Семь правил безопасной работы на персональном компьютере

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

УГРОЗЫ, КОТОРЫЕ ПОДСТЕРЕГАЮТ НАС

- Уязвимости нулевого дня в программном обеспечении
- Ошибки конфигурации программного и аппаратного обеспечения
- Социальная инженерия (манипулирование)
- Фишинг (обман)
- Атаки на «цепочку поставщиков»

IT КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

КАК ЭТО МОЖЕТ ВОЗДЕЙСТВОВАТЬ НА НАС

- Взлом рабочего компьютера
- Взлом домашнего компьютера
- Взлом мобильного устройства
- Взлом прочих устройств (маршрутизатор, телевизор, умная колонка, холодильник и т.д.)

КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

ЗАЩИТА: ТЕОРИЯ И ПРАКТИКА

- Здравый смысл и параноидальный подход
- Настройка компьютера и мобильного устройства
- Сети с нулевым доверием, виртуализация, групповые политики
- Терминальные серверы и фермы, VDI (инфраструктура виртуальных рабочих столов)
- Тонкие клиенты
- Системы мониторинга: SIEM,IDS, IPS

IT КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

СЕМЬ ПРАВИЛ БЕЗОПАСНОЙ РАБОТЫ

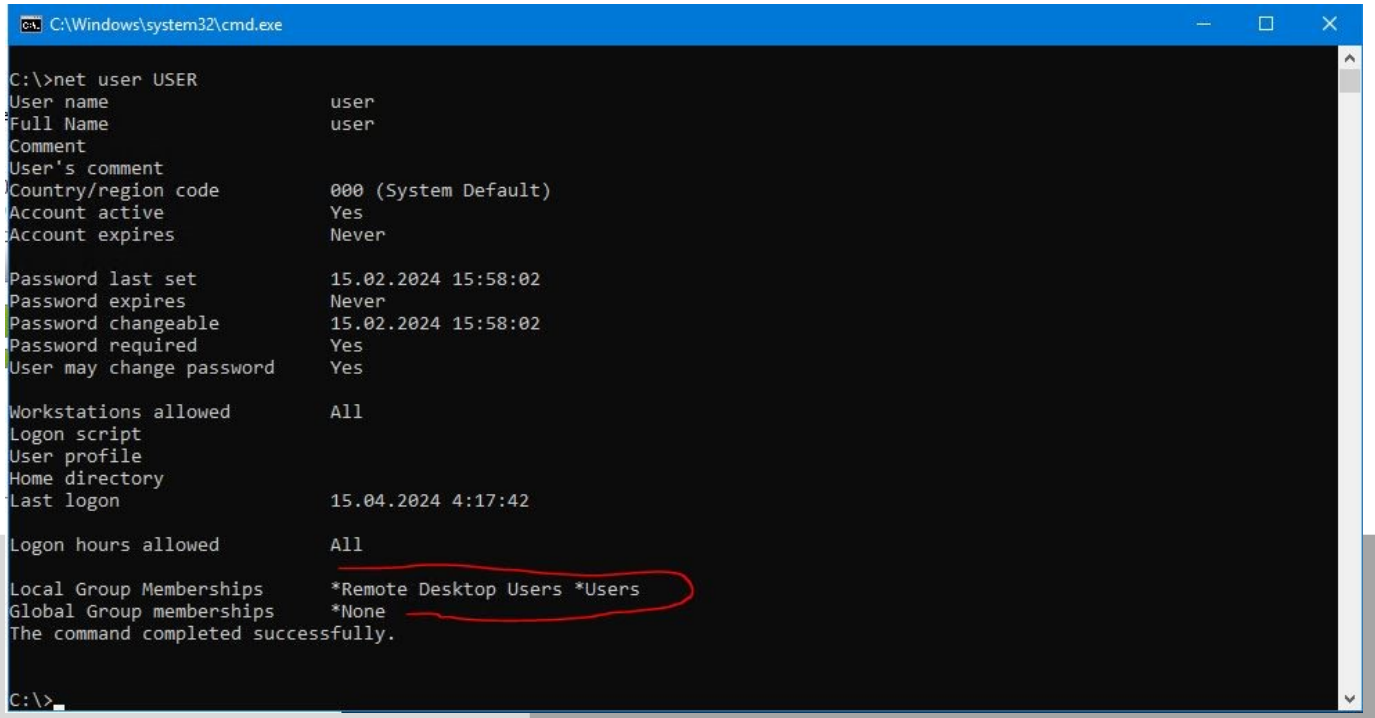
1. Работа без прав администратора
2. Политика ограниченного использования программ
3. Отключение неиспользуемых служб
4. Обновления
5. Резервное копирование
6. Брандмауэр
7. Антивирус

КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Работа без прав администратора

Как проверить:

- Командой net user %USERNAME%, где %USERNAME%=логин пользователя

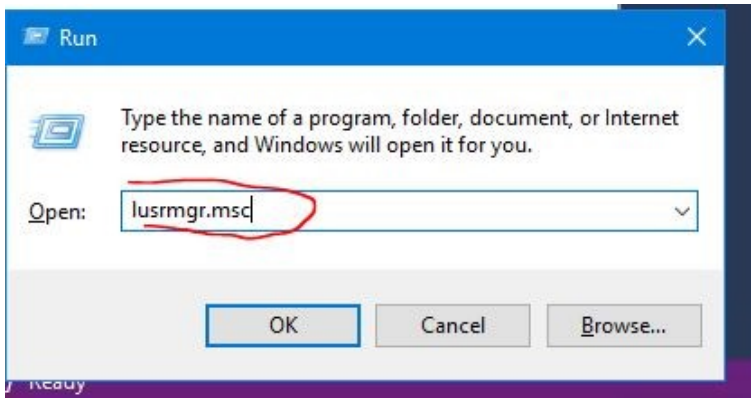


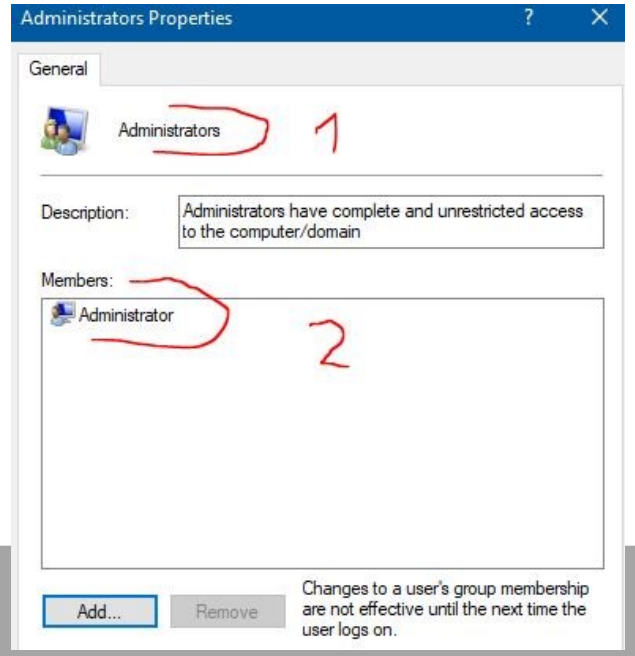
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Работа без прав администратора

Как проверить:

- Графический интерфейс, Пуск → Выполнить → **lusrmgr.msc**





КОНСУЛЬТАНТ

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Политика ограниченного использования программ Software Restriction Policy (SRP)

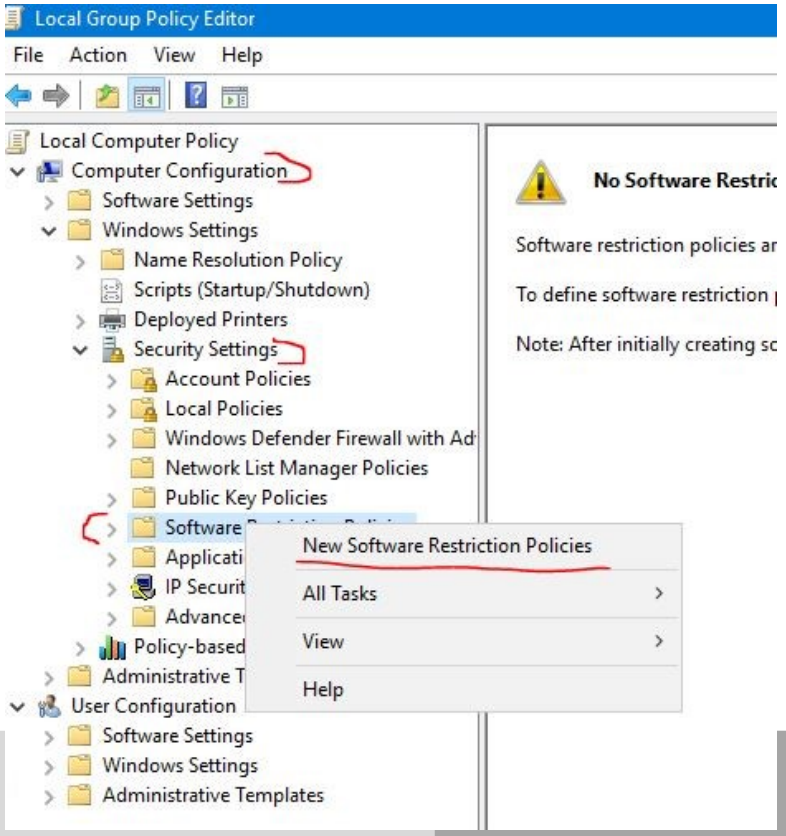
Как работает:

- Запрещено запускать все программы, кроме разрешённых

Как включается:

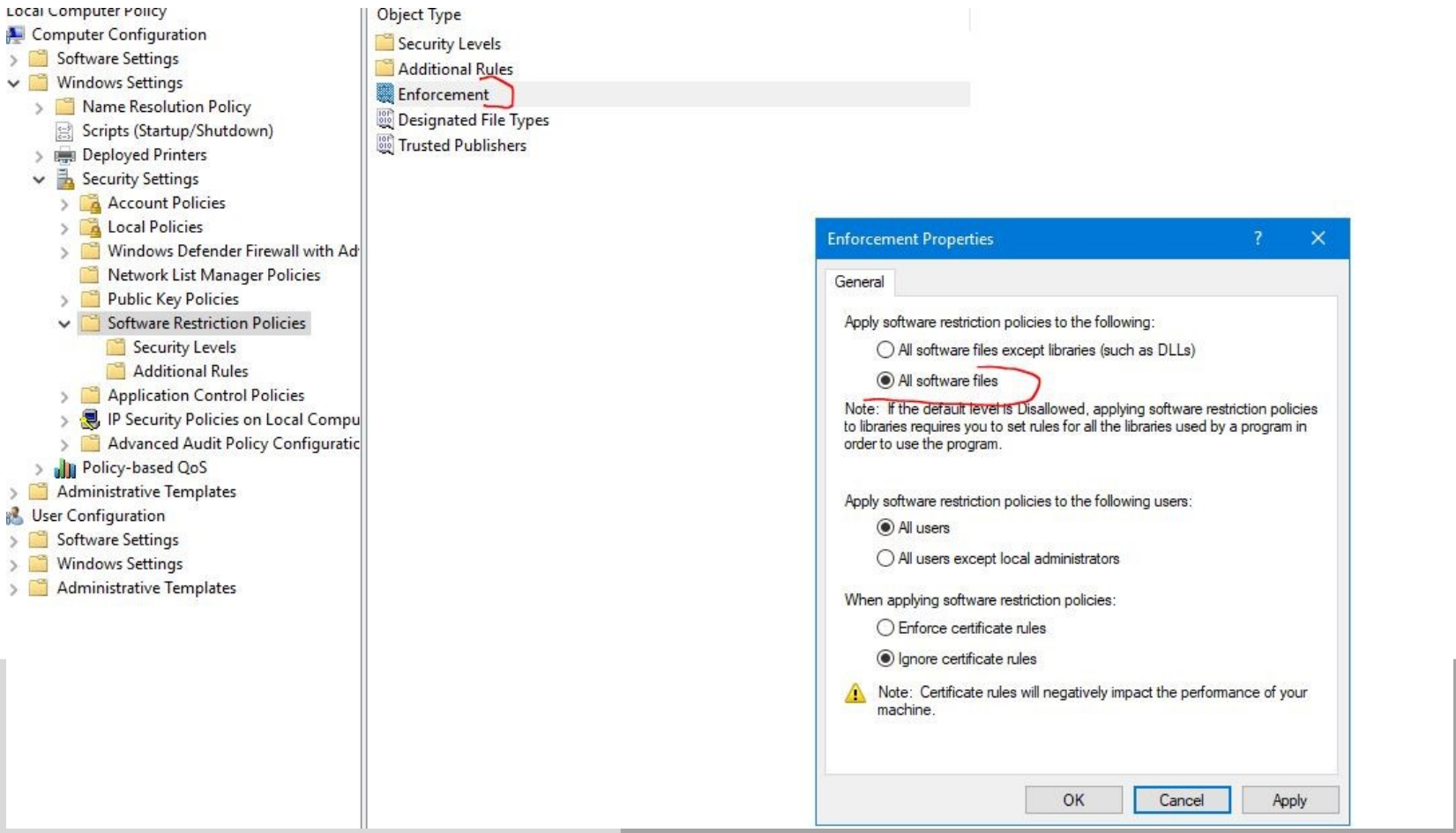
- Пуск → Выполнить → **gpedit.msc**

Software Restriction Policy (SRP)



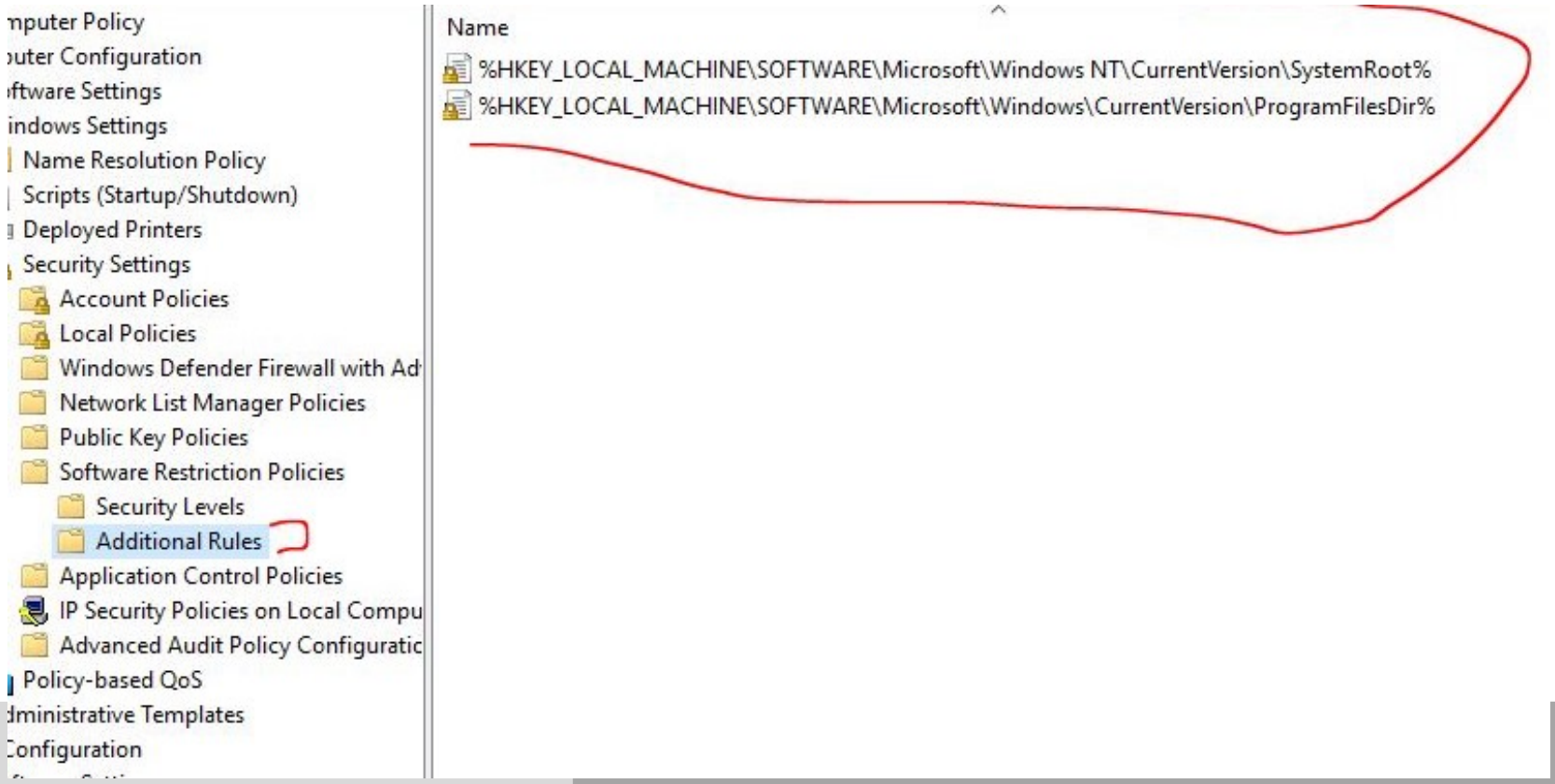
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Software Restriction Policy (SRP)



+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Software Restriction Policy (SRP)



+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Software Restriction Policy (SRP)

Пример разрешающих правил SRP:

- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)%*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramW6432Dir%*

Software Restriction Policy (SRP)

Пример запрещающих правил SRP:

- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\DefaultSpoolDirectory*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%Temp*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%Tracing*
- *%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%Tasks*
- *C:\Windows\System32\Microsoft\Crypto\RSA\MachineKeys*

Software Restriction Policy (SRP)

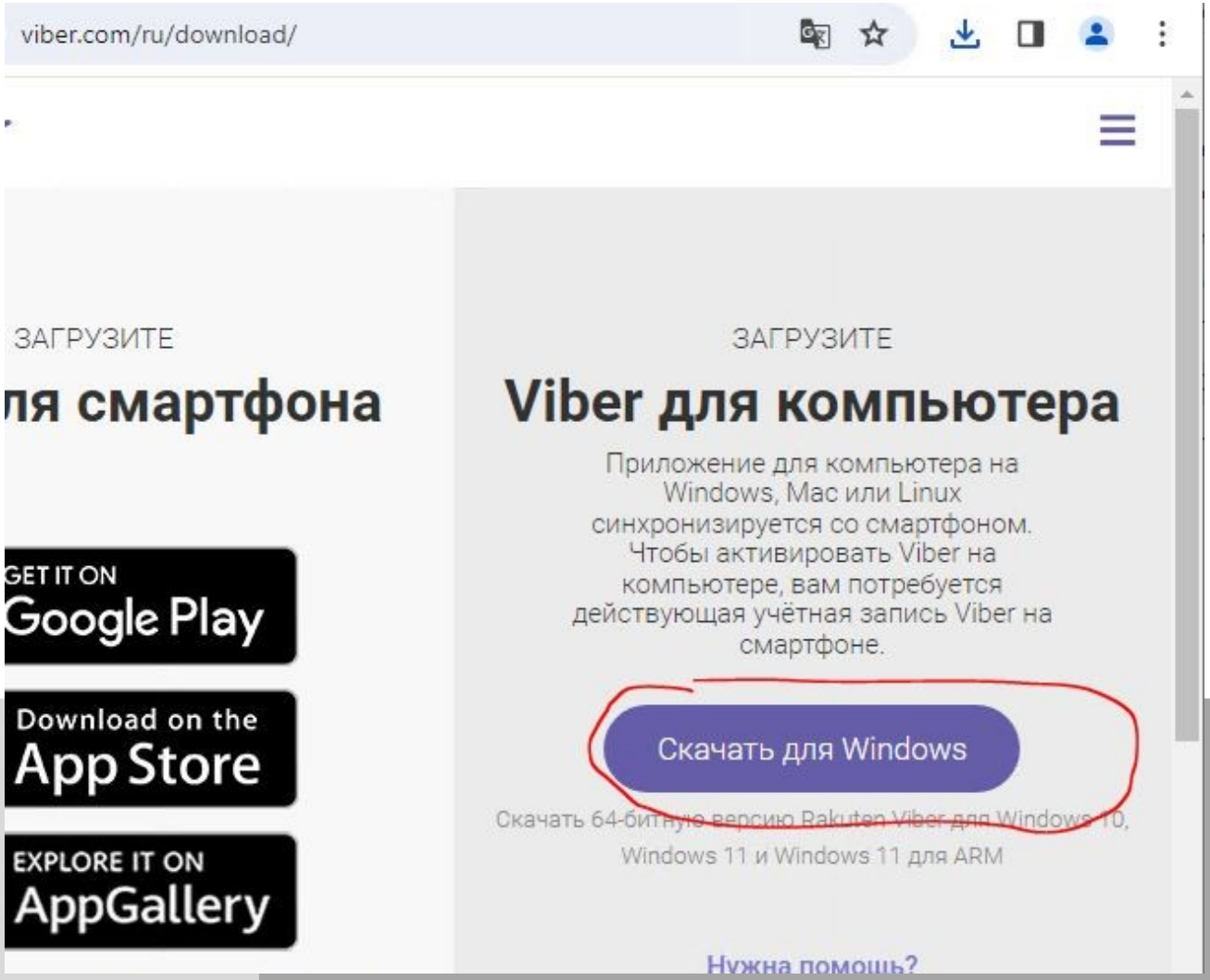
Пример дополнительных запрещающих правил SRP:

- bcdedit.exe
- cipher.exe
- cscript.exe
- wscript.exe
- vssadmin.exe
- hh.exe
- powershe*.exe
- mshta.exe
- wmic.exe

Software Restriction Policy (SRP)

Как это выглядит на практике:

- Скачиваем
- Запускаем
- Блокируем



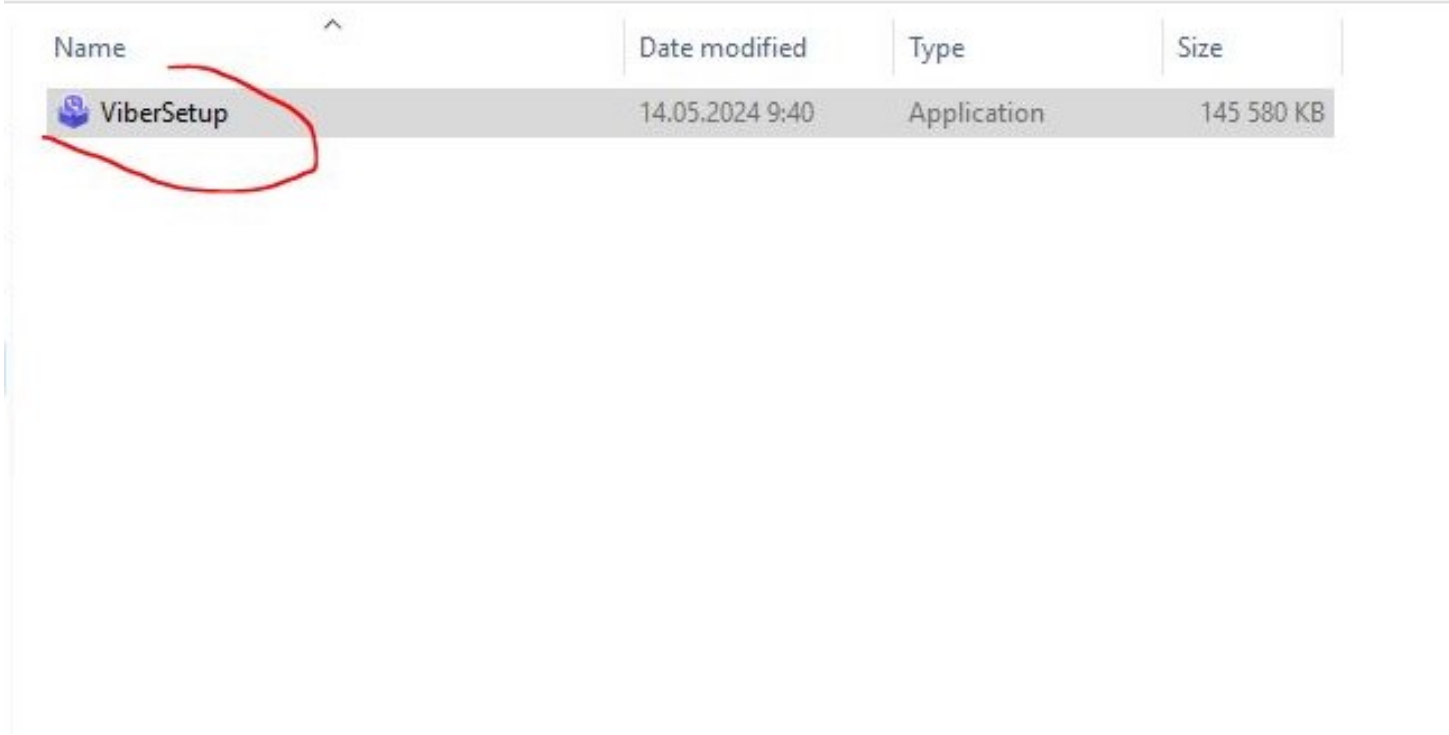
КОНСУЛЬТАНТ

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Software Restriction Policy (SRP)

Как это выглядит на практике:

- Скачиваем
- Запускаем
- Блокируем

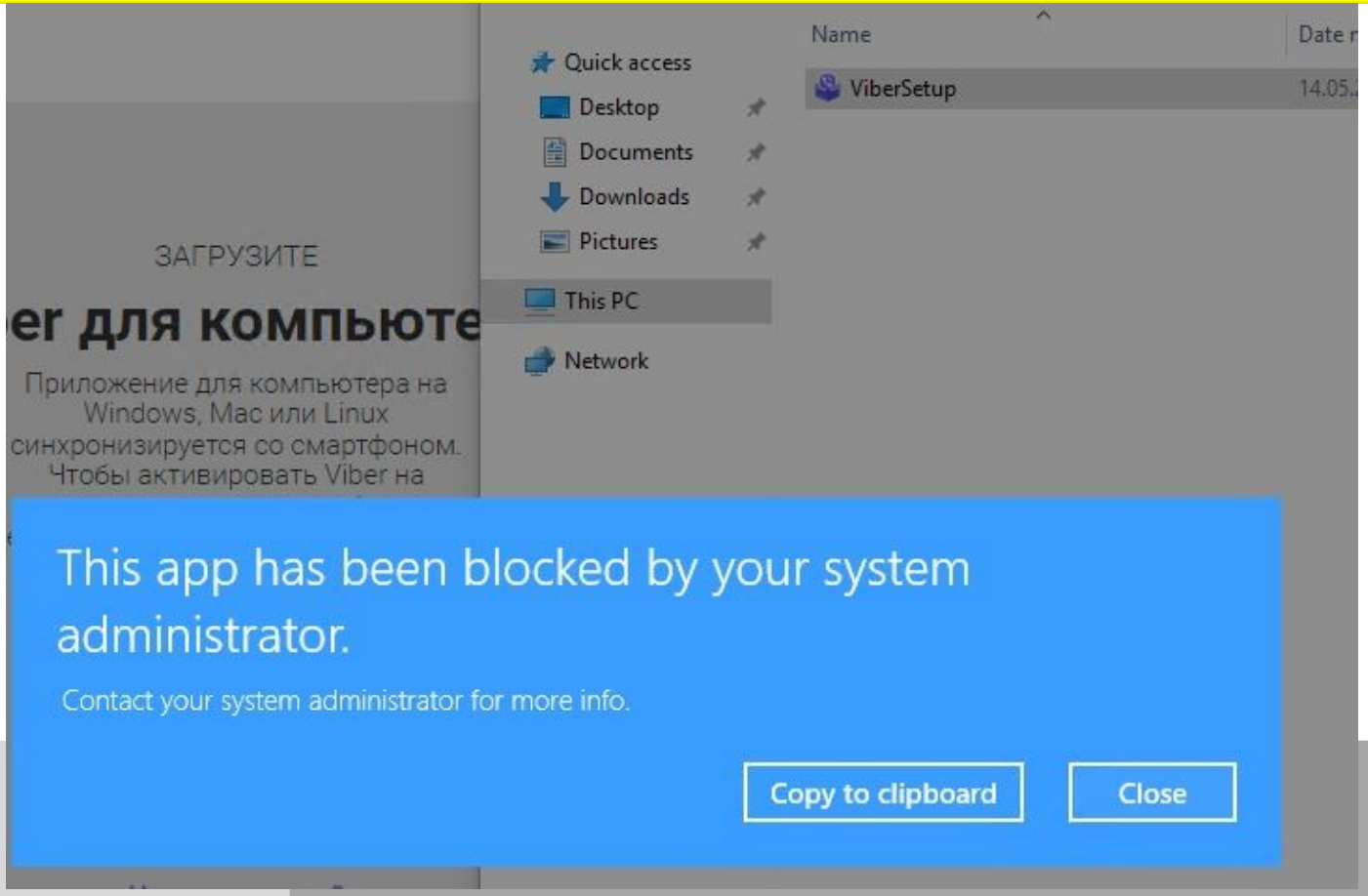


+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Software Restriction Policy (SRP)

Как это выглядит на практике:

- Скачиваем
- Запускаем
- Блокируем

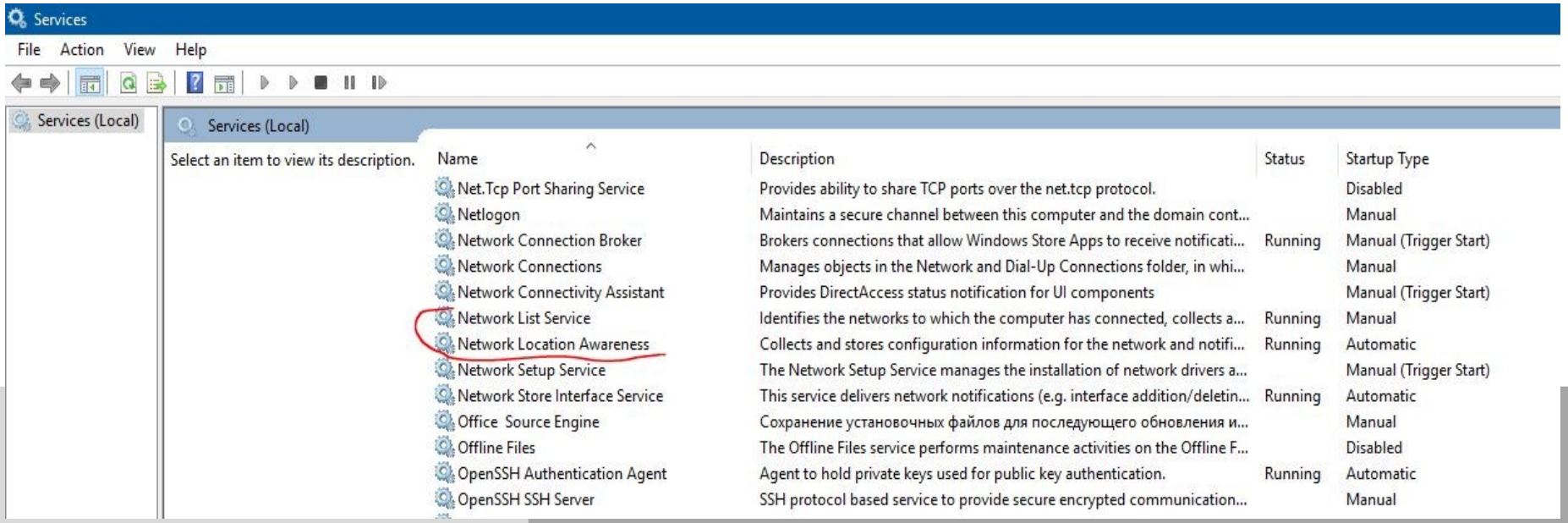


+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Отключение неиспользуемых служб

Как проверить:

- Графический интерфейс, Пуск → Выполнить → **services.msc**

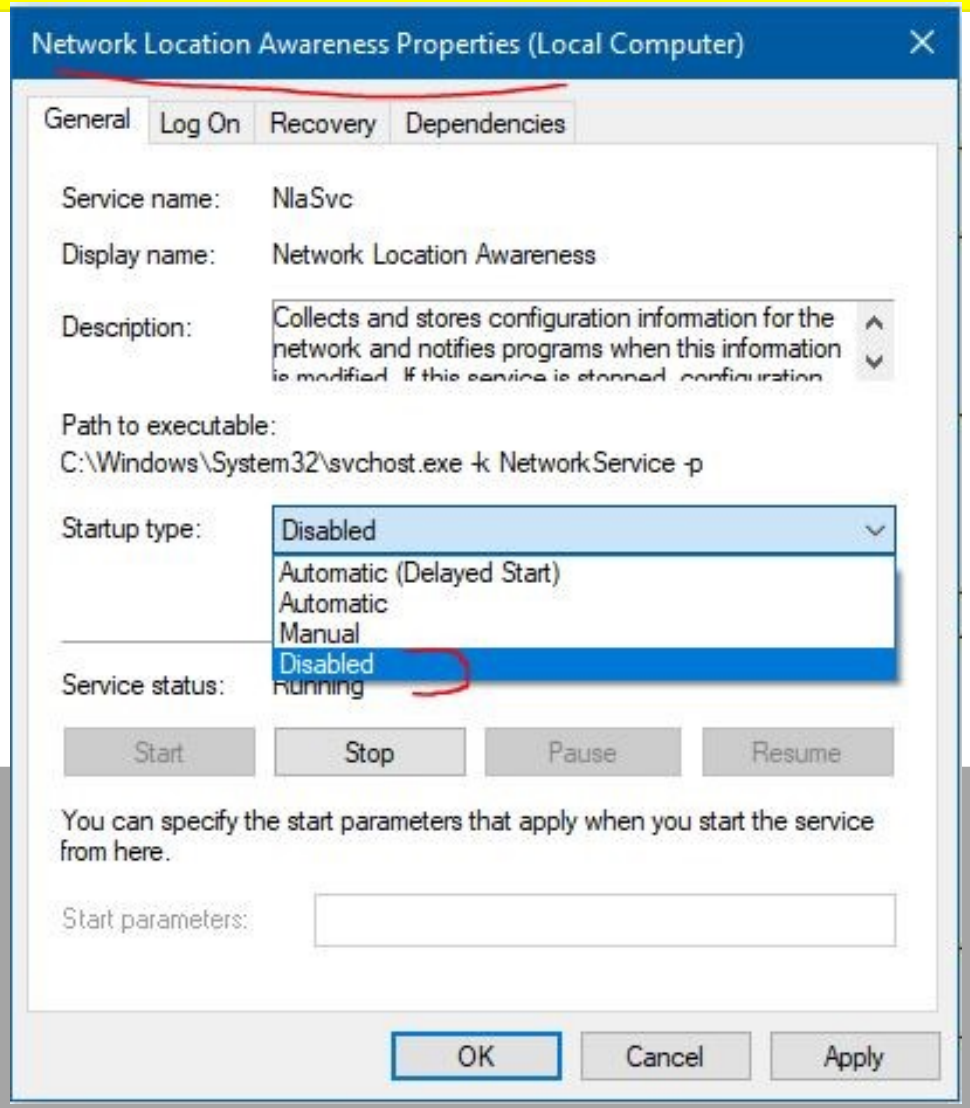


+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Отключение неиспользуемых служб

Отключаем службу NLA:

- Двойной щелчок на службе → Тип запуска → Отключено (Disable)



+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Обязательная установка обновлений

Включаем автоматическую установку обновлений:

1. Пуск → Обновление
2. Пуск → Выполнить → C:\Windows\System32\control.exe /name Microsoft.WindowsUpdate

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Резервное копирование

Программное обеспечение для резервного копирования:

1. Программное обеспечение встроенное в Windows
2. Внешнее программное обеспечение, например Veeam Backup

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Брандмауэр

Что такое брандмауэр он же файрволл?

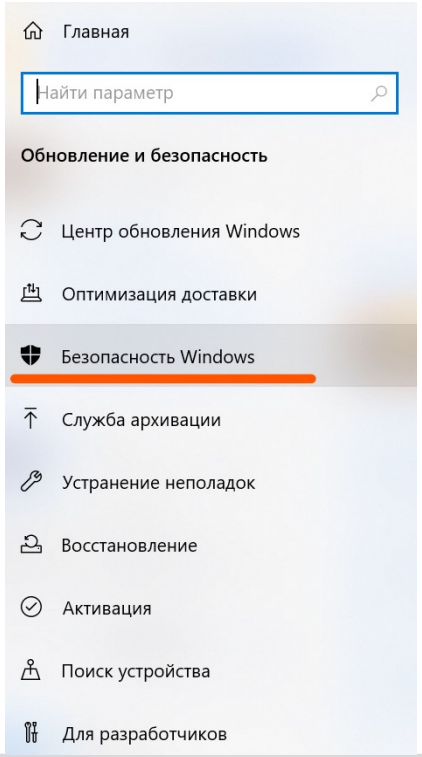
Это **щит** между вашим компьютером и любым другим устройством.

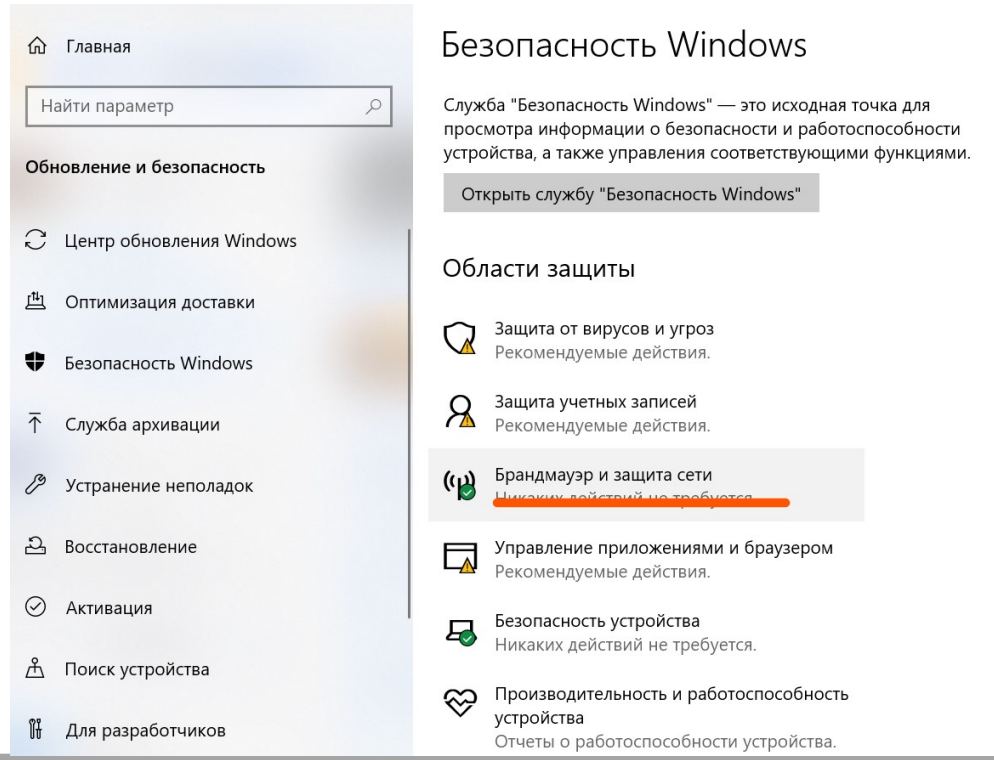
ВАЖНО!

Брандмауэр, обычно, ограничивает подключения других устройств к вашему компьютеру и не ограничивает подключения от вашего компьютера к другим устройствам.

КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

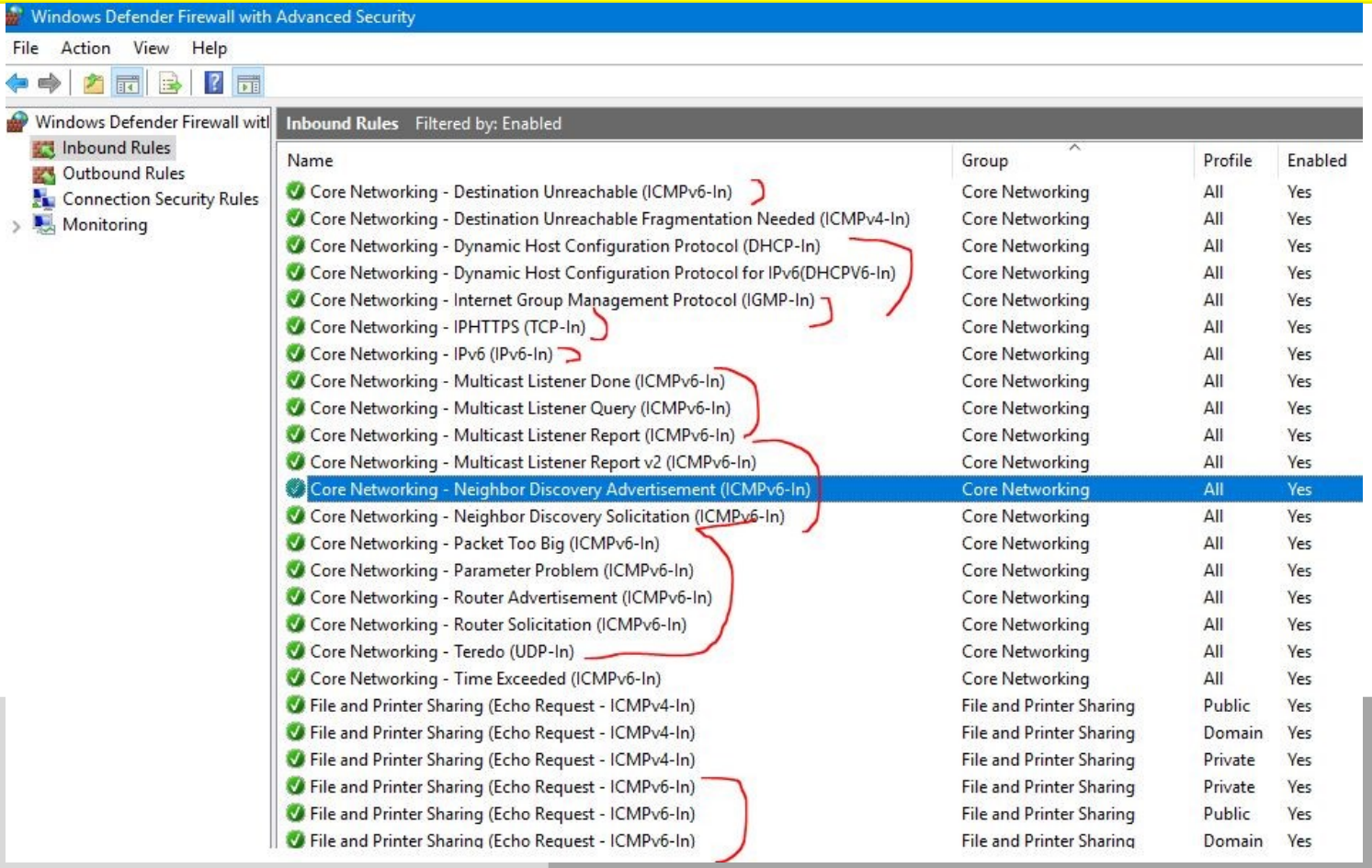
Брандмауэр





+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Брандмауэр



IT КОНСУЛЬТАНТ

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Антивирус не панацея

Если у меня стоит антивирус, я полностью защищен от вирусов?

— Алексей Лукацкий

бизнес-консультант по информационной безопасности Positive Technologies

вопрос эксперту

Если у меня стоит антивирус, я полностью защищен от вирусов?

Если у вас стоит антивирус, то вы не защищены ни от чего. **Существует множество сервисов, которые позволяют проверить вредоносный код** на недетектируемость популярными антивирусами и средствами защиты конечных устройств.

Если у меня стоит антивирус, я полностью защищен от вирусов?

Соответственно, полагаться на антивирус я бы не стал, и именно поэтому в базовых рекомендациях по ИБ для рядовых пользователей и корпораций **установка антивируса не входит даже в десятку защитных мер.**

IT КОНСУЛЬТАНТ

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

СЮРПРИЗ!

Первые 10 человек, которые пришлют заявку на электронную почту **support@itadvisor.ru**, получат возможность бесплатно сделать аудит соответствия настроек **домашнего компьютера** семи правилам безопасной работы на персональном компьютере. Подтверждение, а также организационные моменты «как и каким образом» —напишем на вашу электронную почту.

Первым ДЕСЯТИ записавшимся бесплатный аудит безопасности.

КОНСУЛЬТАНТ
+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru

Ссылки в Telegram

Канал «Проект "Терминальная сеть"»

https://t. me/pts_itadvisor

Группа «Проект "Терминальная сеть"»

https://t. me/+j3PErS9wuVgzMDZi

+7-910-7432838
nvi@itadvisor.ru
https://www.itadvisor.ru