Предотвращение заражения шифровальщиком WannaCry

В настоящее время распространяется шифровальщик WannaCry. Чтобы защтиться от заражения можно использовать следующие варианты:

1. **Включить критические обновления** (обновления безопасности) Windows и установить все предложенные обновления.
Внимание! Если к вас нелицензионная копия — могут быть проблемы!

2. **Установить патчи** закрывающие канал распространения вируса. Их можно скачать на официальном сайте Microsoft.
Зайти на Microsoft Security Bulletin MS17-010 - Critical , выбрать свою версию операционной системы и скачать патч. Затем установить его.
Можно воспользоваться Customer Guidance for WannaCrypt attacks. В конце статьи есть ссылки. В этом случае есть ссылки на патч для WindowsXP.
Чтобы проверить установлен ли уже у вас такой патч нужно
Перейти по ссылке выше и проверить код обновления для вашей системы, например для Windows 7 или Windows Server 2008 R2, код будет 4012212 или 4012215

- Открыть cmd.exe (командную строку)
- Написать: wmic qfe list | findstr 4012212
- Нажать Enter
- Если в ответе вы увидите что-то подобное, это значит что патч у вас уже установлен и можно спать спокойно:

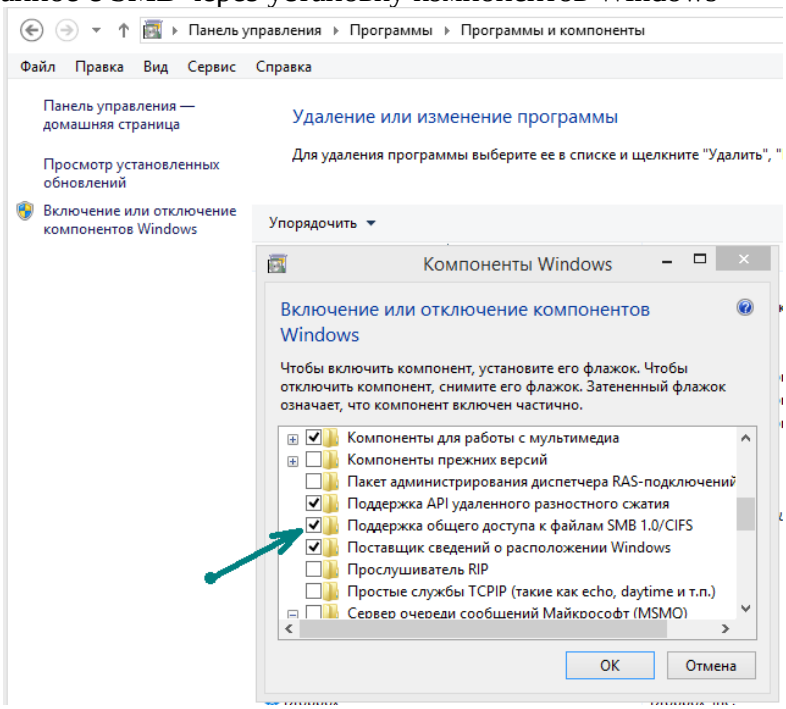
http://support.microsoft.com/?kbid=4012212 P2 Security Update KB4012212 NT AUTHORITY\система 3/18/2017

- Если же ответ вернет вам пустую строку, попробуйте проверить следующий патч из списка

3. Отключить уязвимый протокол. Внимание! Скорее всего перестанут работать сетевые папки и прекратиться доступ по сети к принтерам и т. п.

```
Команды могут быть различными в зависимости от версии Windows. Например так
dism /online /norestart /disable-feature /featurename:SMB1Protocol
```

Или отключить все связанное с SMB через установку компонентов Windows



Источники:

https://geektimes.ru/post/289115/

https://geektimes.ru/post/289153/

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx