Настройка политики безопасности Windows 11

Введение

Настройка политики безопасности в операционной системе Windows включает работу с локальной политикой и групповой политикой (Group Policy Object, GPO). Эти инструменты позволяют администраторам задавать правила безопасности для компьютеров и пользователей, а также централизованно управлять настройками в корпоративной сети.

Версия ОС: Windows 11.

1. Новые настройки реестра

Все последующие действия будут происходить по пути HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\

Чтобы его открыть, нужно проделать следующие действия:

1. Откройте Редактор реестра

1.1 Нажмите клавиши Win + R

1.2 Введите regedit

1.3 Нажмите ОК или Enter

Раздел HKEY_LOCAL_MACHINE находится в левой части окна (панели навигации).

Пример представлен на рисунке 1.

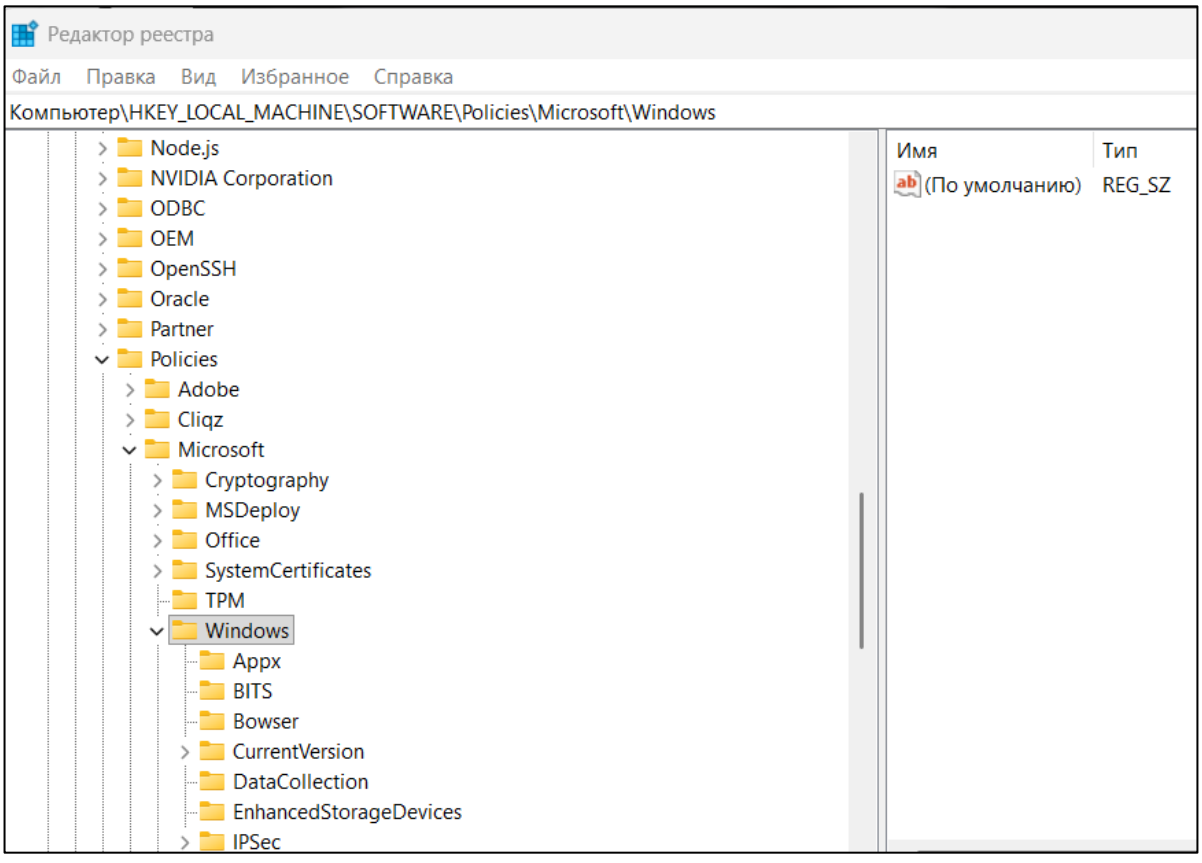

Рисунок 1 – Редактор реестра

1.1 Снижение уровня телеметрии

Телеметрия – это технология удаленного сбора, передачи и анализа данных.

– перейдите по раннему пути, и найдите там раздел DataCollection: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection;

– создайте параметр DWORD с именем AllowTelemetry;

– установите значение 0.

Пример представлен на рисунке 1.1.

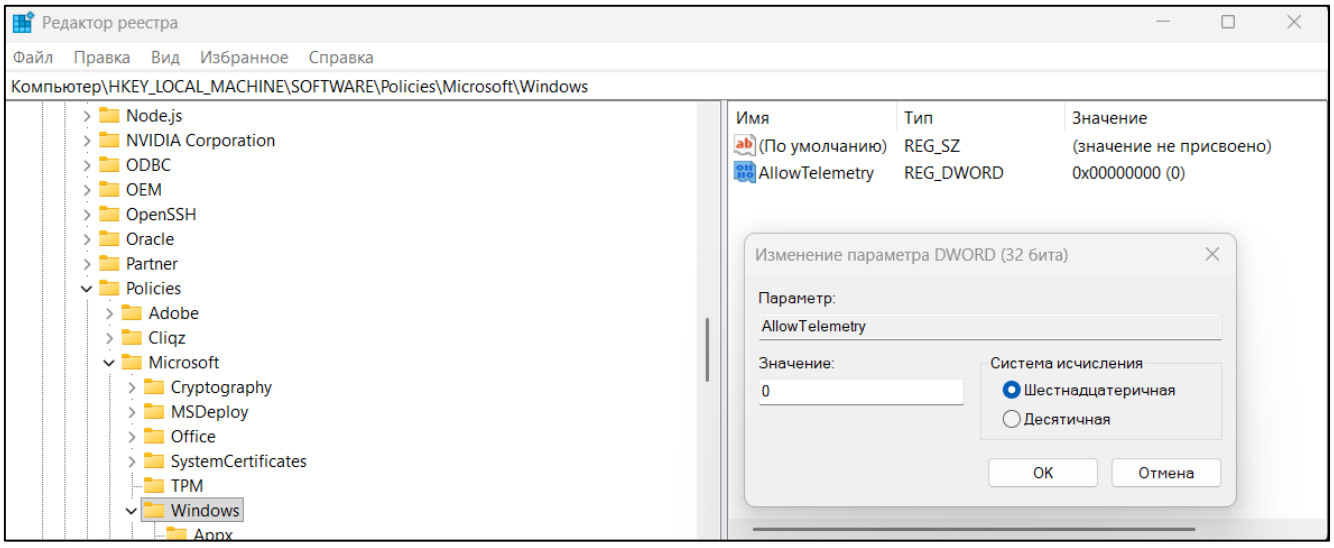

Рисунок 1.1 – Параметр AllowTelemetry

1.2 Отключение рекламы и рекомендаций

1. Перейдите в ContentDeliveryManager по пути: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager

2. Найдите параметр SilentInstalledAppsEnabled

3. Измените значение с 1 на 0

Если у вас отсутствует такой раздел, можно отключить рекомендации через настройки:

1. Откройте Параметры (Win + I)

2. Перейдите в Персонализация → Пуск

3. Найдите переключатель "Показывать рекомендации" и выключите его

Пример представлен на рисунке 1.2.

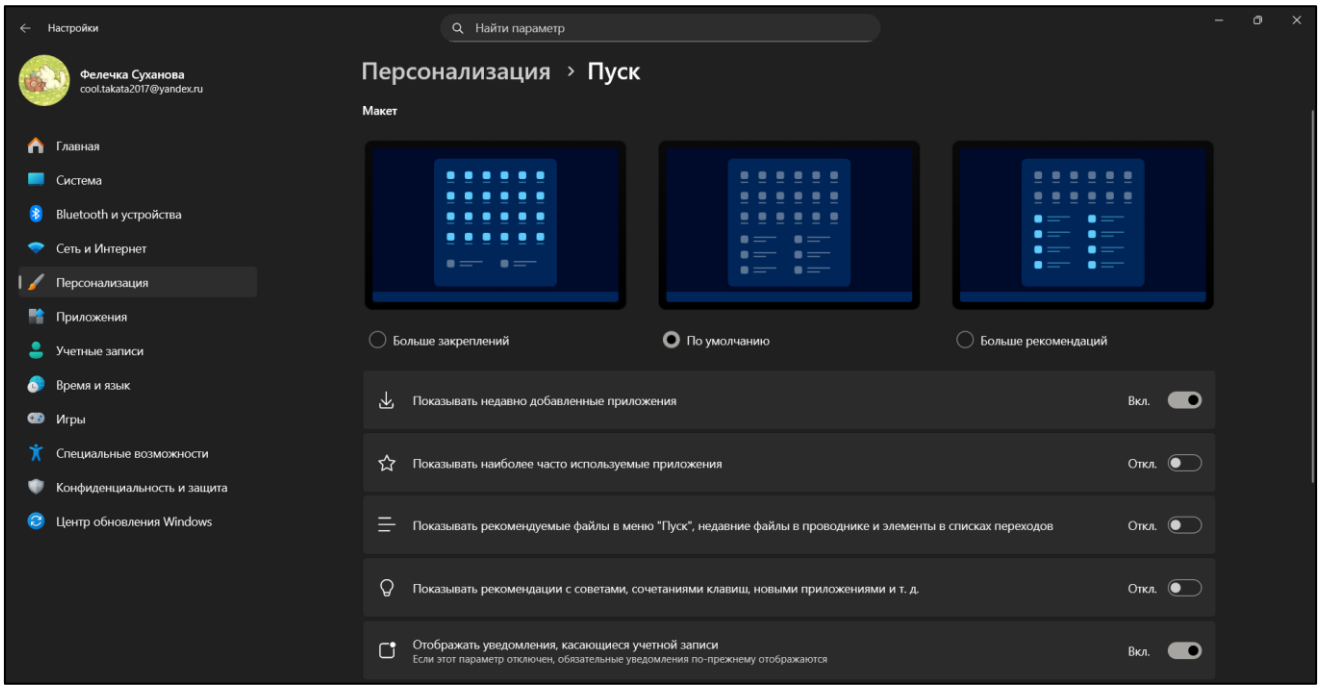

Рисунок 1.2 – Отключение рекомендаций в параметрах

1.3 Блокировка облачных результатов поиска

1. Перейдите в раздел «Search» по следующему пути: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search

2. Создайте параметр DWORD с именем BingSearchEnabled

3. Установите значение 0

Пример представлен на рисунке 1.3.

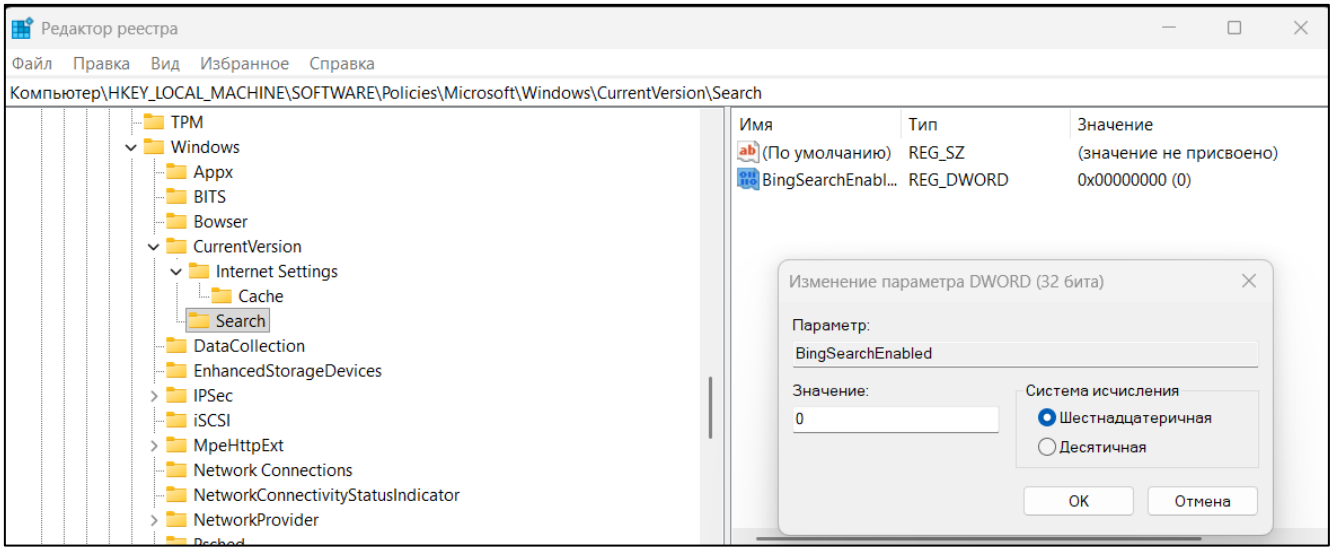

Рисунок 1.3 – Блокировка поиска через Bing

2. Оптимизация служб Windows

2.1 Отключение службы телеметрии

1. Нажмите Win + R и введите cmd для открытия командной строки

2. Введите команду sc query DiagTrack для отслеживания статуса службы

3. Остановите службу командой sc stop DiagTrack

4. Отключите автозапуск командой sc config DiagTrack start= disabled

5. Проверьте результат командой sc query DiagTrack

Пример представлен на рисунке 2.1.

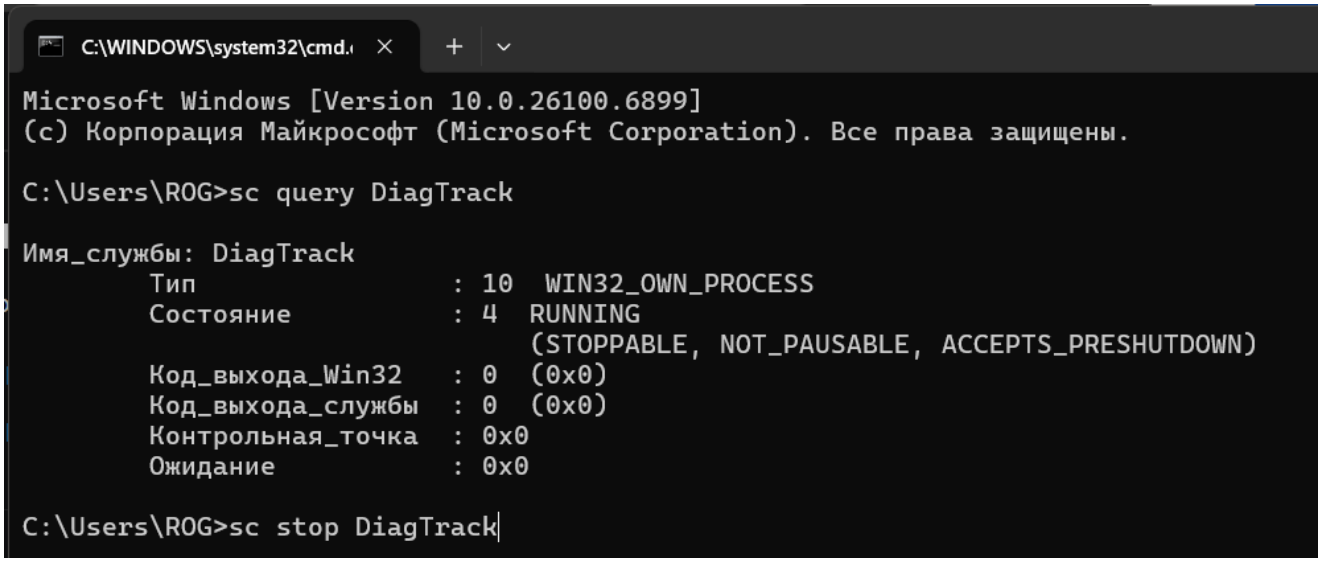

Рисунок 2.1 – Отключение службы диагностики

2.2 Отключение службы геолокации

1. Откройте Параметры (Win + I)

2. Перейдите в Конфиденциальность и защита → Расположение

3. Выключите «Служба определения местоположения»

4. Нажмите «Изменить» и отключите определение местоположения для этого устройства

Пример представлен на рисунке 2.2.

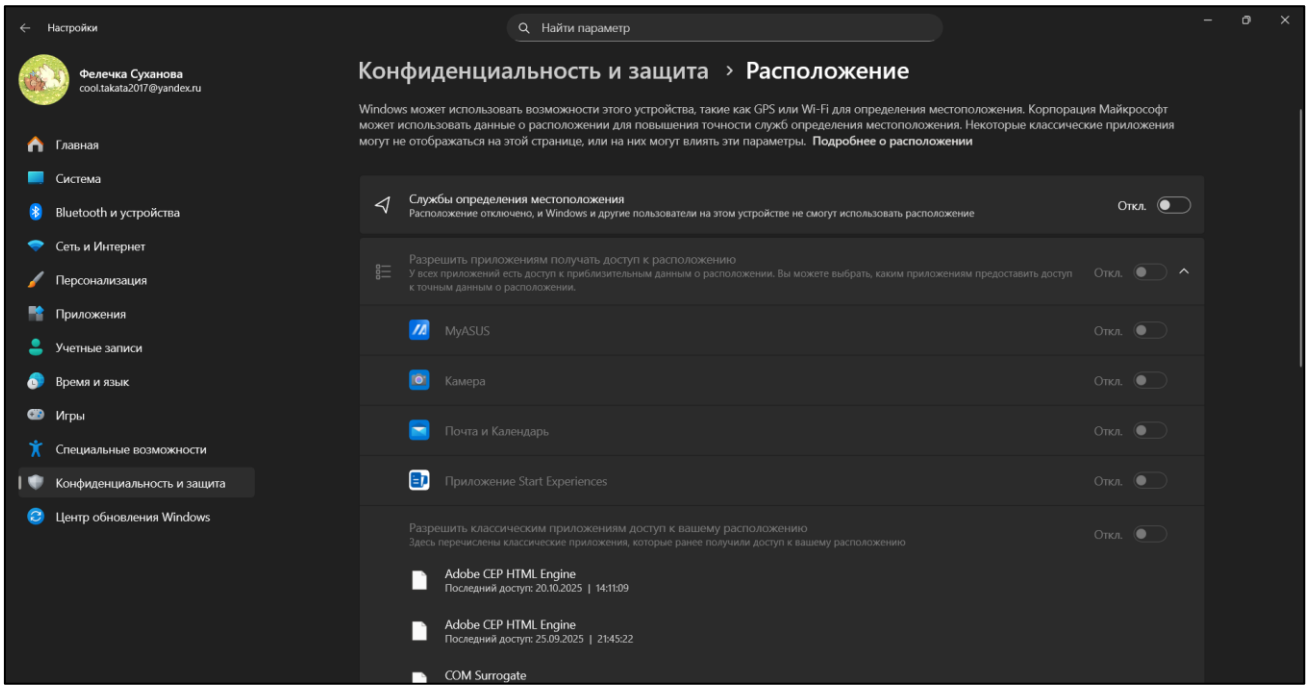

Рисунок 2.2 – Отключение службы определения местоположения

2.3 Отключение лишних служб Xbox

1. Ищите «Xbox Accessory Management» в вашем списке служб

2. Дважды щелкните на «Xbox Accessory Management» или правой кнопкой → «Свойства»

3. Тип запуска выберите «Отключена»

4. Нажмите кнопку «Остановить»

5. Нажмите «Применить» и «ОК»

Пример представлен на рисунке 2.3.

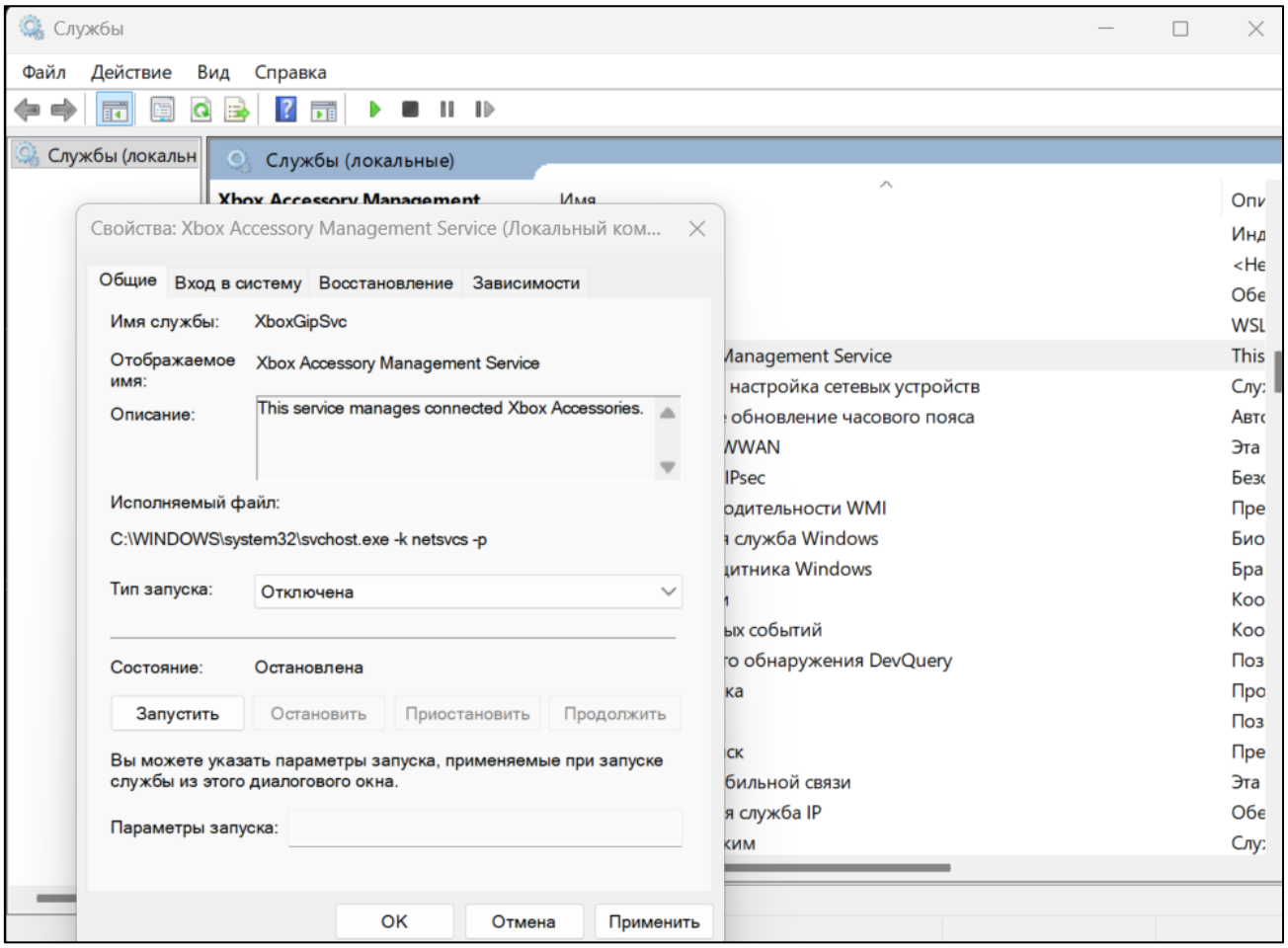

Рисунок 2.3 – Службы Xbox для отключения

3. Настройка Брандмауэра

Прежде всего, убедитесь, что он активен:

1. Нажмите Win + S и введите брандмауэр.

2. Выберите «Брандмауэр Защитника Windows».

3. Откроется главное окно. Вы должны увидеть статус "Подключено" для частных и общедоступных сетей.

Пример представлен на рисунке 3.1.

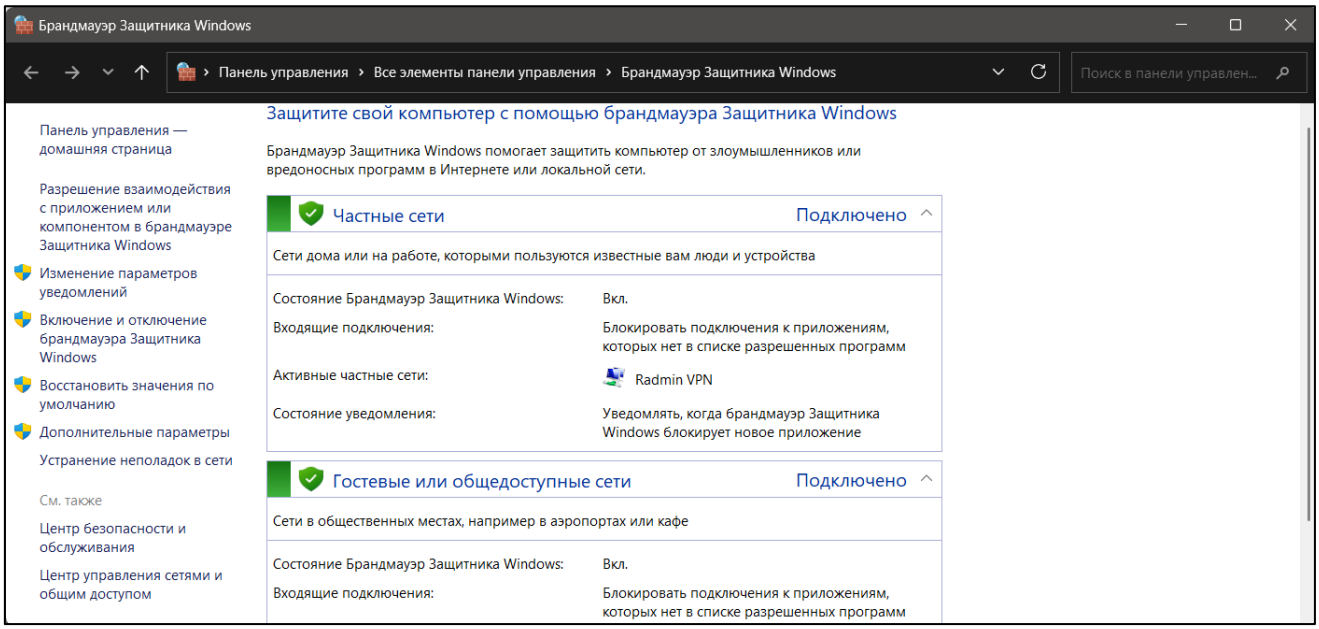

Рисунок 3.1 – Главное окно Брандмауэра

Создание собственных правил нужно для более точного контроля.

Откройте через поиск «Монитор брандмауэра Защитника Windows в режиме повышенной безопасности».

Допустим, вы хотите полностью заблокировать программе исходящий трафик.

1. В «Мониторе...» выберите «Правила для исходящих подключений».

2. Справа нажмите «Создать правило».

3. Выберите «Для программы» → «Далее».

4. Укажите путь к .exe файлу программы → «Далее».

5. Выберите «Блокировать подключение» → «Далее».

6. Оставьте все три галочки (Домен, Частная, Общедоступная) для максимальной защиты → «Далее».

7. Дайте правилу понятное имя и нажмите «Готово».

Теперь это правило будет блокировать программе любой исходящий трафик, независимо от ее собственных настроек. Пример представлен на рисунке 3.2.

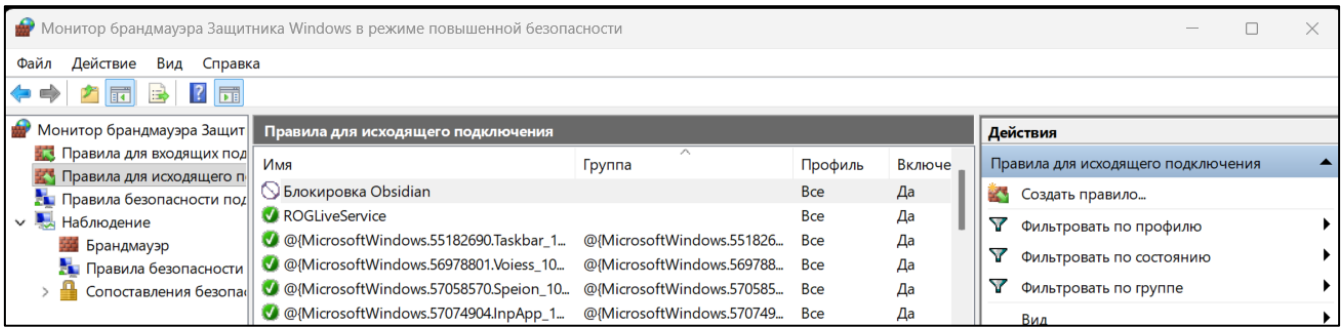

Рисунок 3.2 – Создание нового правила

Вывод

Настройка политики безопасности Windows 11 представляет собой комплексный процесс, включающий три основных направления: редактирование системного реестра для ограничения сбора данных и рекламы, оптимизацию фоновых служб для отключения неиспользуемых функций (телеметрия, геолокация, Xbox) и тонкую настройку Брандмауэра Windows для создания персональных правил фильтрации сетевого трафика.

Эти меры позволяют значительно повысить конфиденциальность и контроль над системой, ограничивая передачу данных в Microsoft и сторонние серверы, а также усиливая защиту от несанкционированного сетевого доступа.