

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»



+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.)



+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



+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



Работа без прав администратора

Как проверить:

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

```
C:\Windows\system32\cmd.exe
C:\>net user USER
User name                user
Full Name                user
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        15.02.2024 15:58:02
Password expires         Never
Password changeable      15.02.2024 15:58:02
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon                15.04.2024 4:17:42

Logon hours allowed      All

Local Group Memberships  *Remote Desktop Users *Users
Global Group memberships *None
The command completed successfully.

C:\>
```



+7-910-7432838

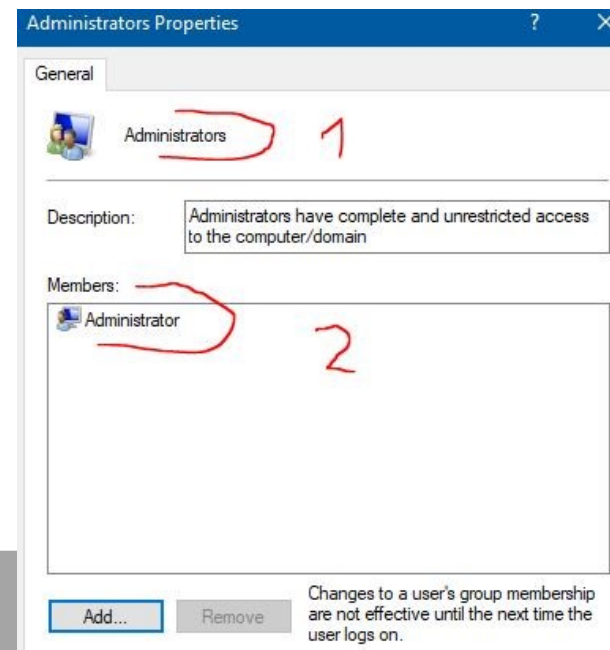
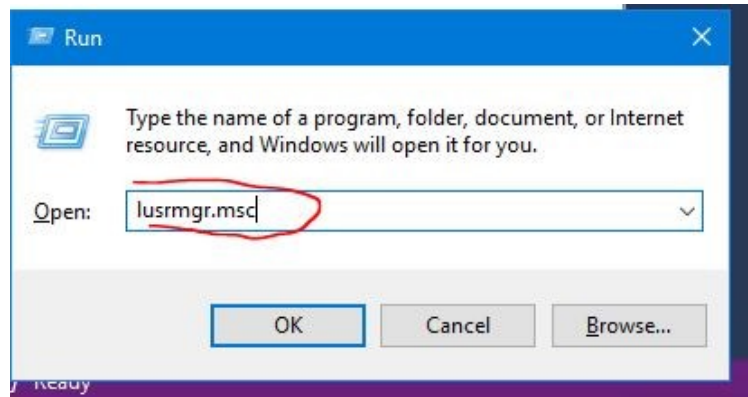
nvi@itadvisor.ru

<https://www.itadvisor.ru>

Работа без прав администратора

Как проверить:

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



Политика ограниченного использования программ Software Restriction Policy (SRP)

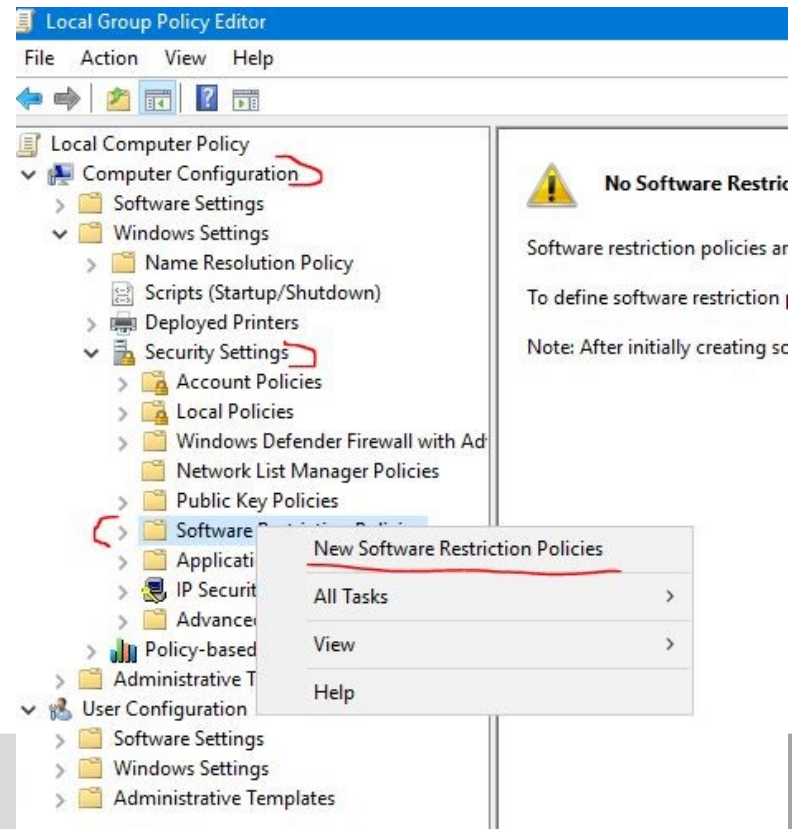
Как работает:

- Запрещено запускать все программы, кроме разрешённых

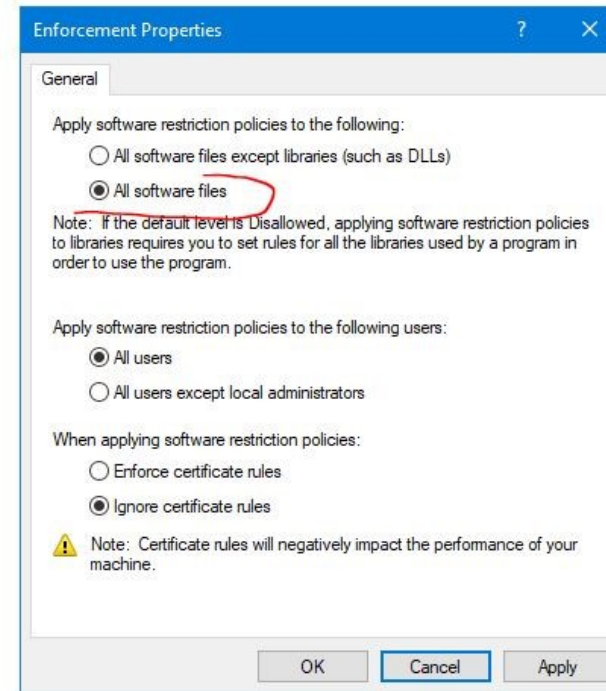
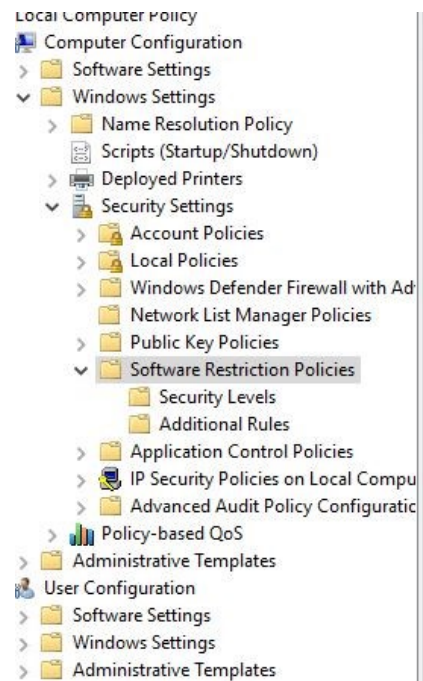
Как включается:

- Пуск → Выполнить → **gpedit.msc**

Software Restriction Policy (SRP)



Software Restriction Policy (SRP)



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

КОНСУЛЬТАНТ

Software Restriction Policy (SRP)

The screenshot displays the Windows Group Policy Editor interface. The left-hand navigation pane shows the following tree structure:

- Computer Policy
- Computer Configuration
- Software Settings
- Windows Settings
- Name Resolution Policy
- Scripts (Startup/Shutdown)
- Deployed Printers
- Security Settings
 - Account Policies
 - Local Policies
 - Windows Defender Firewall with Ad
 - Network List Manager Policies
 - Public Key Policies
 - Software Restriction Policies
 - Security Levels
 - Additional Rules
 - Application Control Policies
 - IP Security Policies on Local Compu
 - Advanced Audit Policy Configuratic
- Policy-based QoS
- Administrative Templates
- Configuration

The right-hand pane shows the 'Name' column of the 'Additional Rules' list, containing two entries:

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

A red hand-drawn line highlights the two entries in the 'Name' column.



+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)

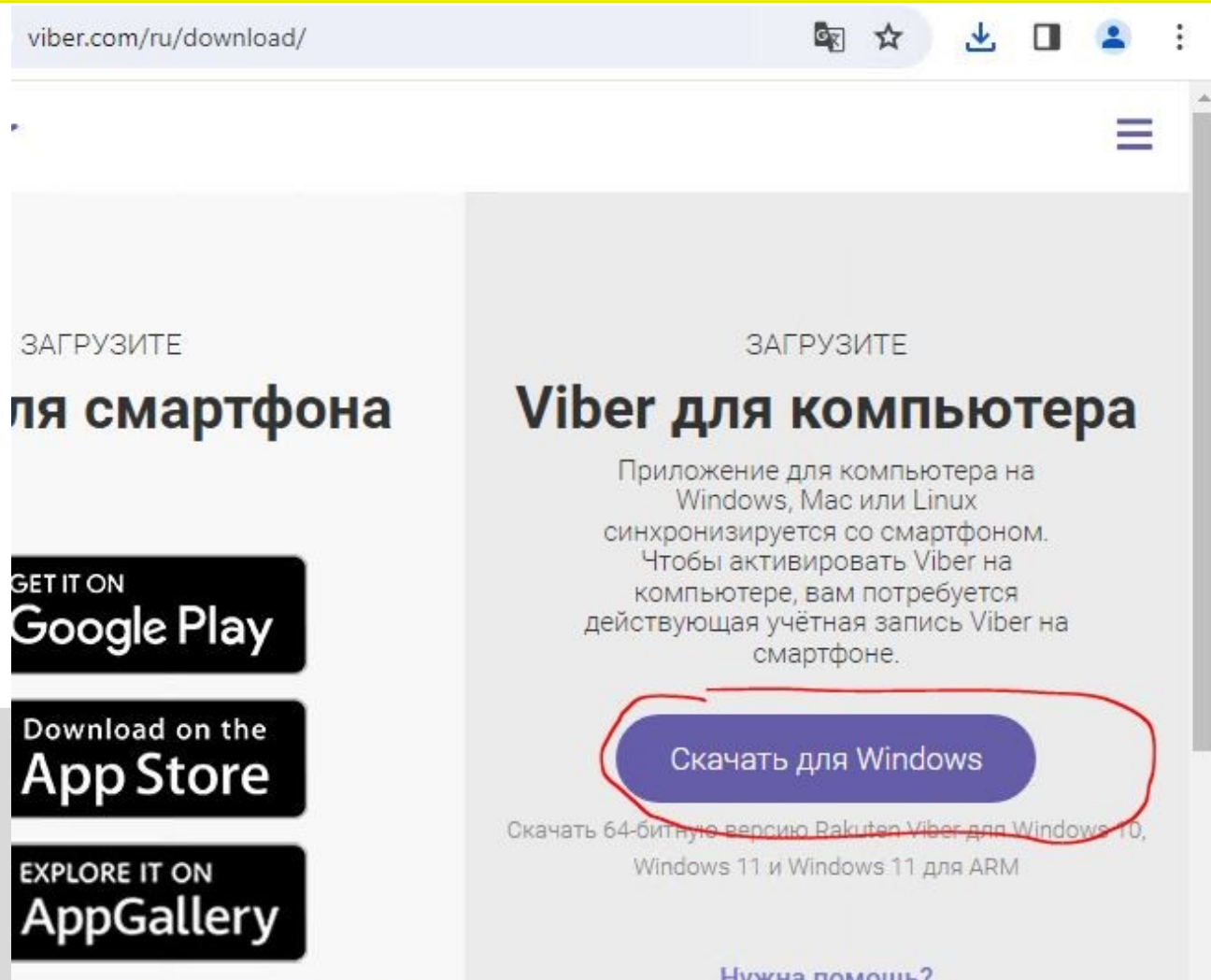
Пример дополнительных запрещающих правил SRP:

- 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



The screenshot shows the Viber website's download page for Windows. The browser address bar displays 'viber.com/ru/download/'. The page is split into two columns. The left column is for mobile devices, with the heading 'ЗАГРУЗИТЕ Viber для смартфона' and buttons for 'GET IT ON Google Play', 'Download on the App Store', and 'EXPLORE IT ON AppGallery'. The right column is for desktop computers, with the heading 'ЗАГРУЗИТЕ Viber для компьютера'. Below the heading, it states: 'Приложение для компьютера на Windows, Mac или Linux синхронизируется со смартфоном. Чтобы активировать Viber на компьютере, вам потребуется действующая учётная запись Viber на смартфоне.' A blue button labeled 'Скачать для Windows' is circled in red. Below the button, it says 'Скачать 64-битную версию Rakuten Viber для Windows 10, Windows 11 и Windows 11 для ARM'. At the bottom right, there is a link 'Нужна помощь?'.




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

Software Restriction Policy (SRP)

**Как это выглядит
на практике:**

- Скачиваем
- Запускаем
- Блокируем

Name	Date modified	Type	Size
 ViberSetup	14.05.2024 9:40	Application	145 580 KB

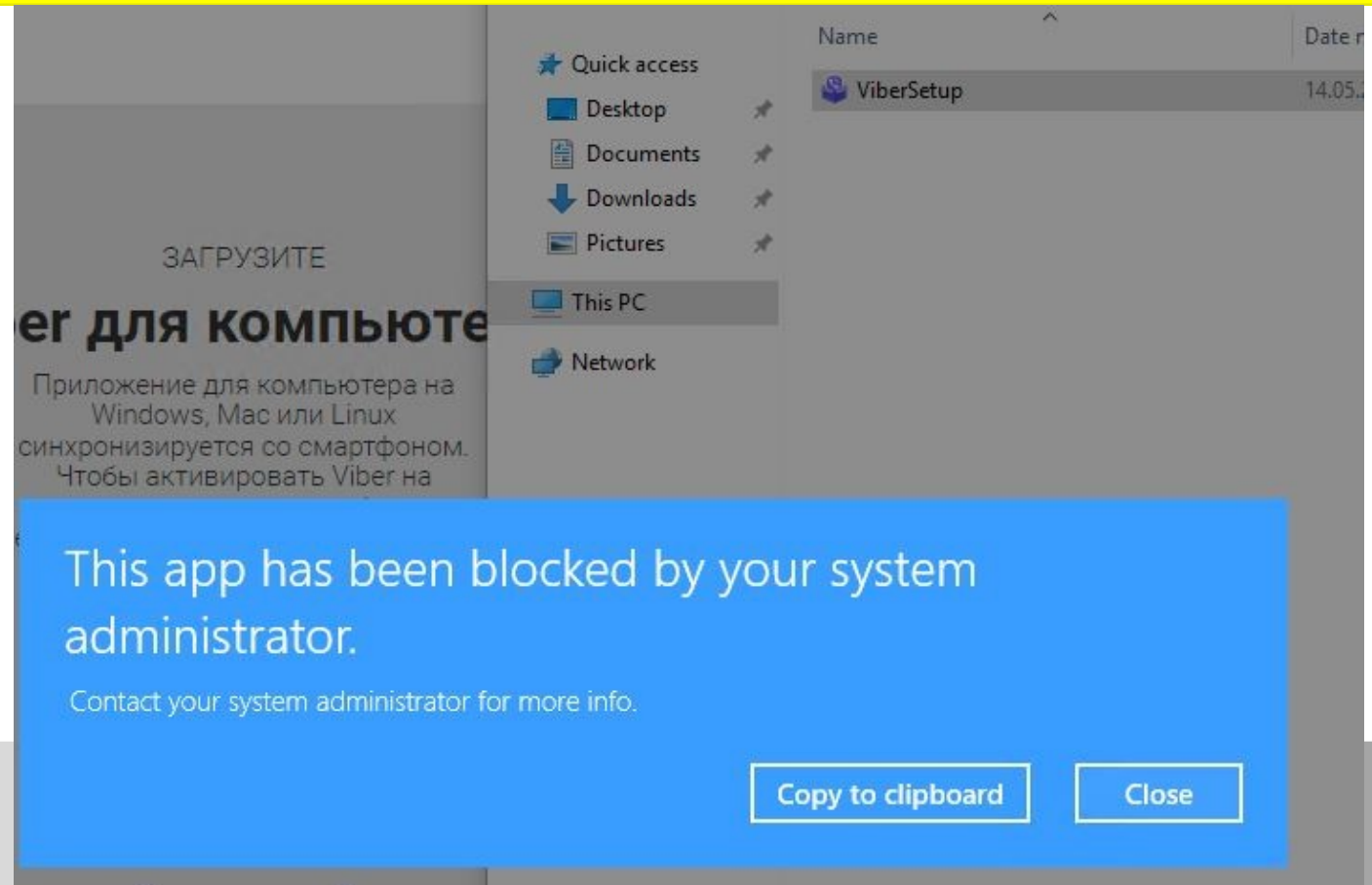


+7-910-7432838
nvi@itadvisor.ru
<https://www.itadvisor.ru>

Software Restriction Policy (SRP)

Как это выглядит на практике:

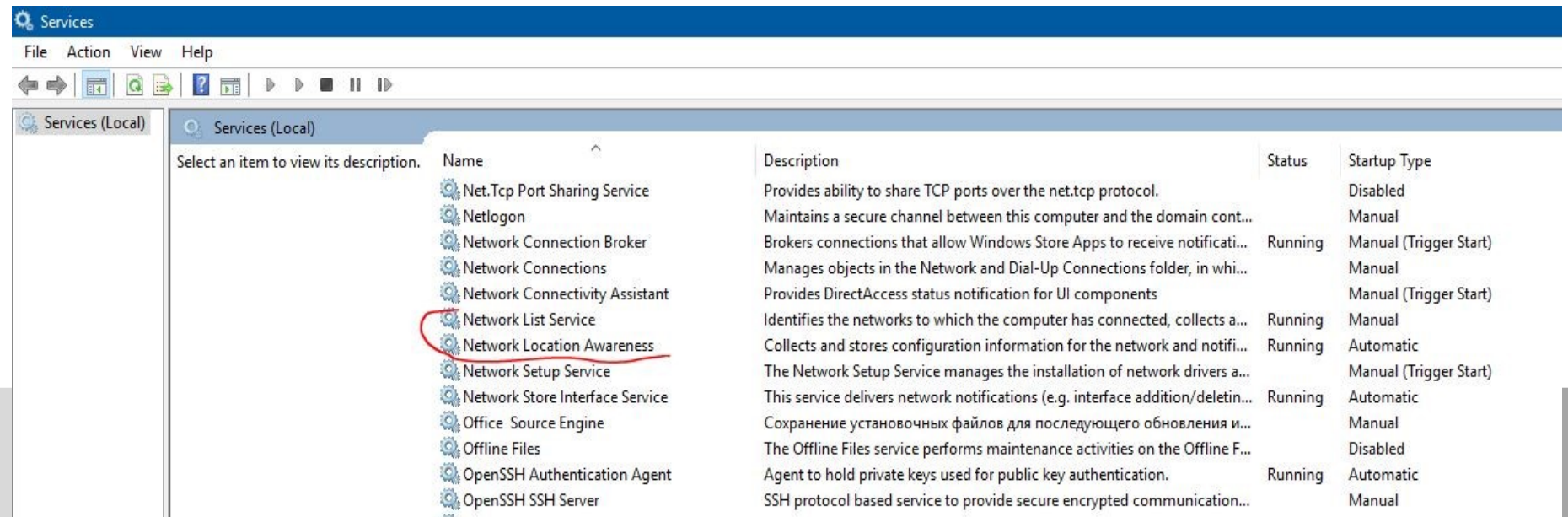
- Скачиваем
- Запускаем
- Блокируем



Отключение неиспользуемых служб

Как проверить:

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

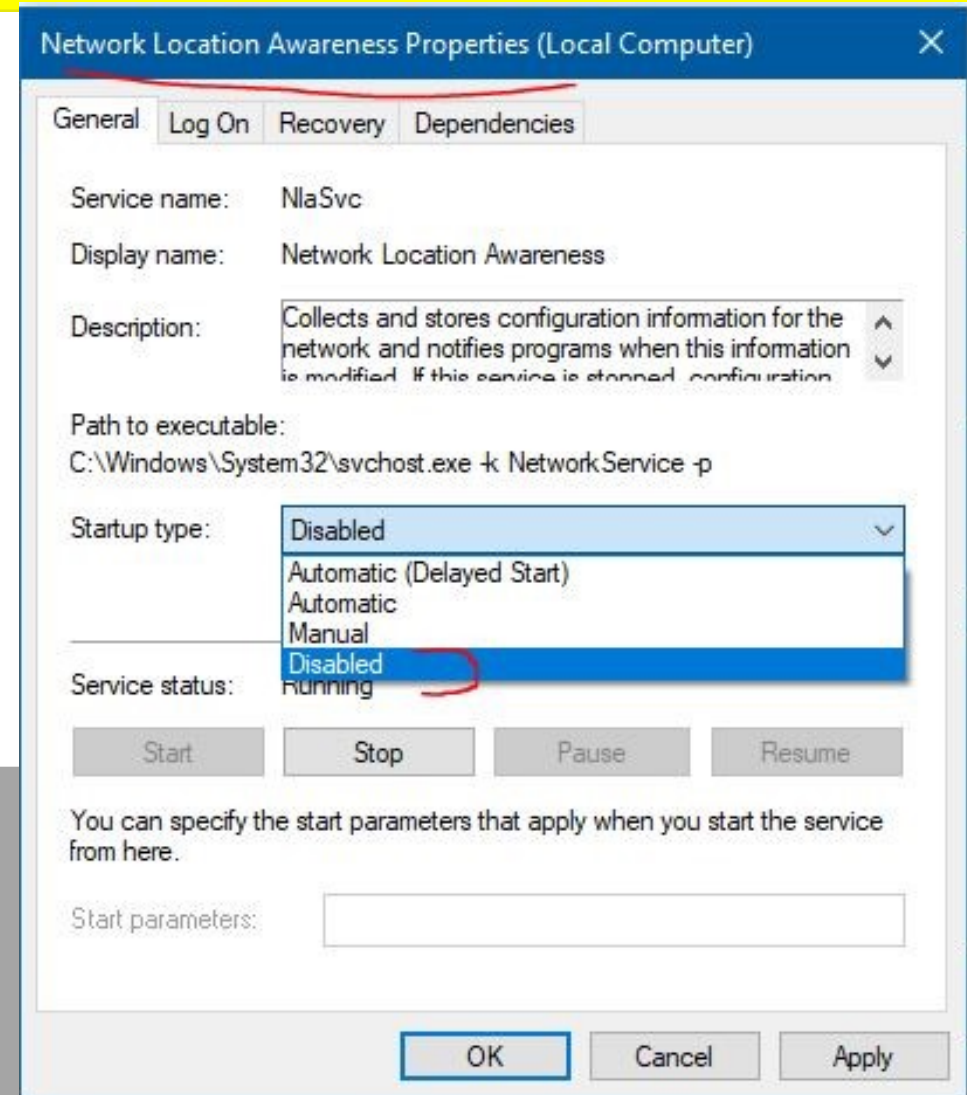


+7-910-7432838
nvi@itadvisor.ru
<https://www.itadvisor.ru>

Отключение неиспользуемых служб

Отключаем службу NLA:

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



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.

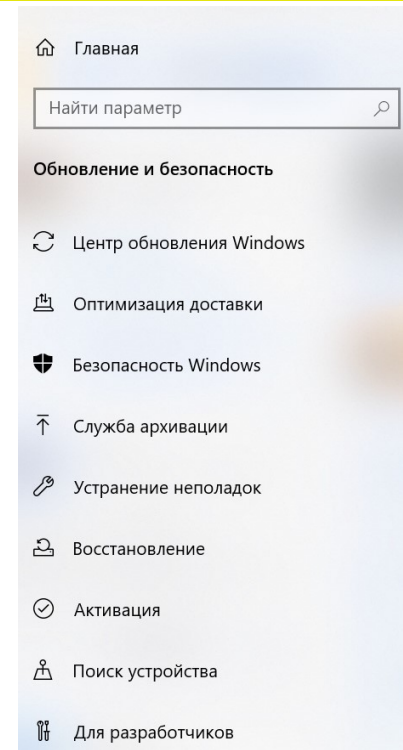
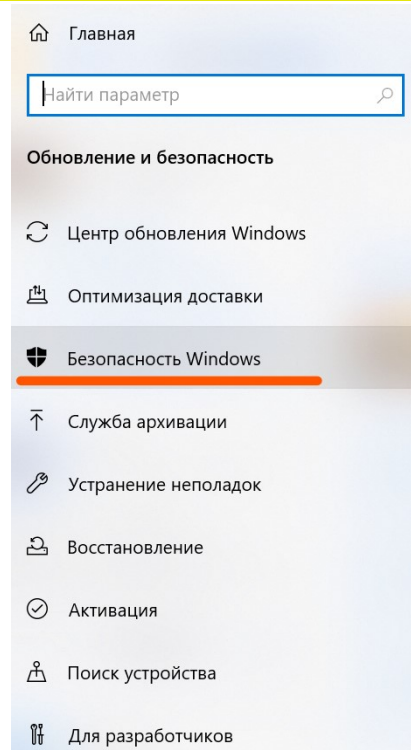


+7-910-7432838

nvi@itadvisor.ru

<https://www.itadvisor.ru>

Брандмауэр



Безопасность Windows

Служба "Безопасность Windows" — это исходная точка для просмотра информации о безопасности и работоспособности устройства, а также управления соответствующими функциями.

Открыть службу "Безопасность Windows"

Области защиты

Защита от вирусов и угроз
Рекомендуемые действия.

Защита учетных записей
Рекомендуемые действия.

Брандмауэр и защита сети
Никаких действий не требуется.

Управление приложениями и браузером
Рекомендуемые действия.

Безопасность устройства
Никаких действий не требуется.

Производительность и работоспособность устройства
Отчеты о работоспособности устройства.



+7-910-7432838

nvi@itadvisor.ru

<https://www.itadvisor.ru>

Брандмауэр

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Inbound Rules Filtered by: Enabled

Name	Group	Profile	Enabled
Core Networking - Destination Unreachable (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Protocol (DHCP-In)	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)	Core Networking	All	Yes
Core Networking - Internet Group Management Protocol (IGMP-In)	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Report v2 (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Public	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Public	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	Yes



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

КОНСУЛЬТАНТ

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



— Алексей Лукацкий

бизнес-консультант
по информационной
безопасности Positive
Technologies



вопрос эксперту

Антивирус не панацея

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.**



+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.



+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>