности вашего компьютера

- Следите за обновлениями своей операционной системы и приложений. Включите функции автоматического обновления, если они доступны, и регулярно выполняйте проверки обновлений;
- Не отключайте брандмауэр и антивирусное программное обеспечение - злоумышленнику нужно всего лишь шагнуть в дверной проем, чтобы полностью взломать систему;
- Изучите и практикуйте цифровую безопасность.

Памятка ««Лечение» компьютера после заражения вирусами»

Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей
Хабаровского края)»
680000, г. Хабаровск, ул. Комсомольская, 87
тел. / факс: (4212) 30-57-13
Инстаграм: @dop.obrazovanie27
e-mail: yung_khb@mail.ru
http://www.kcdod.khb.ru
Подписано в печать: 30.09.2021 г.