Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №3**

**Тема «Настройка Брандмауэра Windows»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 1 группы ФИТ

Немкович Анастасия Вадимовна

Минск 2023

**Цель**

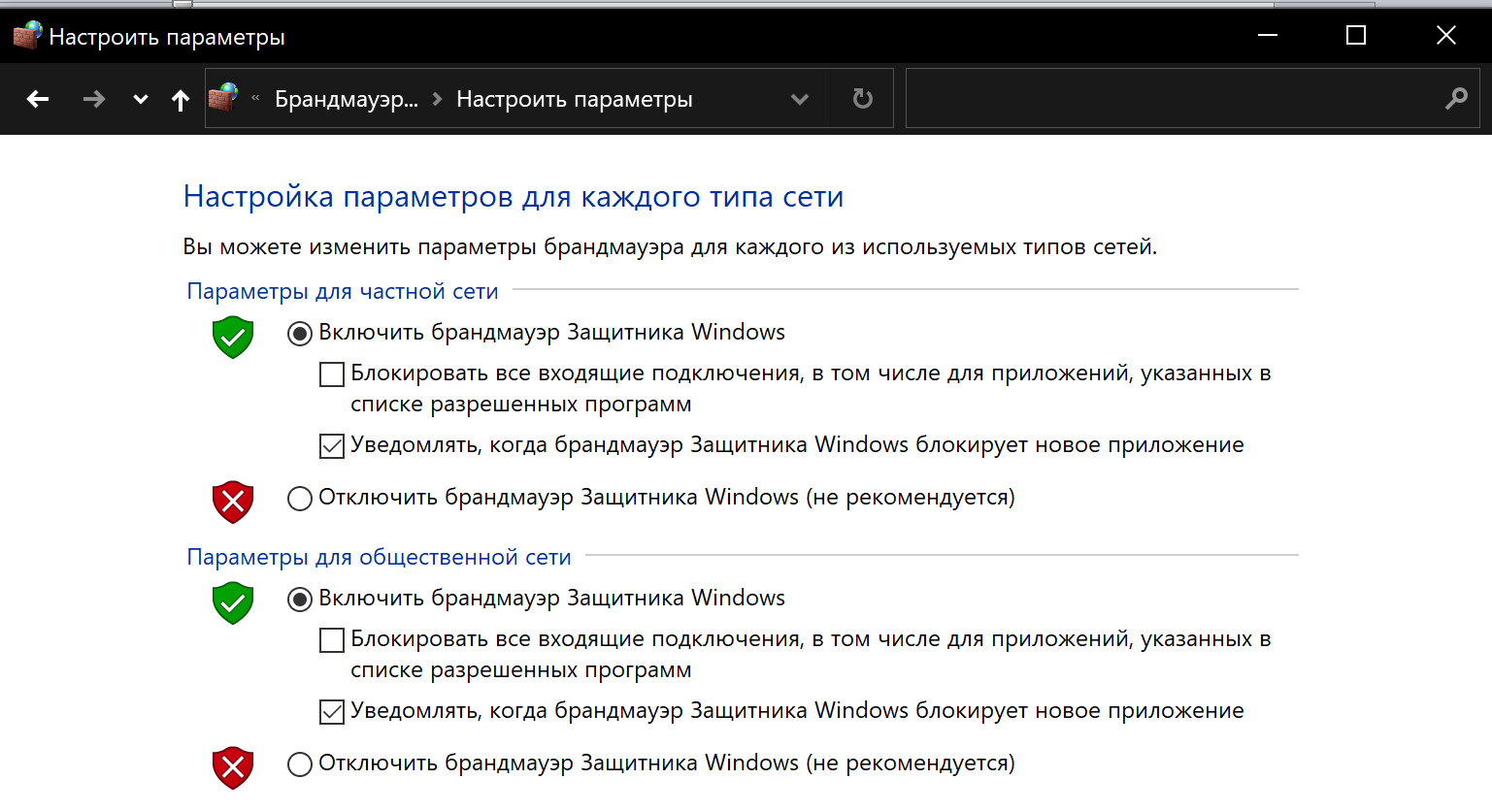
Овладеть навыками настройки и использования Брандмауэра Windows.

**Ход работы**

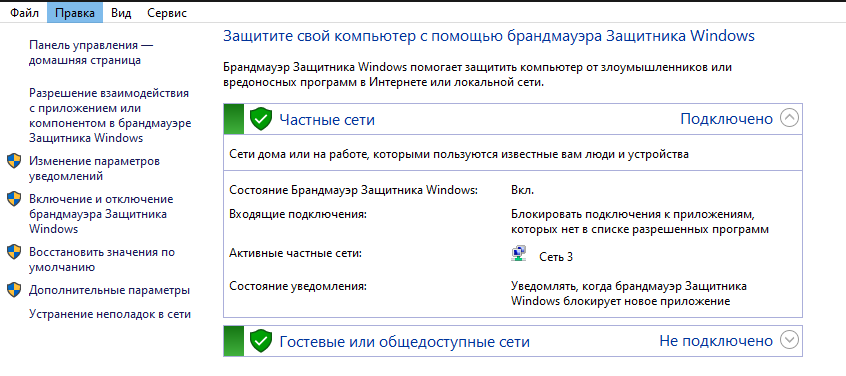
Брандмауэр – это защитный экран между глобальным интернетом и локальной компьютерной сетью организации. Он выполняет функцию проверки и фильтрации данных, поступающих из интернета. В зависимости от настроек брандмауэр может пропустить их или заблокировать (например, если обнаружит «червей», вирусы и хакерскую атаку).

Нужно различать сетевой брандмауэр (или, по-другому, сетевой экран) и брандмауэр, встроенный в операционную систему Windows. В первом случае решение устанавливается на границе (физической или логической) компьютерной инфраструктуры организации и защищает все ПК, подключенные к локальной сети – как программное, так и программно-аппаратное решение. Во втором случае это программа, работающая для защиты отдельно взятого компьютера пользователя.

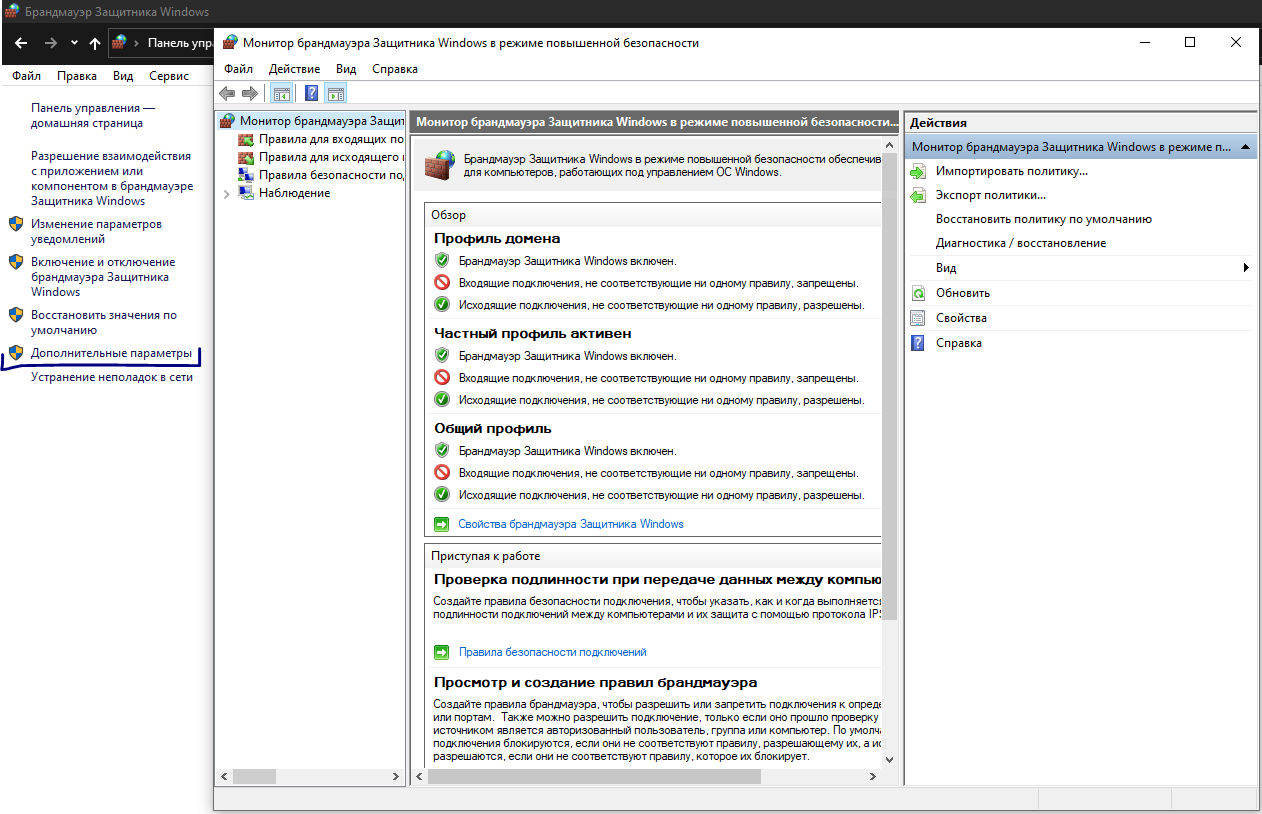
Для начала включим Брандмауэр Защитника Windows, перейдя в Панель управления и выбрав соответствующий пункт:



Включенный Брандмауэр выглядит следующим образом:

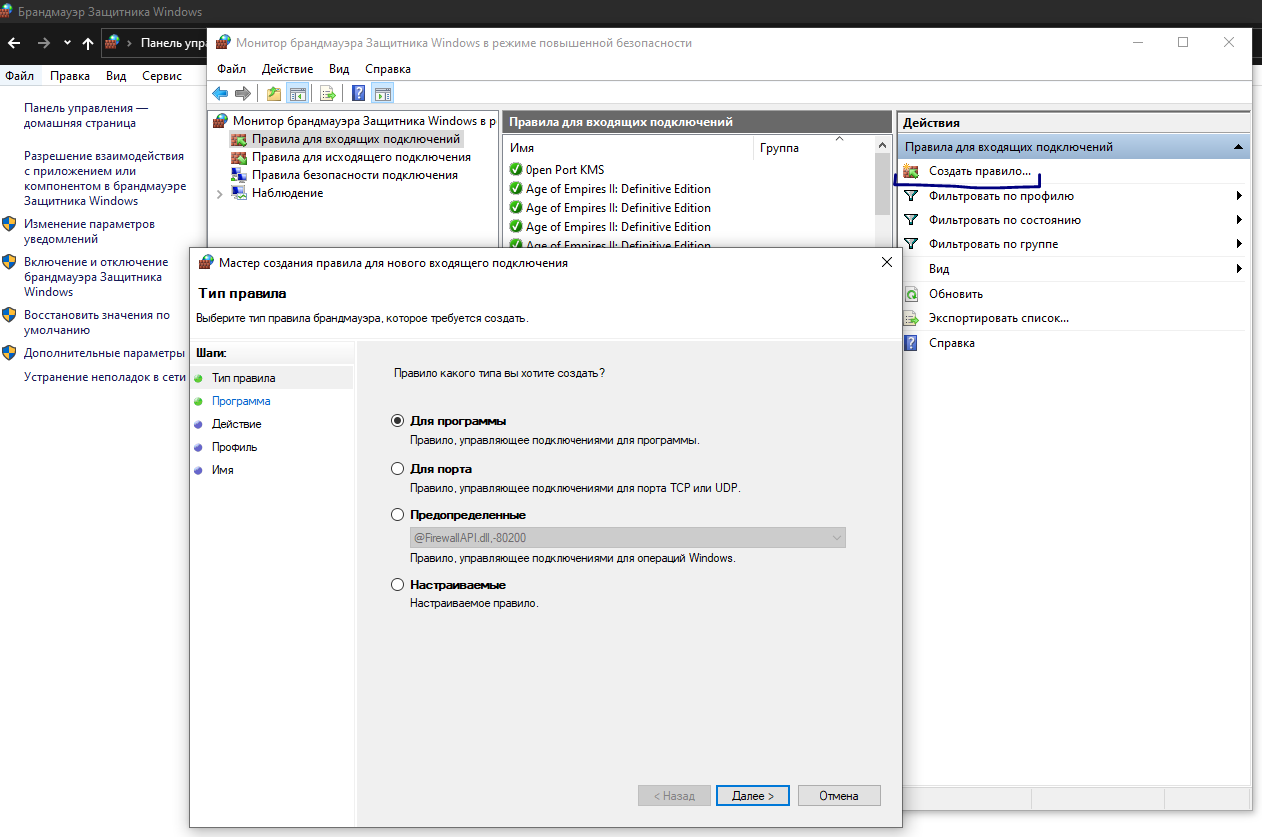


Перейдем во вкладку дополнительные параметры:

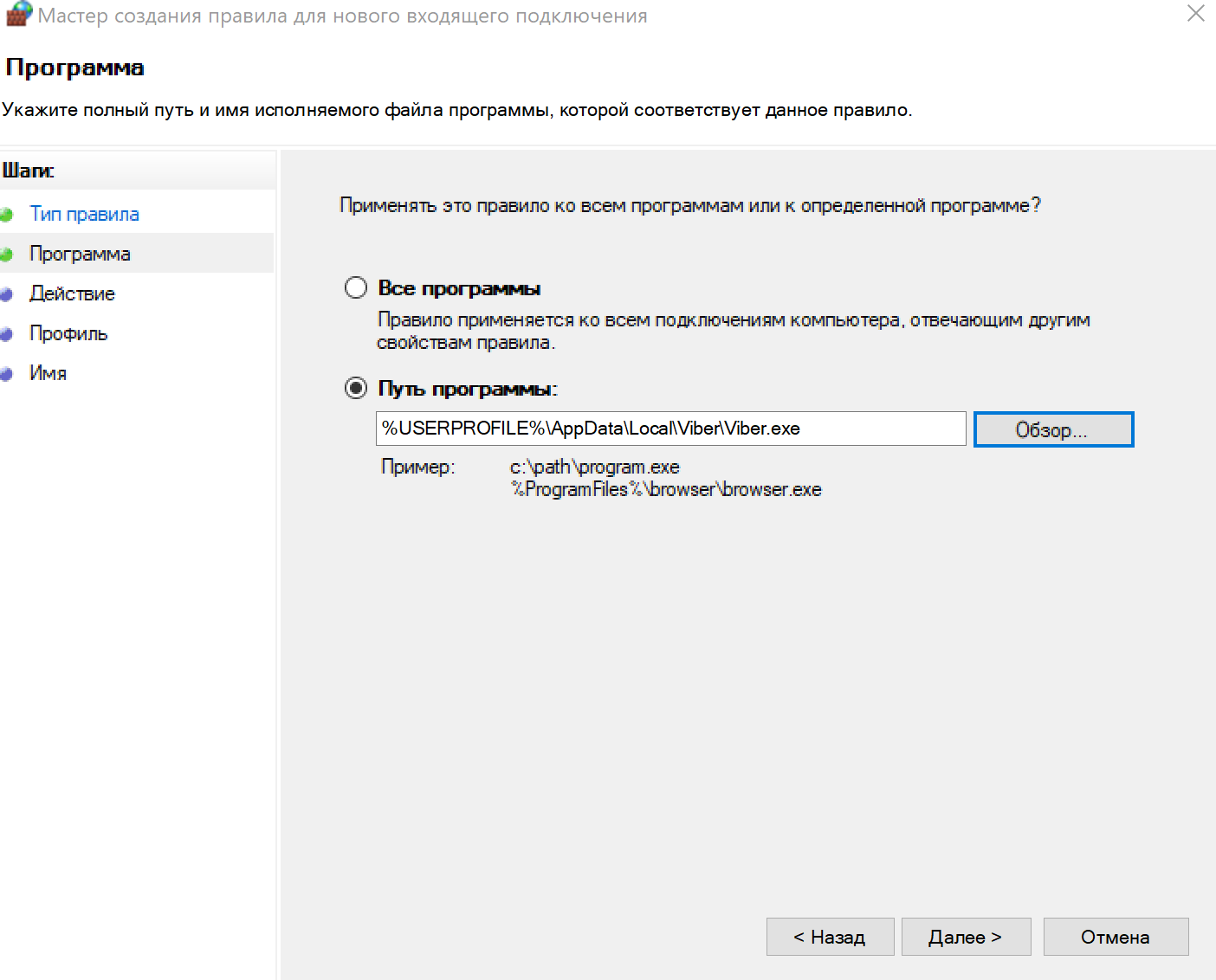


1. Создать правила для **входящих подключений** (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):
   1. Для 1 программы (по выбору) на **блокировку** подключения

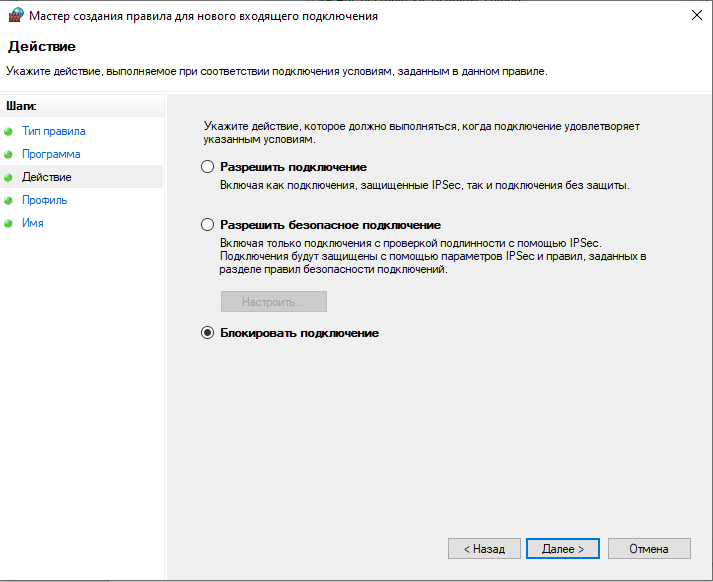
В левом меню выберем пункт «Правила для входящих подключений», в правом контекстном меню – пункт «Создать правило». В появившемся окне выбираем тип – «Для программы»:



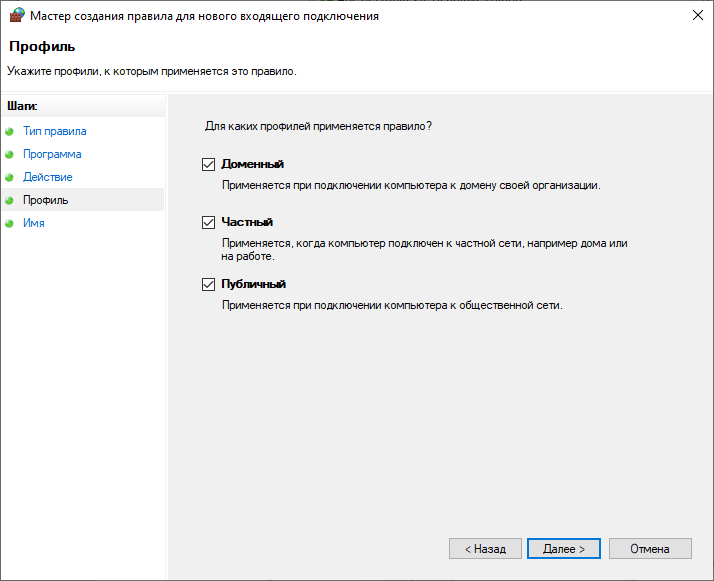
Указываем путь к программе:



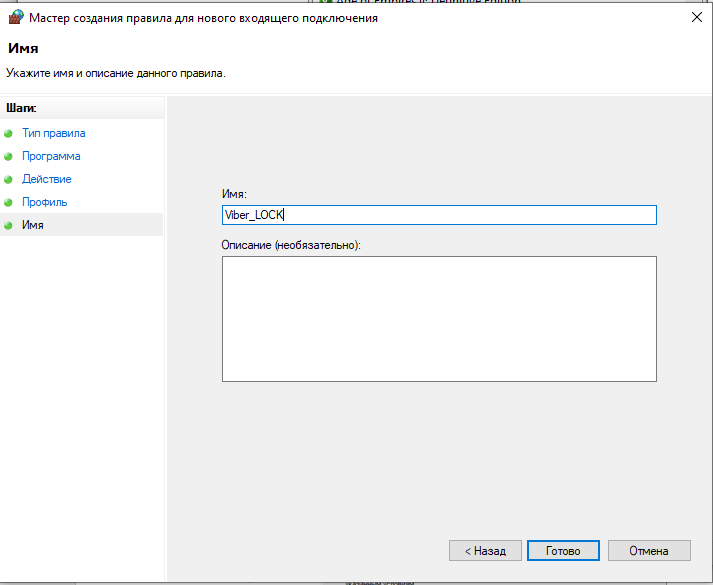
Выбираем действие «Блокировать подключение»:



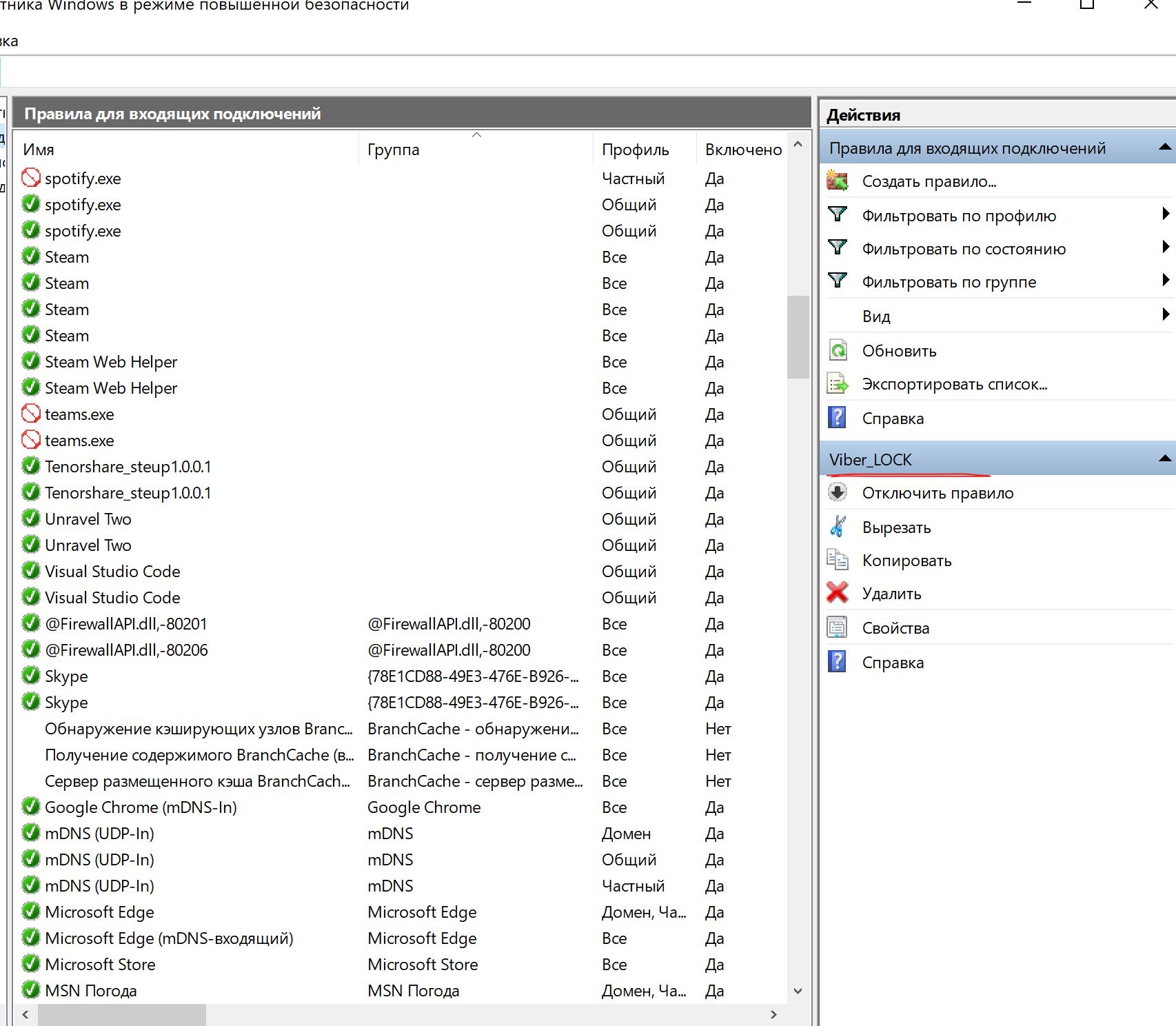
Оставляем по умолчанию:



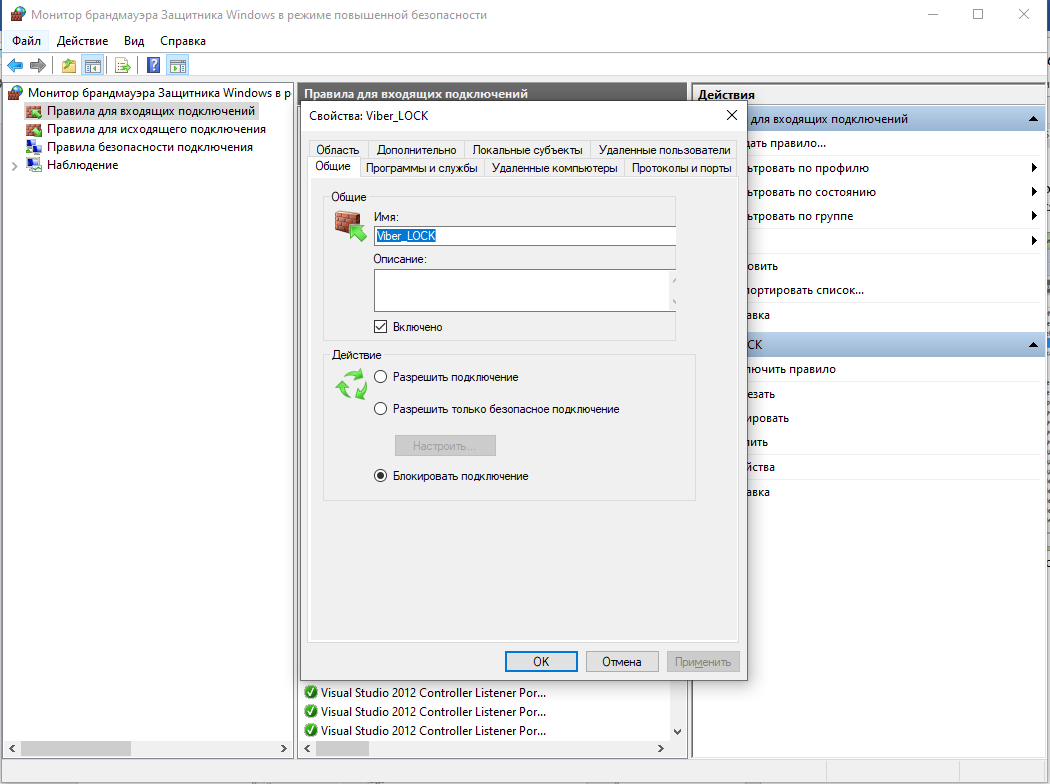
Назначим правилу имя:



В общем списке появилось созданное правило:

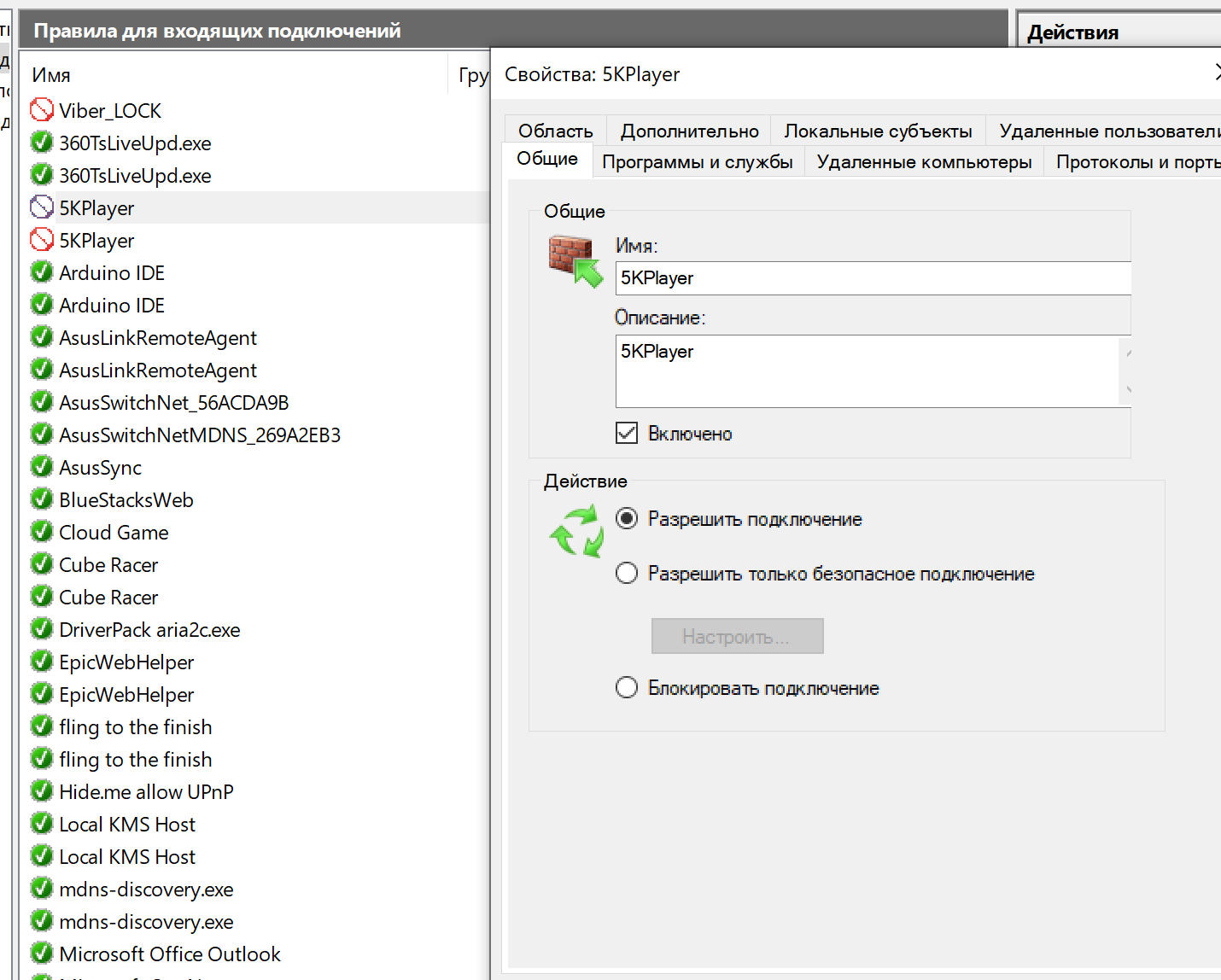


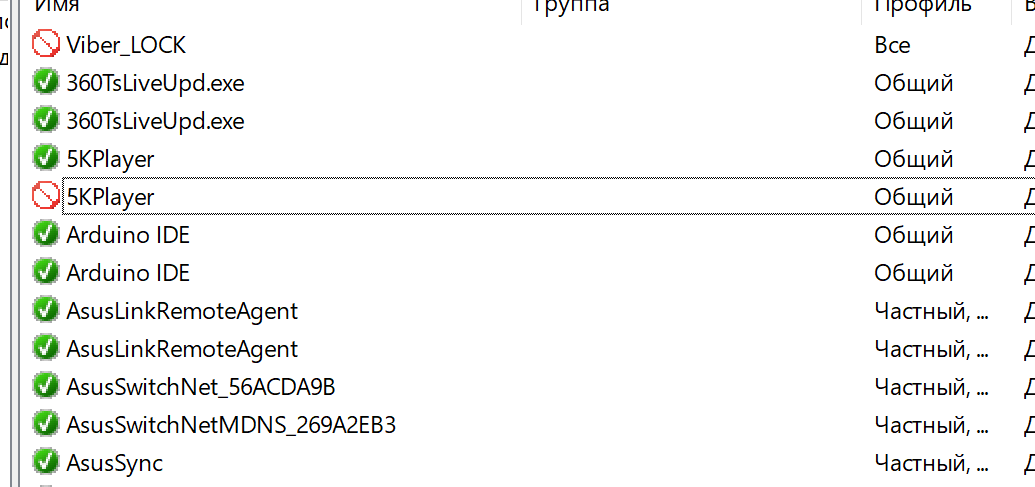
При двойном нажатии можно просмотреть свойства правила:



* 1. Для 1 программы (по выбору) на **разрешение** подключения

Создадим разрешение через свойства правила:



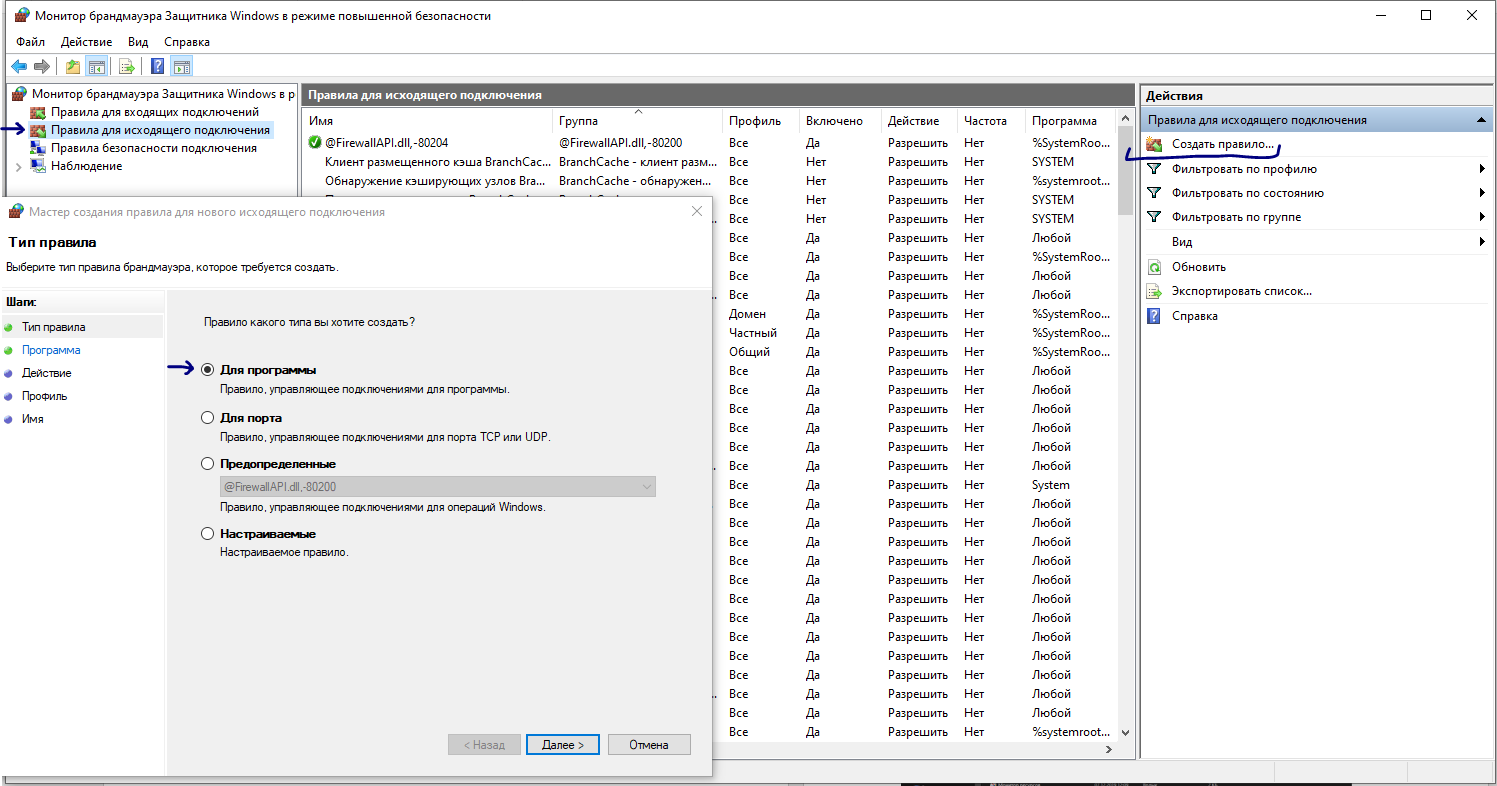


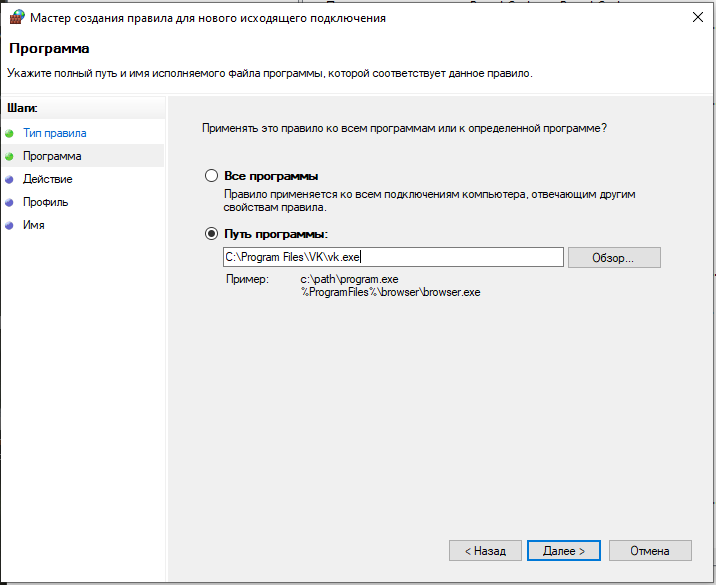
1. Создать правила **для исходящих подключений** (с помещением в электронный конспект копий экрана с пояснениями действий):

Исходящие подключение: с персонального ПК подключение к серверу.

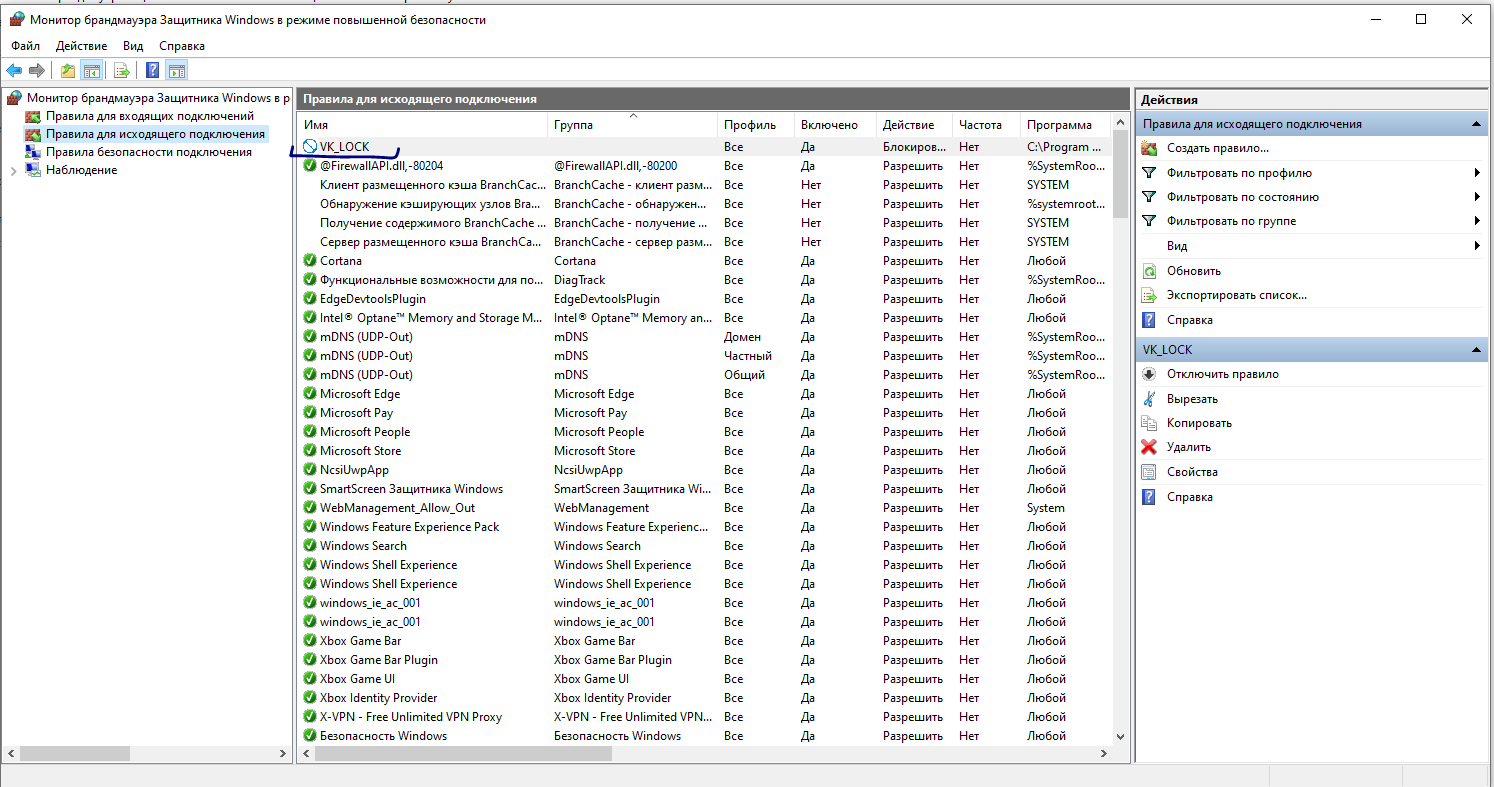
Входящее подключение: на персональный ПК с сервера.

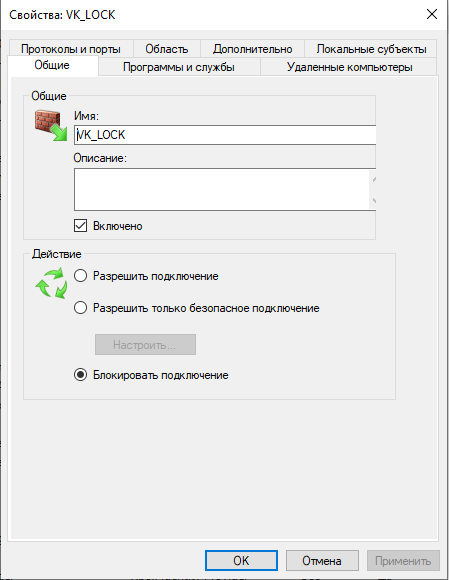
* 1. Для 1 программы (по выбору) на **блокировку** подключения



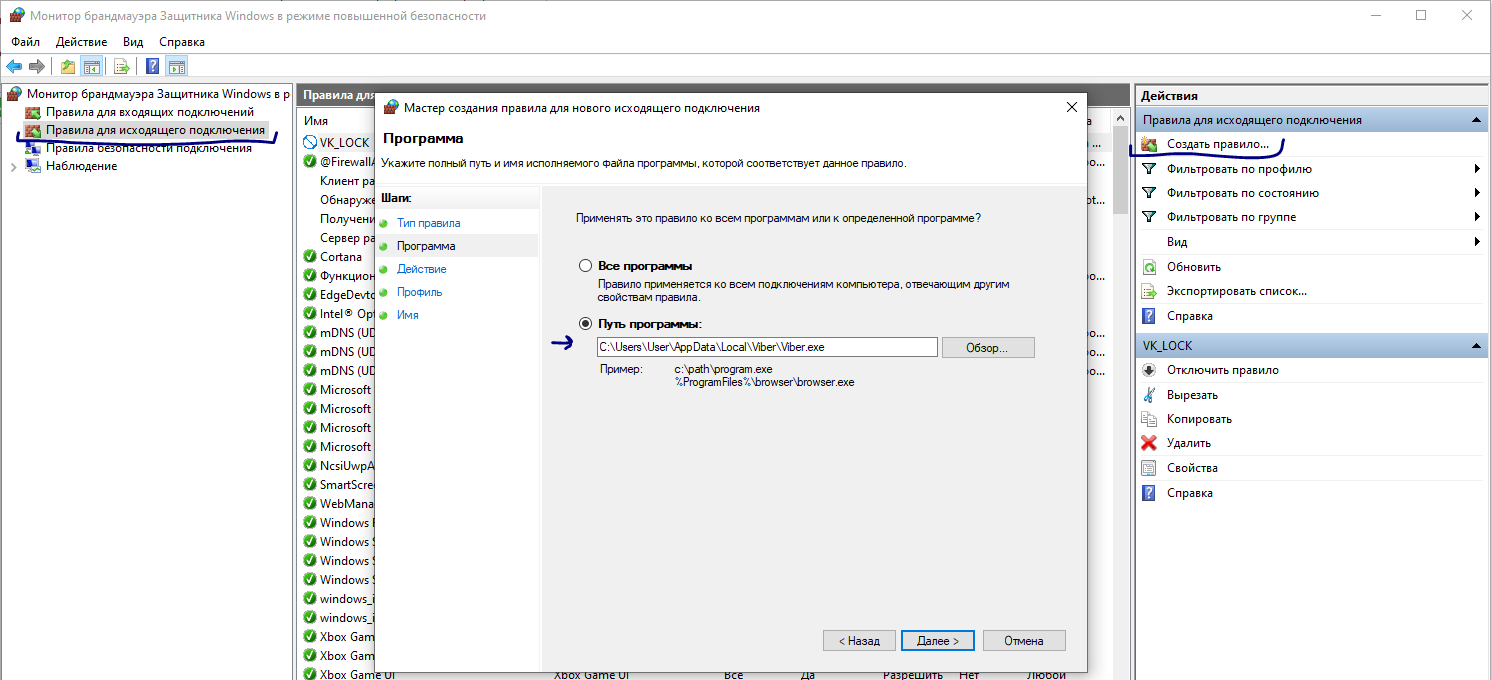


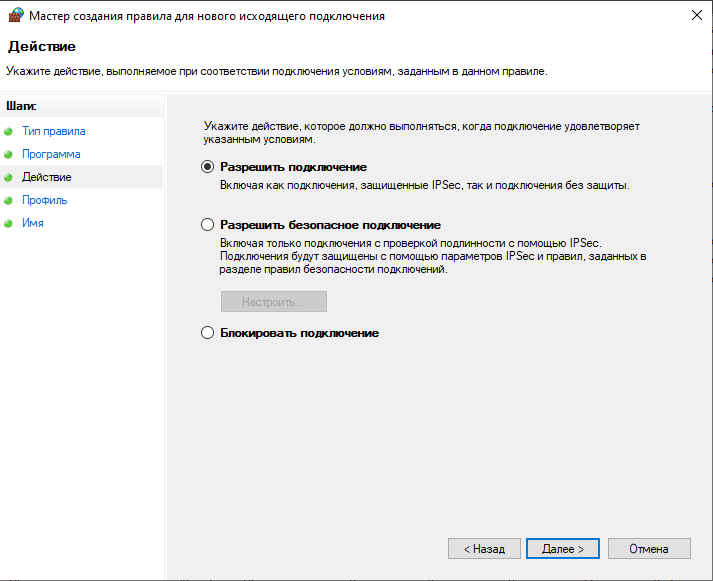
Стандартно задаем имя правила, применяем его. Правило появится в общем списке, двойным щелчком можно просмотреть его свойства:



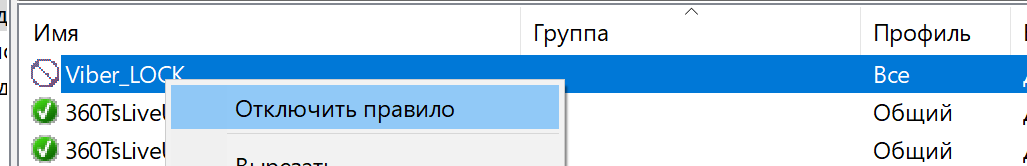


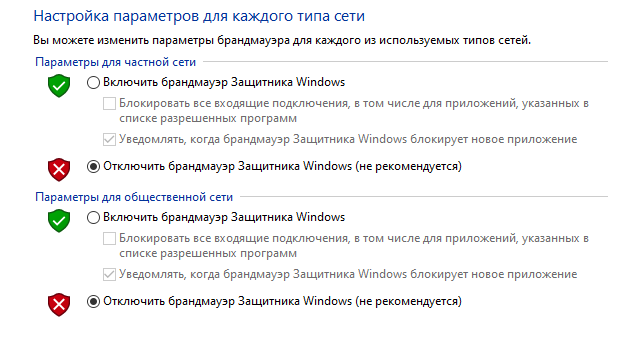
* 1. Для 1 программы (по выбору) на **разрешение** подключения



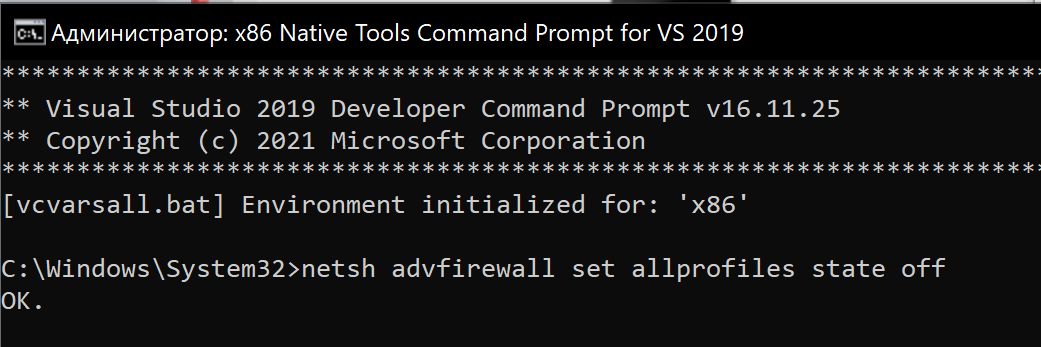


1. **Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.**





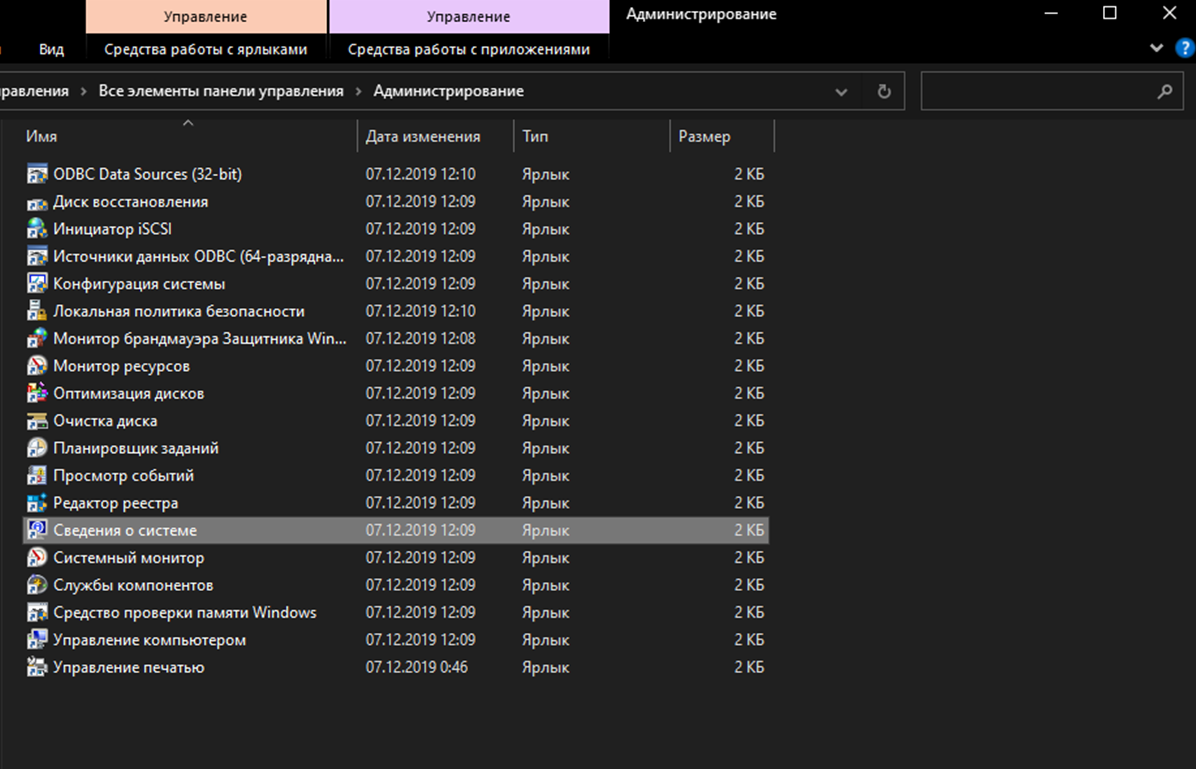
Выключение/включение брандмауэра из командной строки для всех профилей:



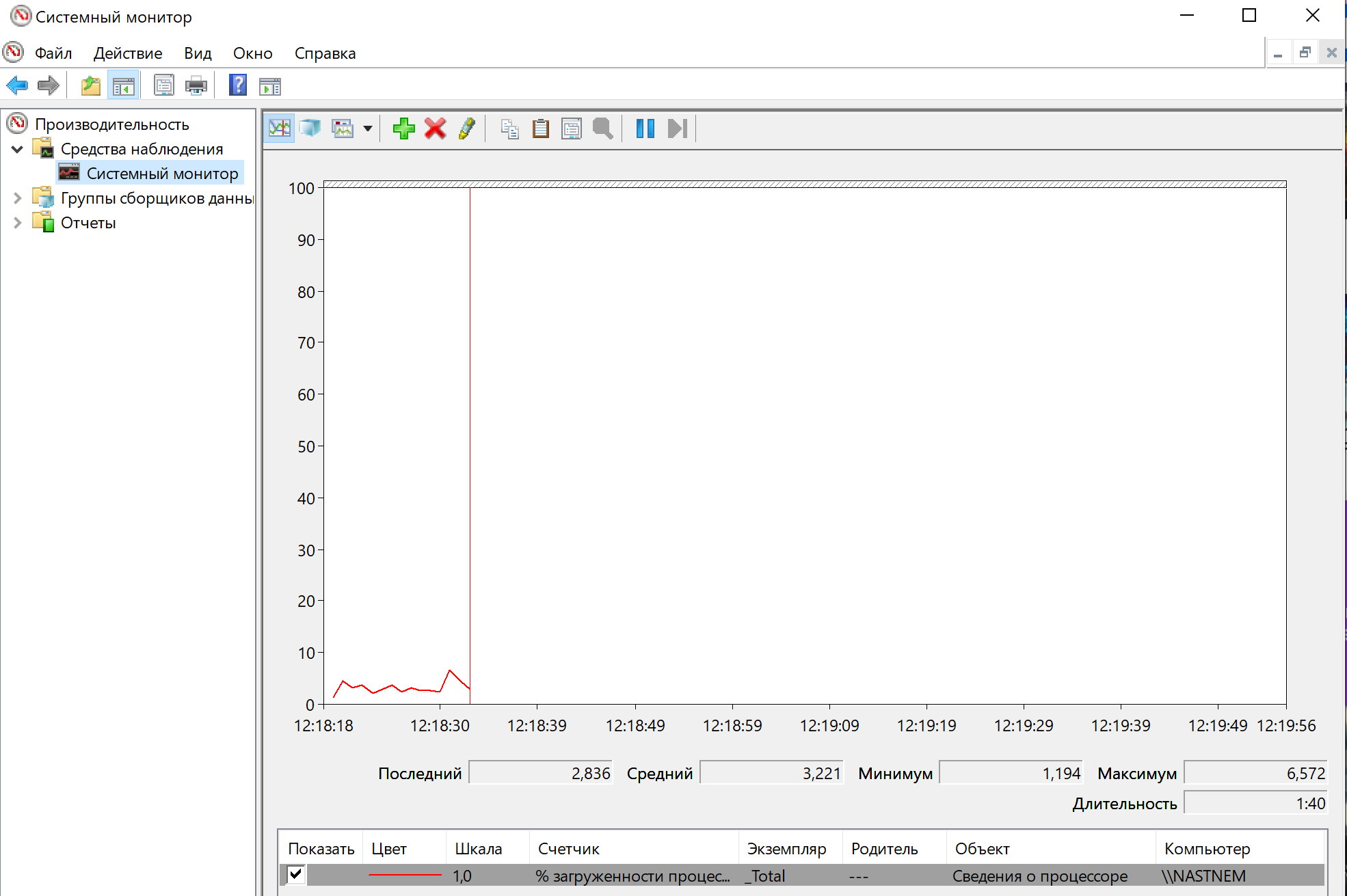
1. **Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).**

В Windows файлы с расширением **msc** являются оснащением консоли управления Windows для управления системными параметрами и процессами.

1. Администрирование – Win + R – **control admintools**: ведет к папке в панели управления, содержащей средства для системного администрирования.

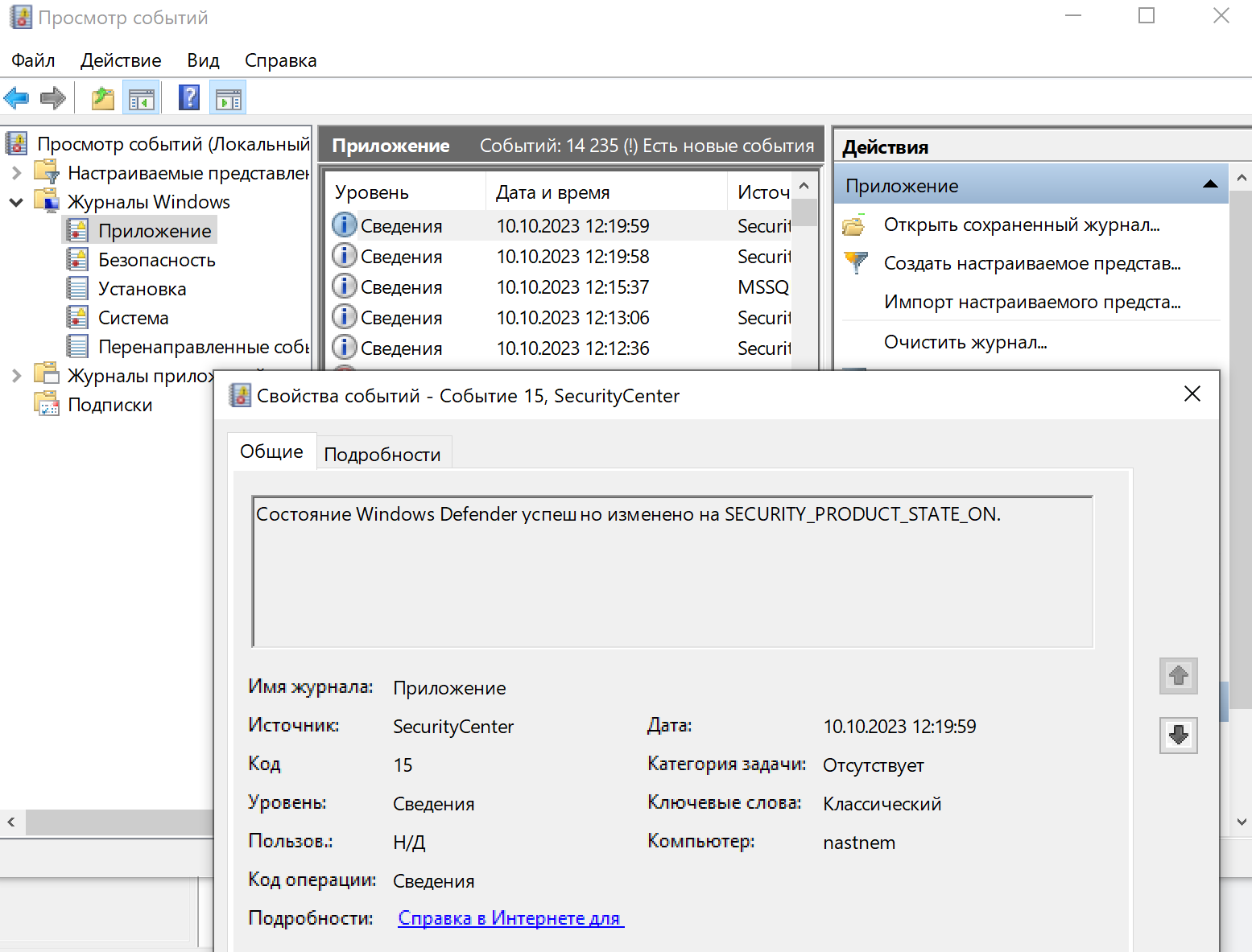


1. Win + R - **perfmon.msc** – системный монитор Windows; имеет несколько режимов отображения и позволяет выводить показания счетчиков производительности в режиме реального времени, а также сохранять данные в лог-файлы для последующего изучения:

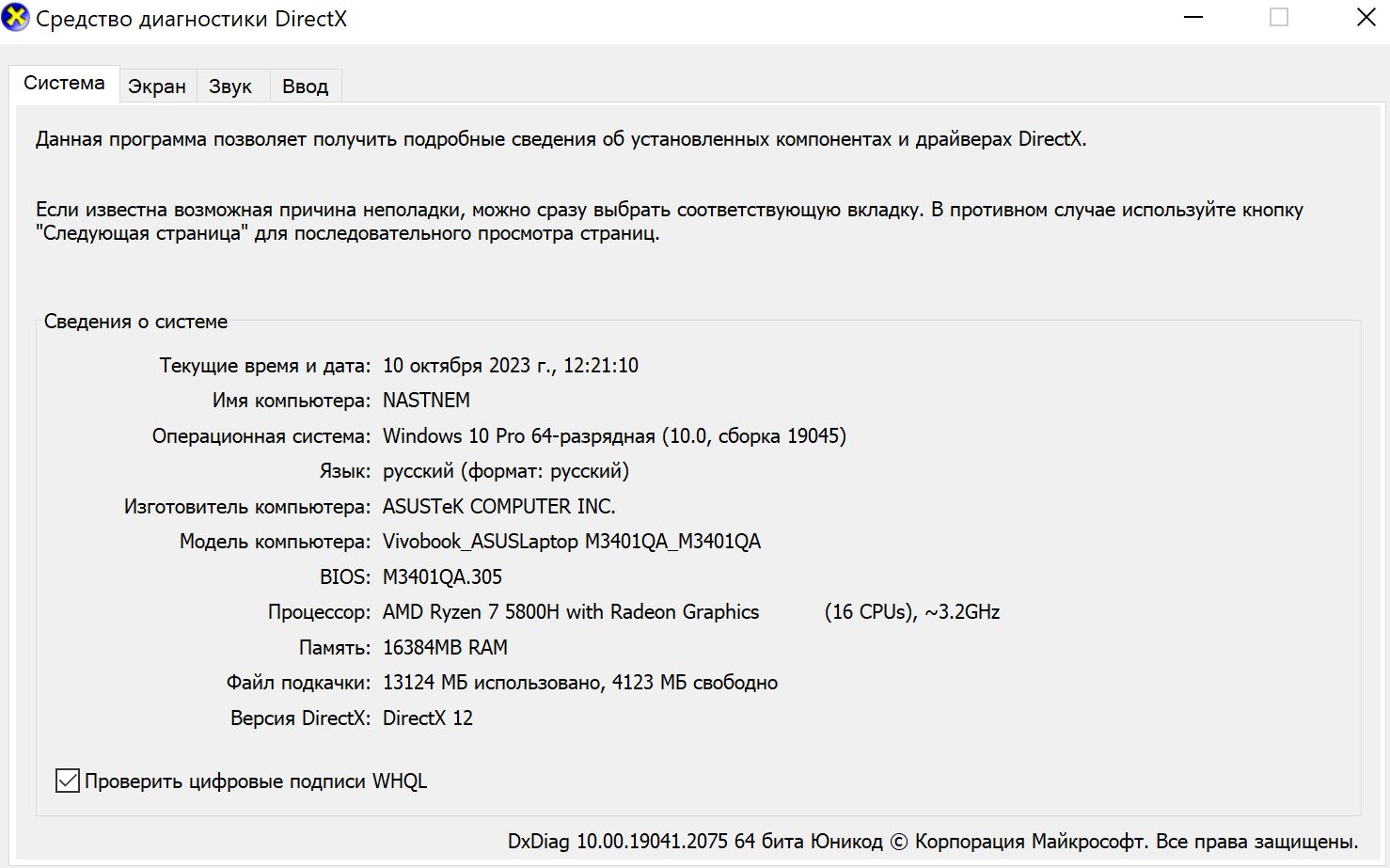


1. Win + R – **eventvwr.msc** – просмотр событий (Event Viewer). При выборе какого-либо события, в нижней части будет отображаться информация о нем. Эта информация может помочь найти решение проблемы в Интернете и стоит понимать, какое свойство что означает:

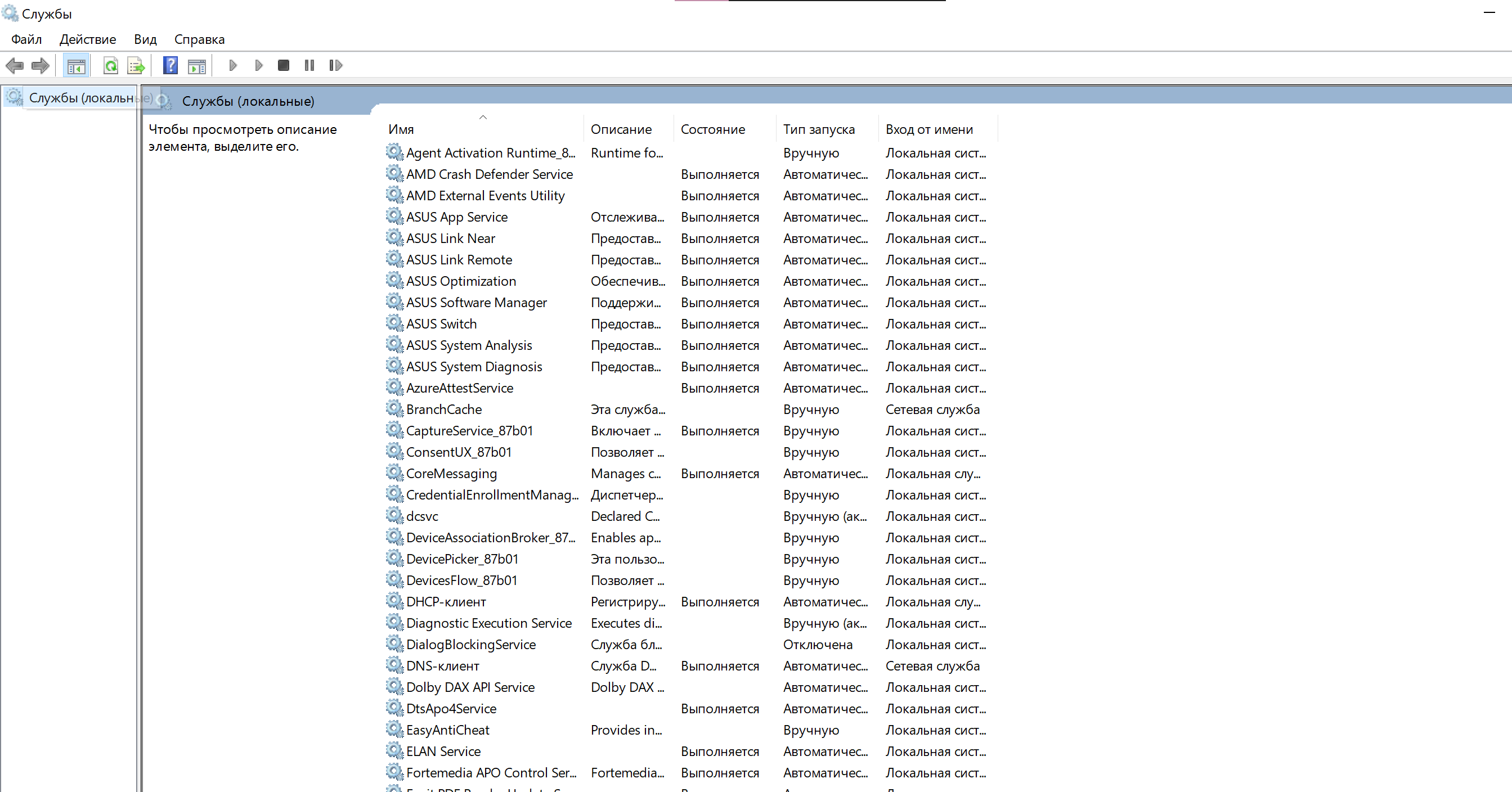
Имя журнала – имя файла журнала, куда была сохранена информация о событии. Источник – название программы, процесса или компонента системы, которое сгенерировало событие (если вы видите здесь Application Error), то имя самого приложение вы можете увидеть в поле выше. Код – код события, может помочь найти информацию о нем в Интернете. Правда, искать стоит в англоязычном сегменте по запросу Event ID + цифровое обозначение кода + название приложения, вызывавшего сбой (поскольку коды событий для каждой программы уникальны). Код операции – как правило, здесь всегда указано «Сведения», так что толку от этого поля мало. Пользователь и компьютер – сообщает о том, от имени какого пользователя и на каком компьютере был запущен процесс, вызвавший событие.



1. Средство диагностики Win + R – **dxdiag**: Это средство используется для сбора информации об устройствах для устранения неполадок со звуком и видео DirectX. Такую информацию может попросить сотрудник службы поддержки, или вы можете опубликовать ее на форуме для получения помощи.

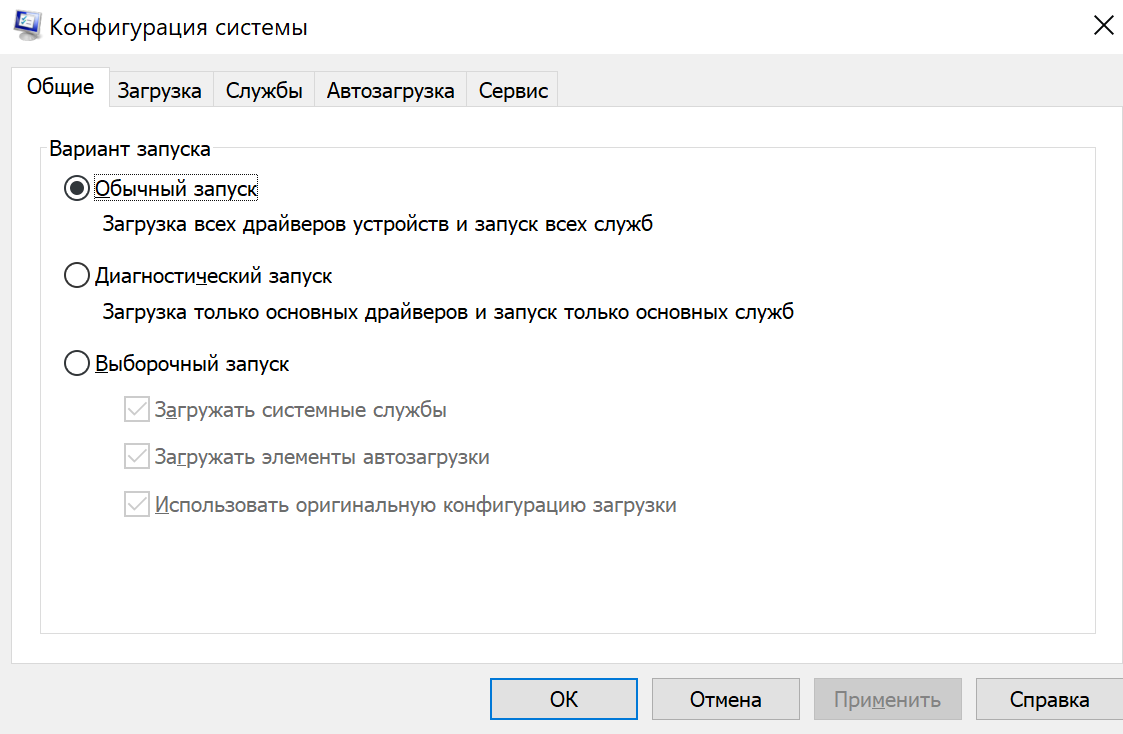


1. Диспетчер системных служб Win + R – **services.msc**:



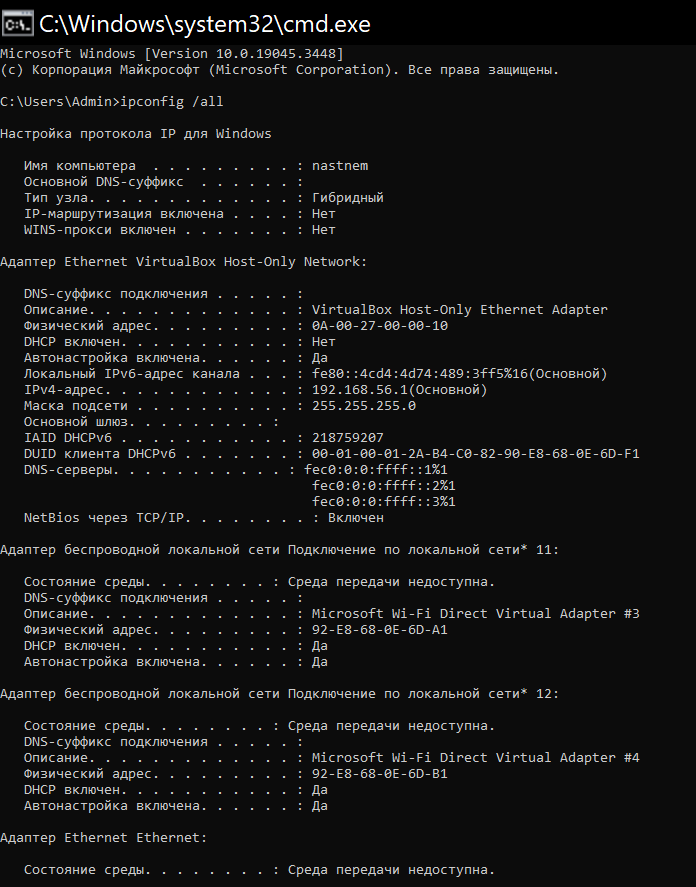
**Службы Windows** – это специальные программы, которые запускаются в фоновом (скрытом) режиме, отвечающие за корректное выполнение других программ, и, в частности, функций Windows.

1. Win + R – **msconfig** (Microsoft System Configuration Utility) – это встроенная утилита операционной системы Windows с помощью которой можно изменить варианты запуска системы, изменить параметры загрузки, включить или отключить службы и программы запускаемые при старте системы, а также выполнить запуск различных диагностических и статистических утилит.

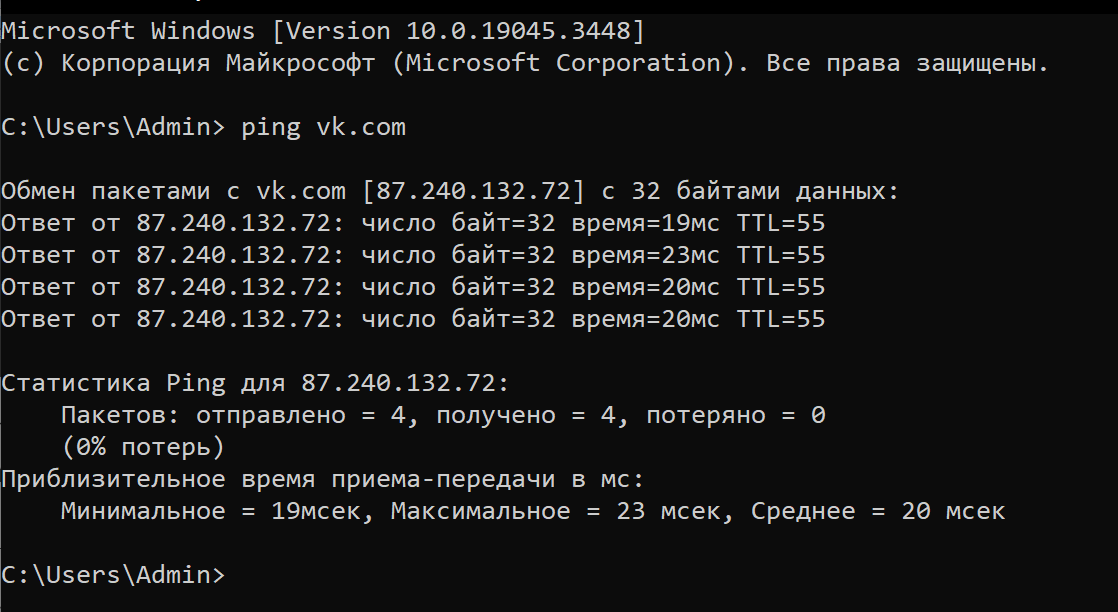


1. Win + R – **cmd**: командная строка Windows – это программное обеспечение в виде текстового интерфейса для управления операционной системой посредством ввода специальных команд.

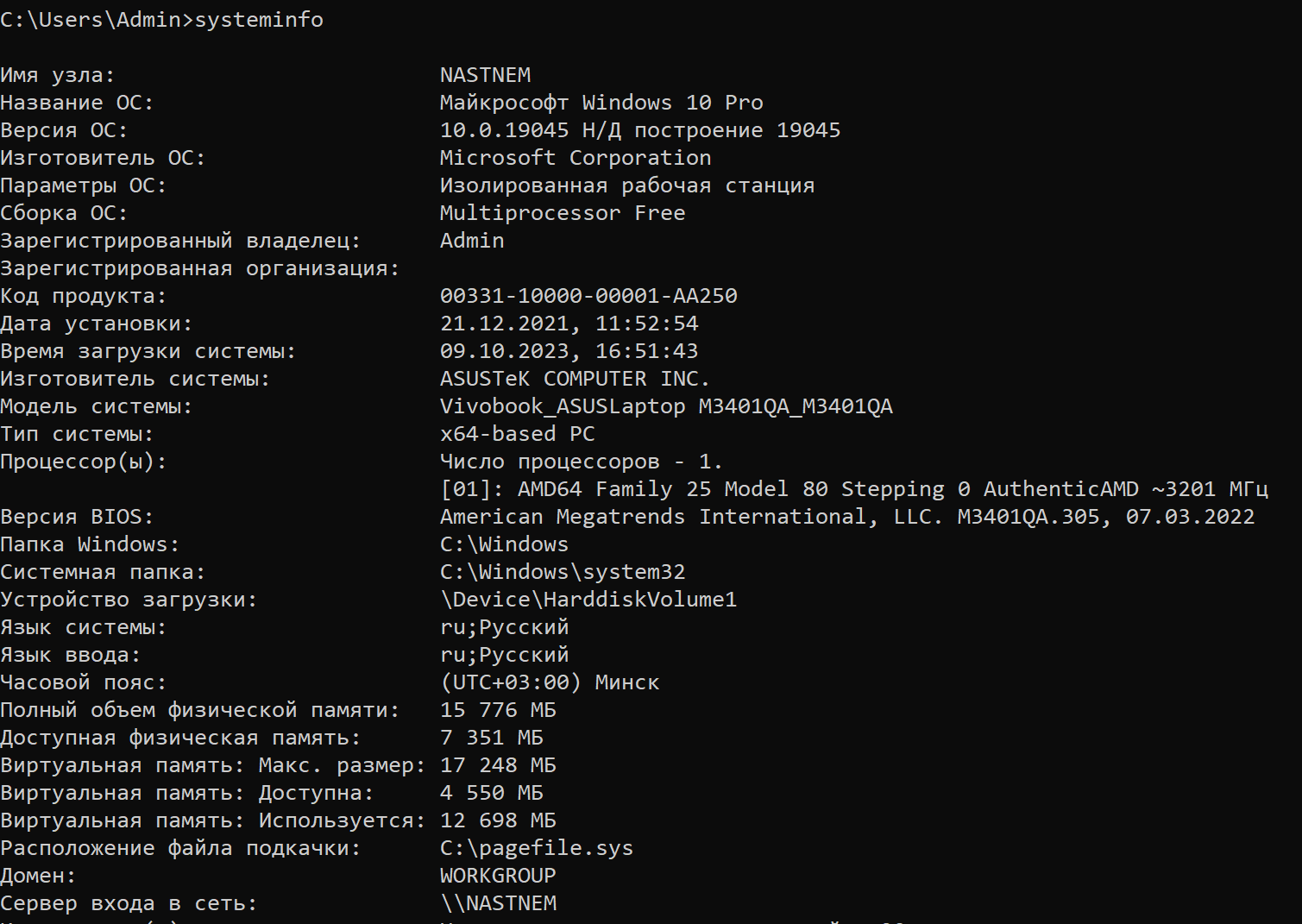
Сведения о сетевых адаптерах: ipconfig /all



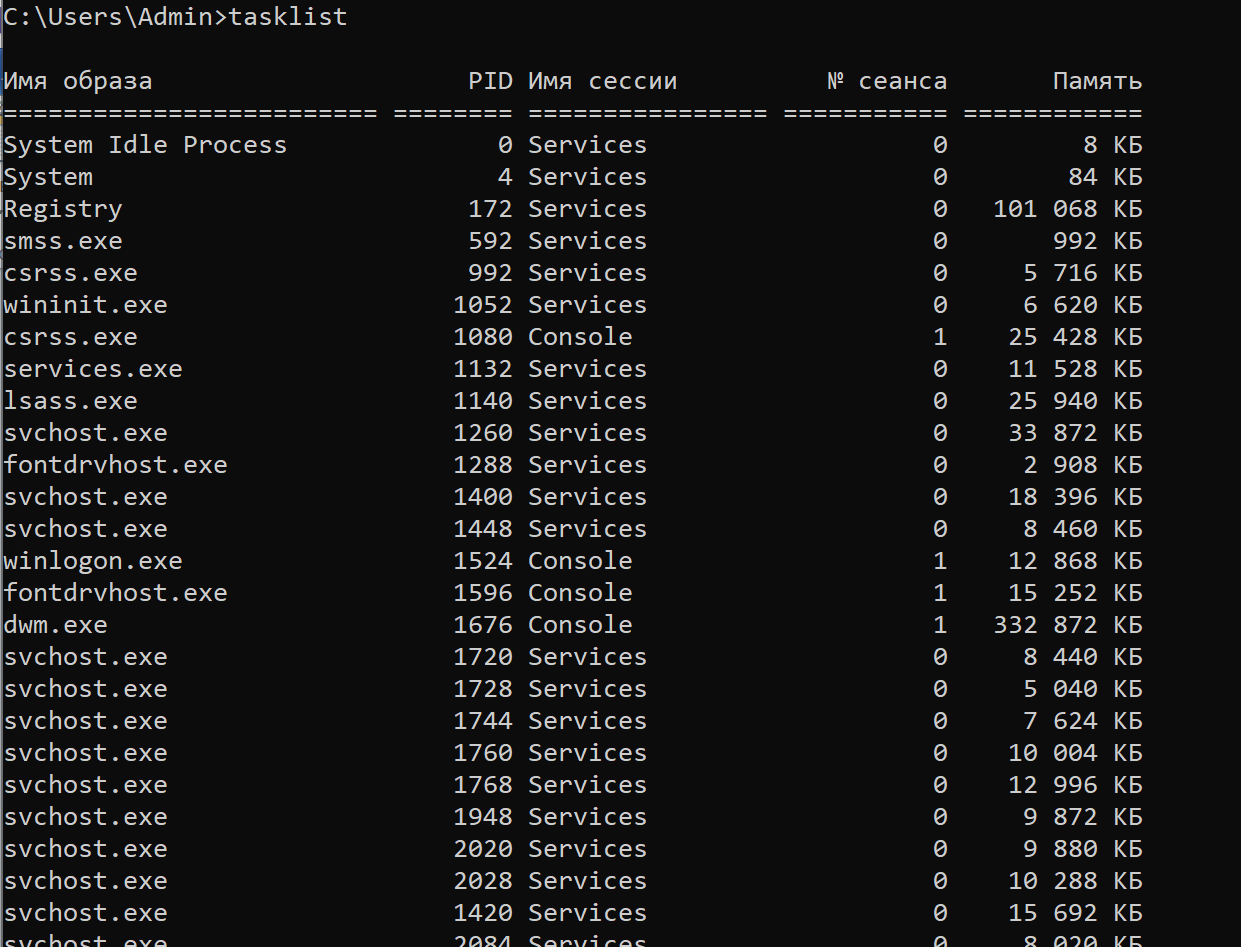
Проверка подключение на уровне IP к другому компьютеру TCP/IP: ping, отправляя сообщения эхо-запросов протокола ICMP. Отображаются сообщения о получении соответствующих эхо-ответов, а также время кругового пути.  Ping – это основная команда TCP/IP, используемая для устранения неполадок подключения, доступности и разрешения имен.



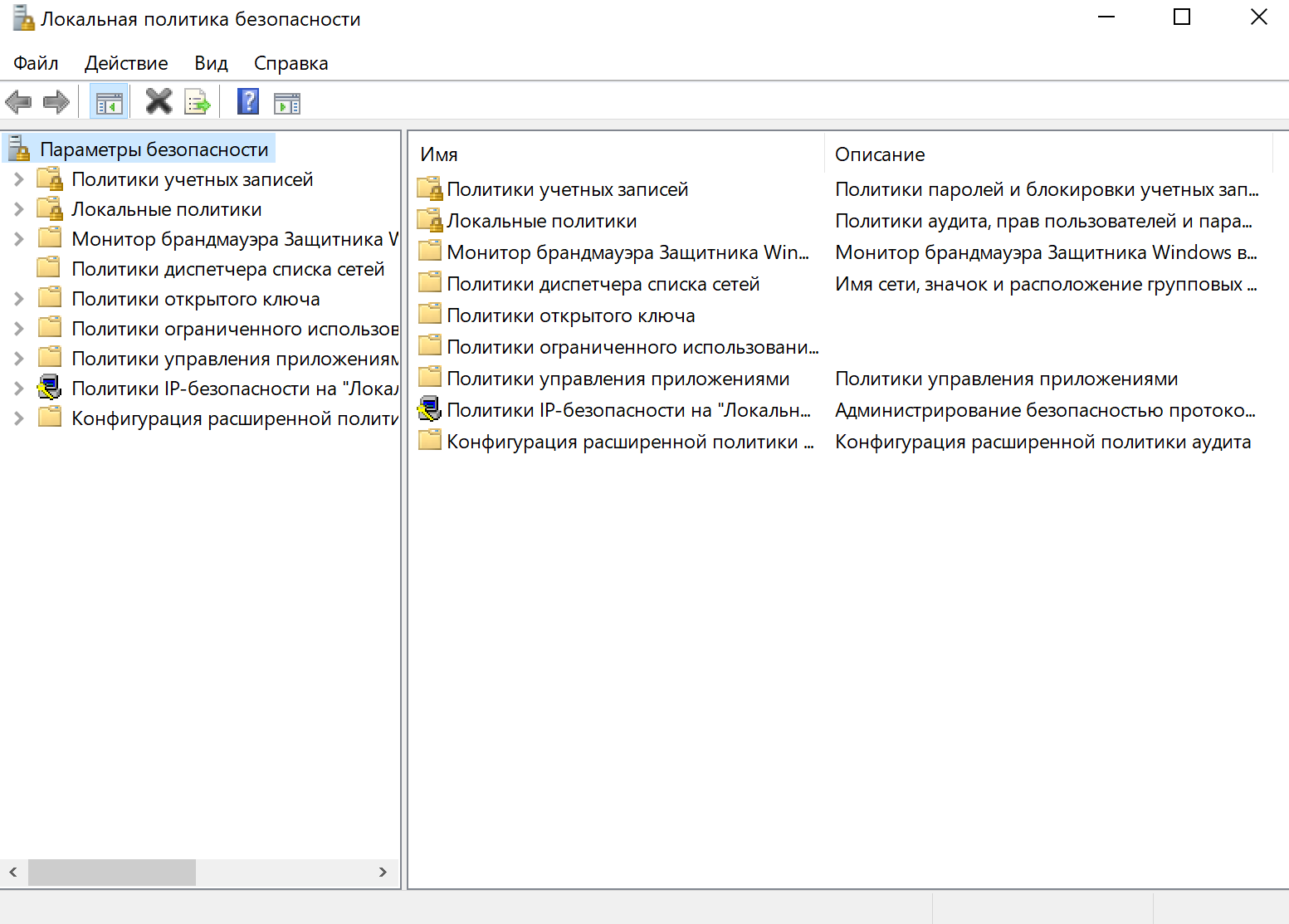
Отображение подробных сведений о конфигурации компьютера и его операционной системы, включая конфигурацию операционной системы: systeminfo, в информационную сводку также входят сведения о безопасности, идентификатор продукта и свойства оборудования (например, ОЗУ, дисковое пространство и сетевые карты).



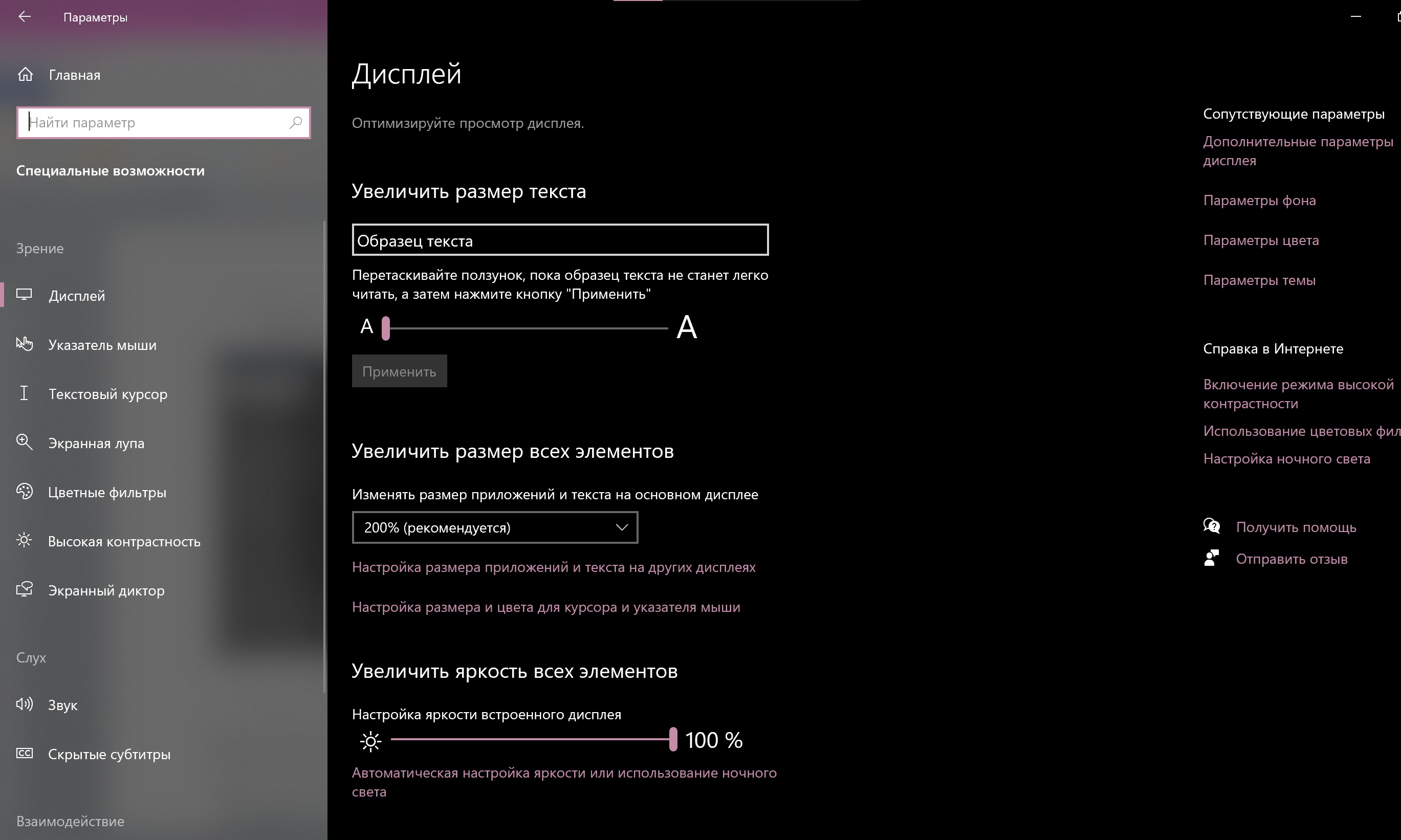
Отобразить список запущенных в данный момент процессов на локальном или удаленном компьютере: tasklist



1. Локальные параметры безопасности, настройка политики безопасности – **secpol.msc:**

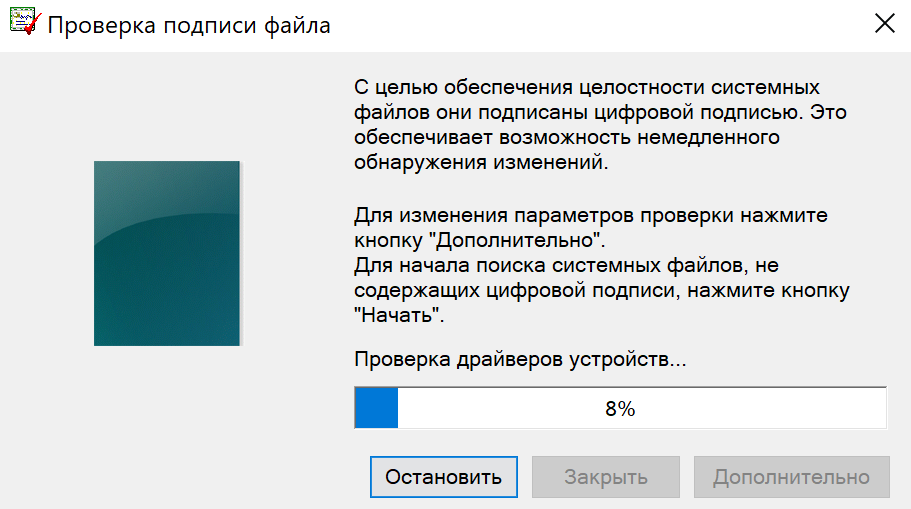
****

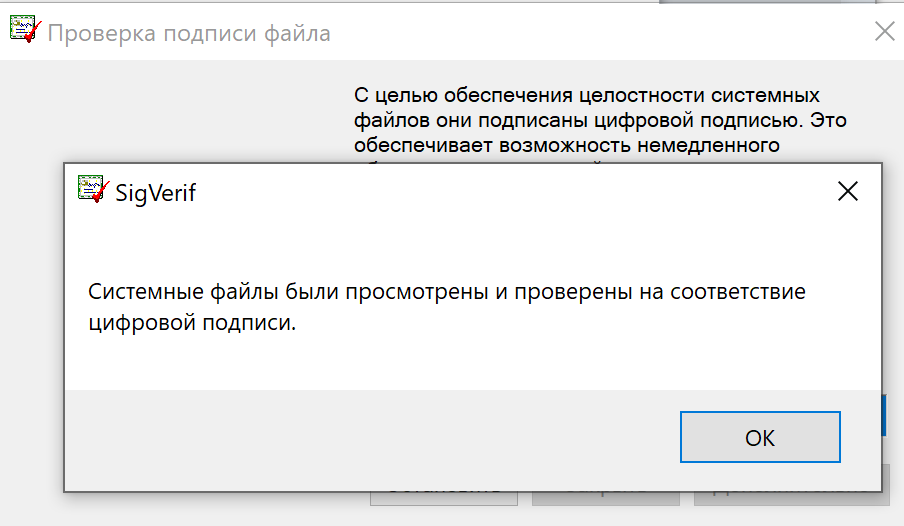
1. Диспетчер служебный программ **utilman**: служит для запуска специальных возможностей на экране блокировки.



1. Утилита «Проверка подписи файла» служит для поиска файлов, не имеющих цифровой подписи.

Цифровая подпись – это криптографический механизм, который используется для проверки подлинности и целостности цифровых данных.





**Вывод**

Firewall – межсетевой экран, который контролирует трафик, поступающий в компьютер.

Фильтруется вся информация, которая приходит. И в зависимости от настроек, входящий трафик либо пропускается, либо отбрасывается. Это программа или программно-аппаратный комплекс, который стоит между сетью внутренней и сетью внешней. Интернет – это внешняя сеть. Внутренняя сеть – сеть организации, домашняя сеть, даже один компьютер считается сетью.

Любая информация, поступающая во внутреннюю сеть, фильтруется этим экраном, файерволом или брандмауэром – это все синонимы, каждый использует эти названия так, как ему привычнее.

Техподдержка Microsoft рекомендует не отключать брандмауэр «Защитника Windows» даже если у пользователя есть сторонняя программа с аналогичными задачами.

Считается что однозначной классификации нет, однако с течением времени выделились основные принципы работы. Итак, файервол в зависимости от типа, выполняет следующие функции:

* Фильтрует пакеты данных по заголовкам. Слабость данного подхода в том, что если пакеты фрагментированные или есть подмена IP, то есть возможность пробить защиту.
* Устанавливает шлюз в рамках сеанса между получателем и отправителем пакета, однако содержимое пакетов не контролируется.
* Становится посредником в соединении – создают шлюз между отправителем и получателем, однако контролируют содержимое пакетов на предмет передаваемых команд и потенциально небезопасных инструкций. Минус – работают относительно медленно и требуют достаточно много вычислительной мощности.
* Работает как инспектор состояния – гармонично анализирует данные, используя преимущества всех трех перечисленных выше вариантов.
* Кроме того, файервол может определять какое именно программное обеспечение пытается выйти в интернет и блокировать эту попытку. Большинство современных файерволов способны работать в режиме обучения, позволяя пользователю настроить сетевую политику для всех программ, пытающихся выйти в интернет.