**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
ИМЕНИ М.Т. КАЛАШНИКОВА»

Институт «Информатика и вычислительная техника»

Кафедра «Защита информации в компьютеризированных системах»

Отчёт

по лабораторной работе №1

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

на тему «Формирование доверенной среды ПО антивирусными средствами защиты»

Выполнил: студент группы С17-361-1

Буров К.А.

Проверил: Кудашев П.А.

Ижевск 2021

**Цель работы:**

Для обеспечения безопасности информации при работе, связанной с использованием автоматизированных рабочих мест, настроить доверенную среду, посредством применения специализированного программного обеспечения в интерактивном режиме с помощью создания правил и запретов для исполняемых процессов.

**Задачи:**

1. Подготовить рабочую станцию к созданию доверенной среды.
2. Скачать и установить специализированное программное обеспечение.
3. Настроить интерактивный режим работы программы.
4. Для каждого возникающего события определить название процесса, путь до исполняемого файла и на основе его назначения выбрать соответствующее сетевое правило.
5. Настроить системные запреты по умолчанию и при необходимости для каждого конкретного процесса.

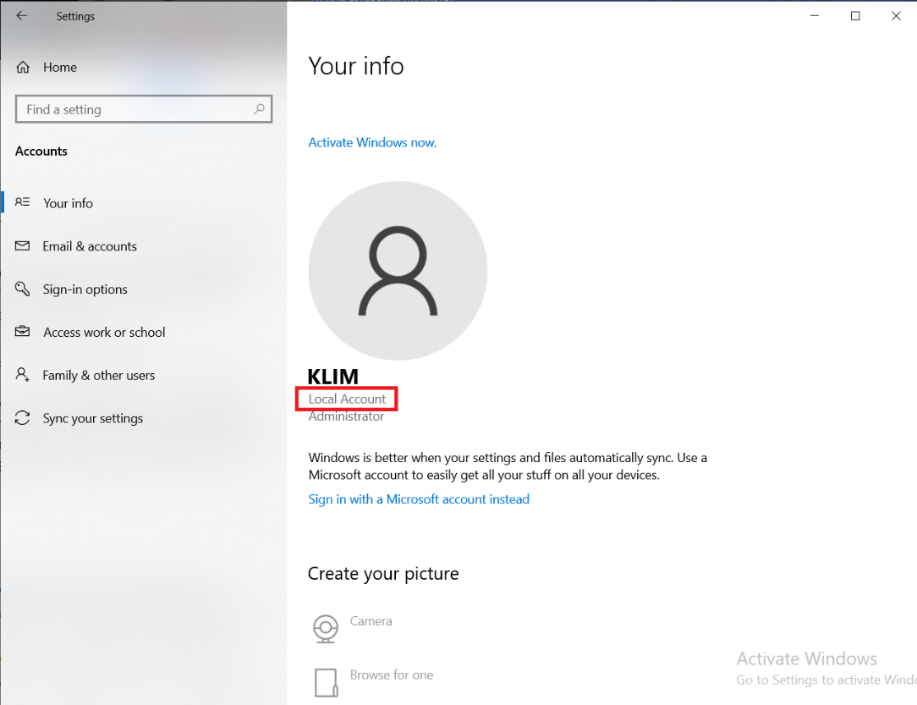
**Ход работы**

Перед настройкой доверенной среды сторонними средствами подготовим рабочую станцию. В подготовку будут входить: отключение ненужных служб, настройка телеметрии и т.д.

В процессе подготовки с помощью утилиты Services были отключены следующие службы:

* служба пульса (Hyper-V);
* служба виртуализации удалённых рабочих столов Hyper-V;
* служба синхронизации времени Hyper-V;
* служба завершения работы в качестве гостя (Hyper-V);
* служба обмена данными (Hyper-V);
* служба сеансов виртуальных машин Hyper-V;
* служба данных датчиков;
* служба наблюдения за датчиками;
* служба датчиков;
* функциональные возможности для подключённых пользователей и телеметрия;
* служба географического положения;
* вторичный вход в систему;
* удаленный реестр;
* рабочая станция;
* модуль поддержки NetBIOS через TCP/IP;
* вспомогательная служба IP;
* факс (для юзеров, не использующих факс);
* диспетчер печати (нет принтера, нет и службы);
* служба шифрования дисков BitLocker (отключаем в случае неиспользования шифрования жесткого диска);
* сетевая служба Xbox Live (деактивируем вследствие отсутствия игровой приставки и подписки на Xbox Live);
* служба управления аксессуарами Xbox Live;
* менеджер аутентификации Xbox Live;
* служба сохранений игр Xbox Live;
* служба поддержки Bluetooth (в случае, если не используем сеть Bluetooth);
* общий доступ к интернету (ICS) (не раздаем интернет по Wi-Fi с ноутбука, нет смысла и держать службу включенной);
* изоляция ключей CNG (отключаем, если к ПК не подключено криптографическое оборудование);
* служба лицензий клиента (деактивируем при отсутствии надобности в магазине Microsoft Store);
* служба диагностического отслеживания

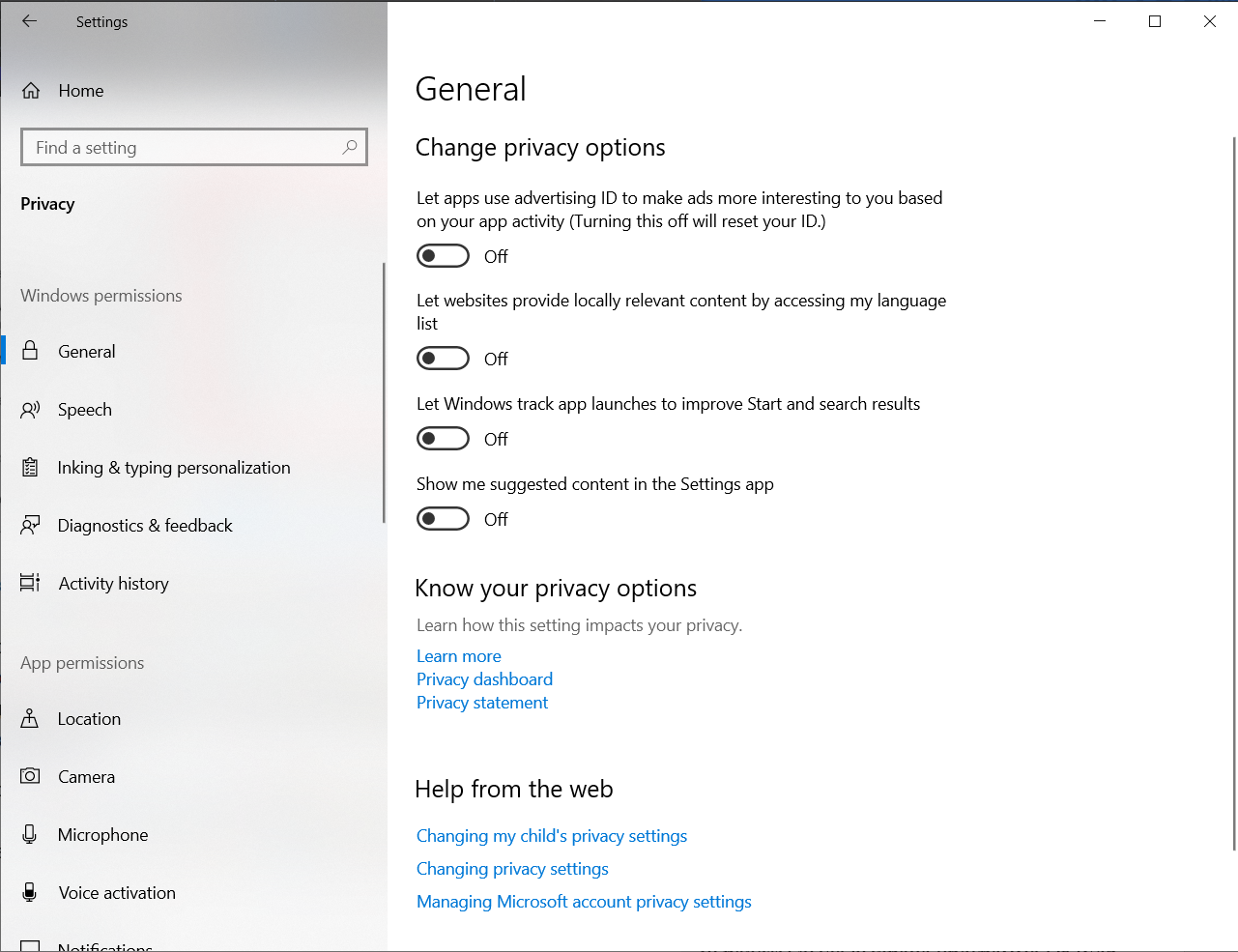
Также будем использовать локальную учетную запись для предотвращения нежелательной отправки данных в Microsoft



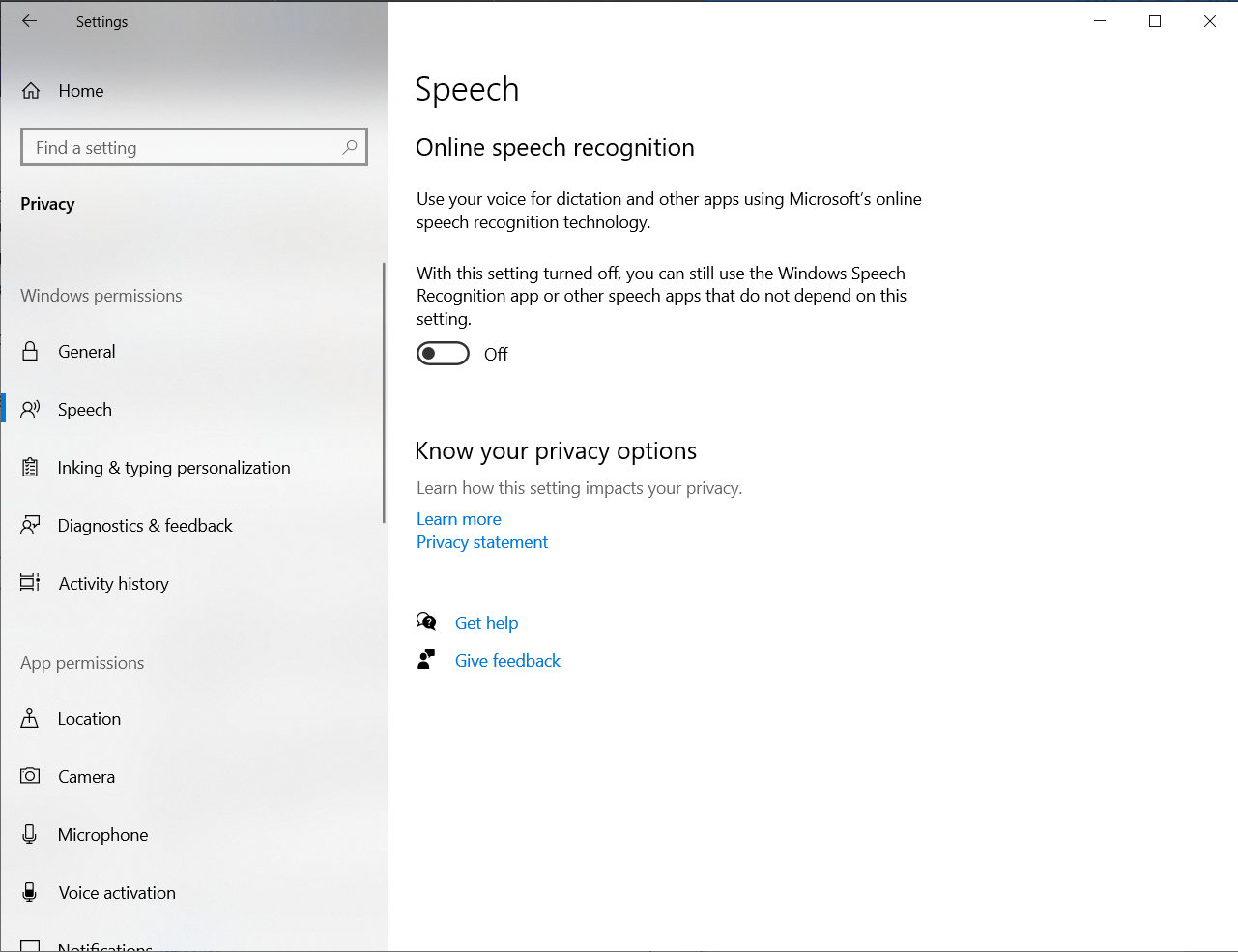
Перейдем в раздел Параметры –> Конфиденциальность->

В разделе Общие отключаем следующие настройки:

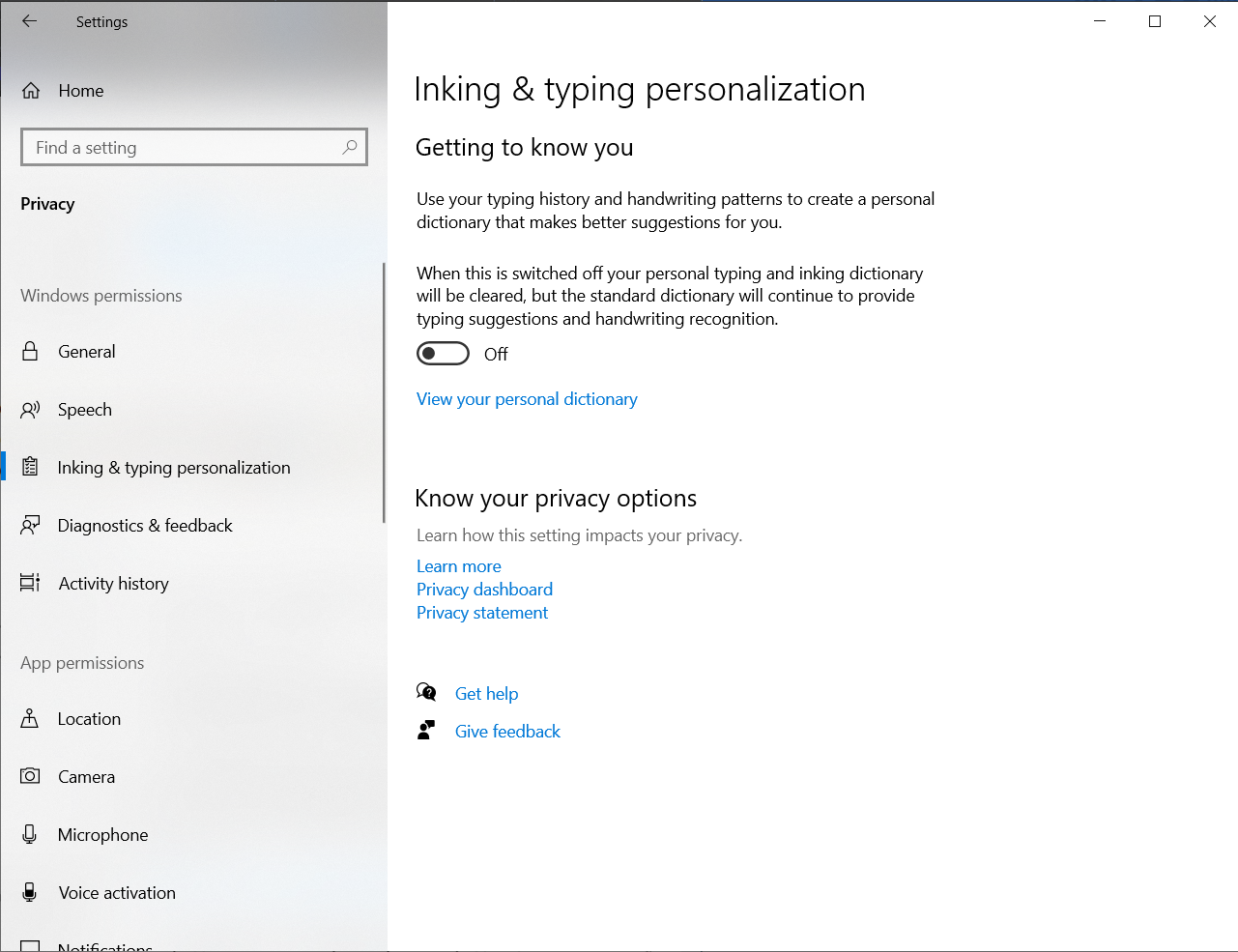
* Использование рекламного идентификатора
* Доступ к списку языков
* Отслеживание запуска приложений
* Показ рекомендуемого содержимого



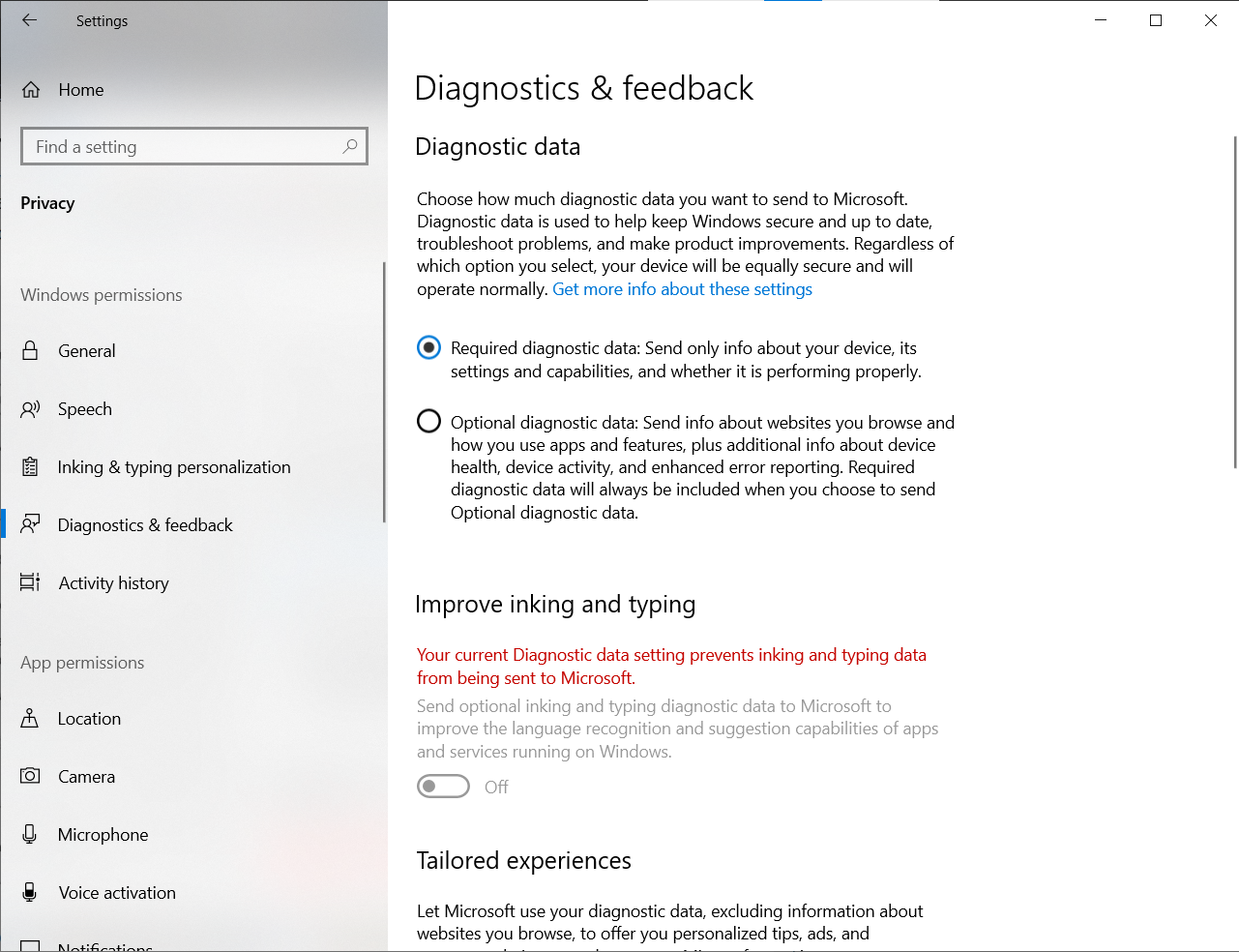
В разделе Голосовые функции отключаем распознавание голоса



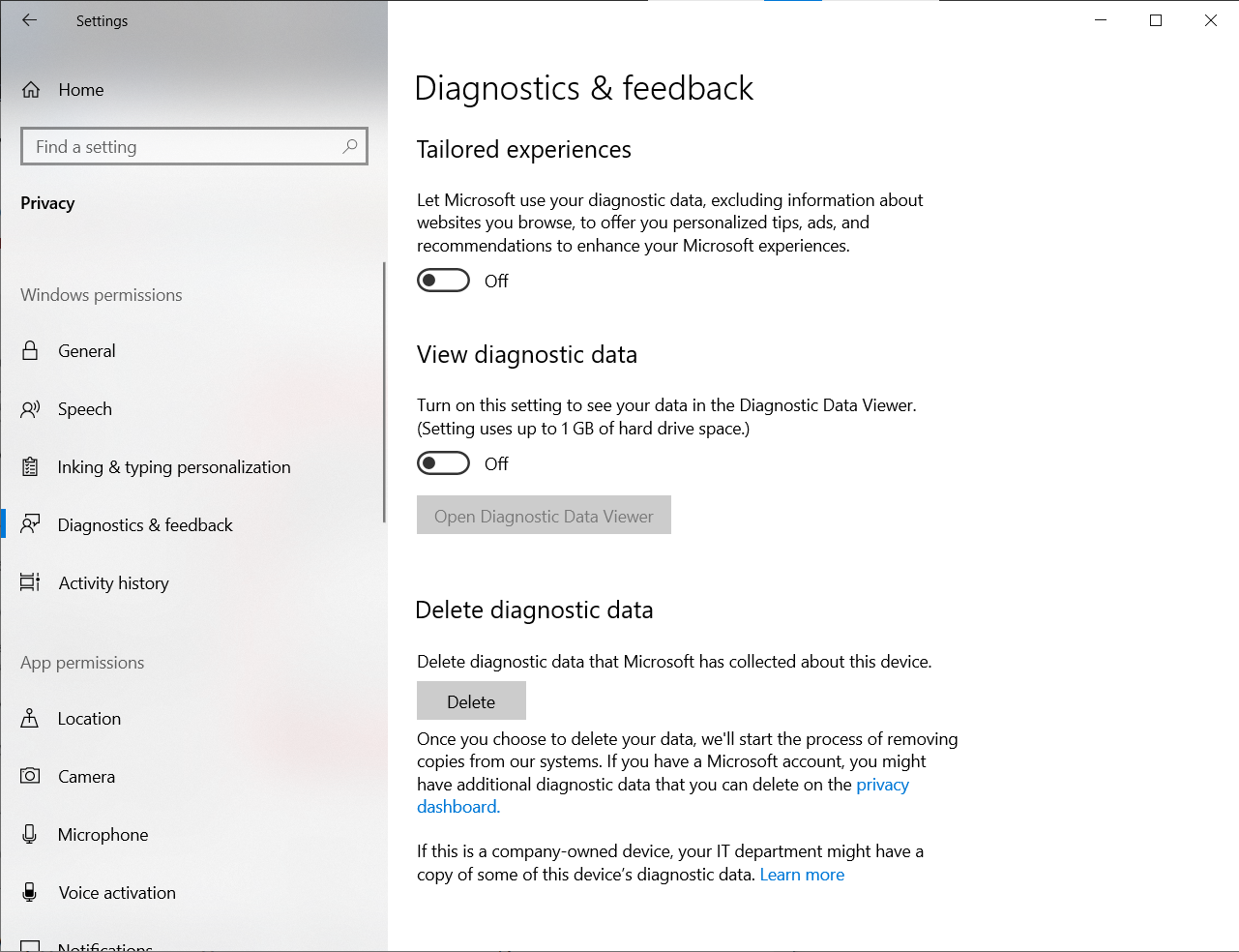
В разделе Персонализация ввода с клавиатуры отключаем эту настройку



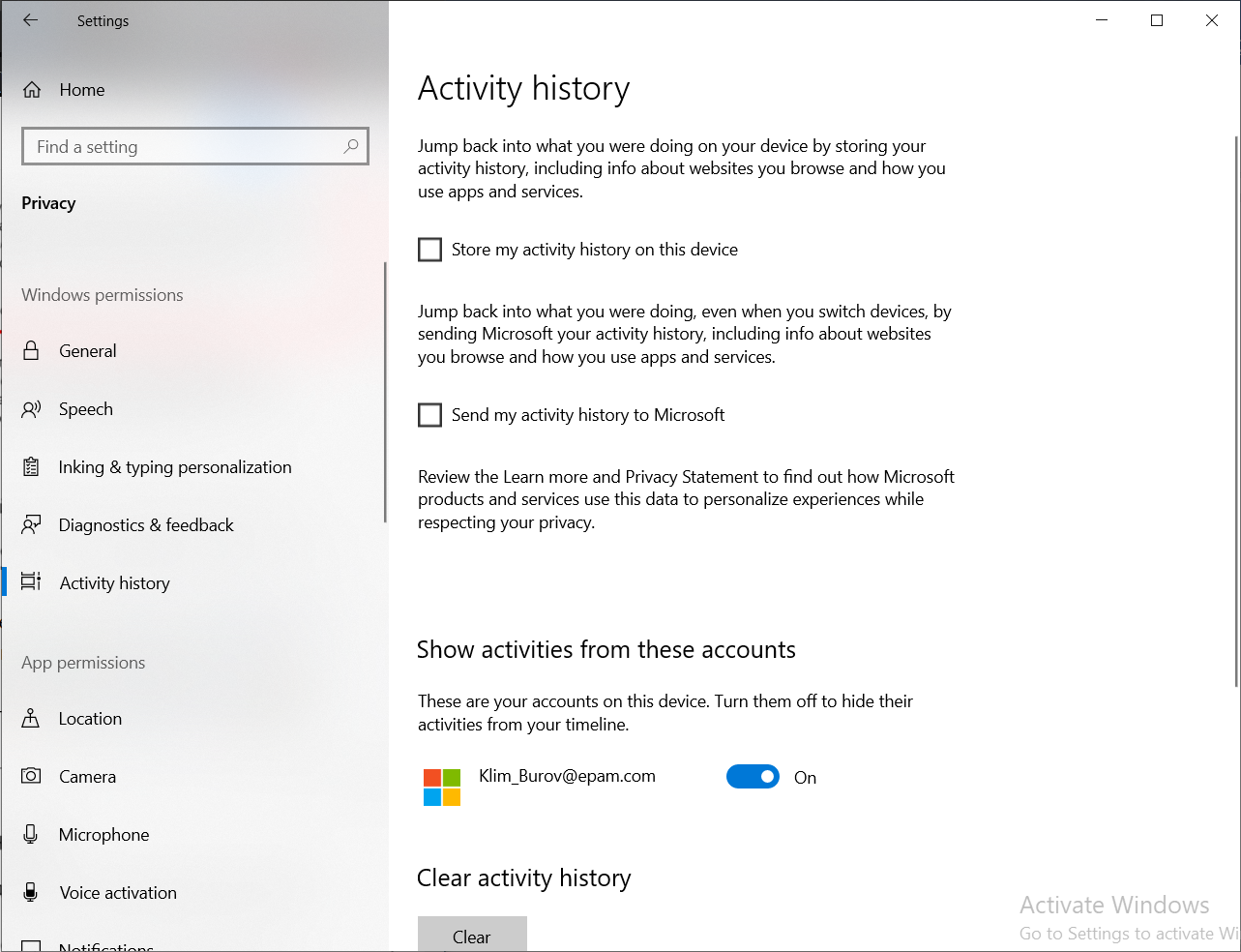
В разделе Диагностика выбираем отправку только основных данных



Также отключаем Персонализированные возможности и Просмотр диагностических данных (можно оставить) и удаляем сохраненные данные

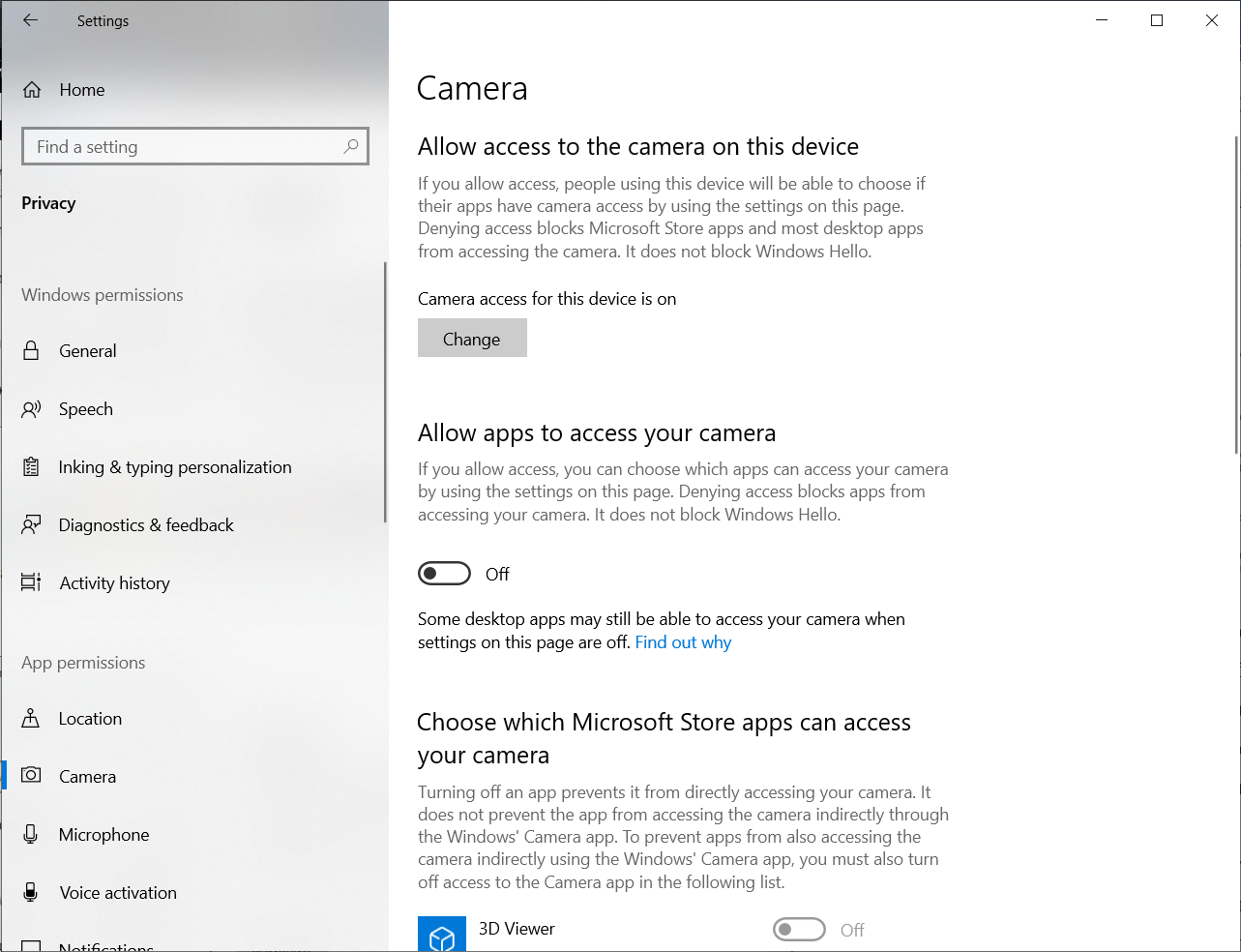


В разделе Журнал действий убираем галочки Сохранить журнал на устройстве и Отправить журнал в Microsoft

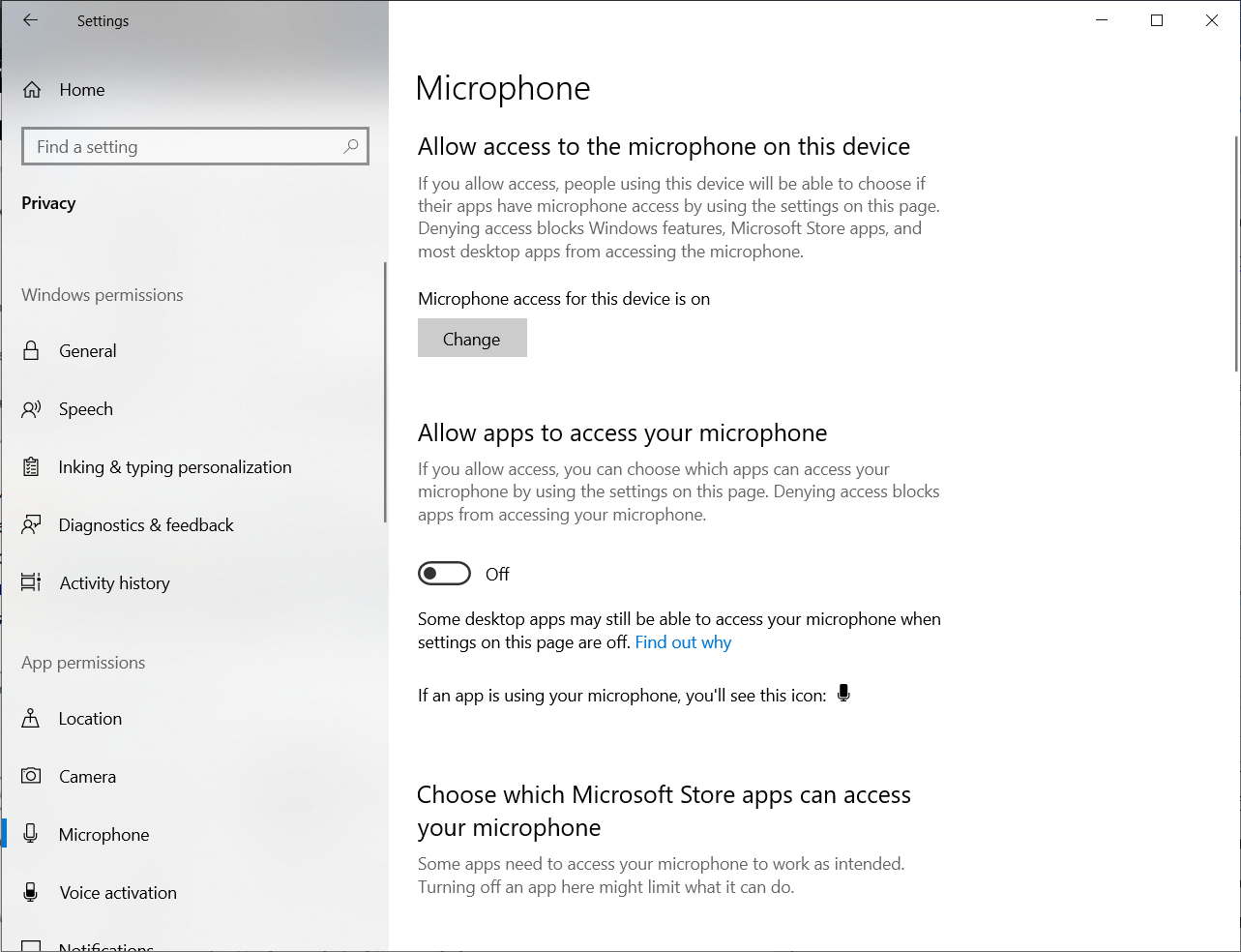


В разделе Расположение отключаем определение местоположения

В разделе Камера выключаем опцию Разрешить приложениям доступ к камере (приложения будут запрашивать доступ по необходимости)

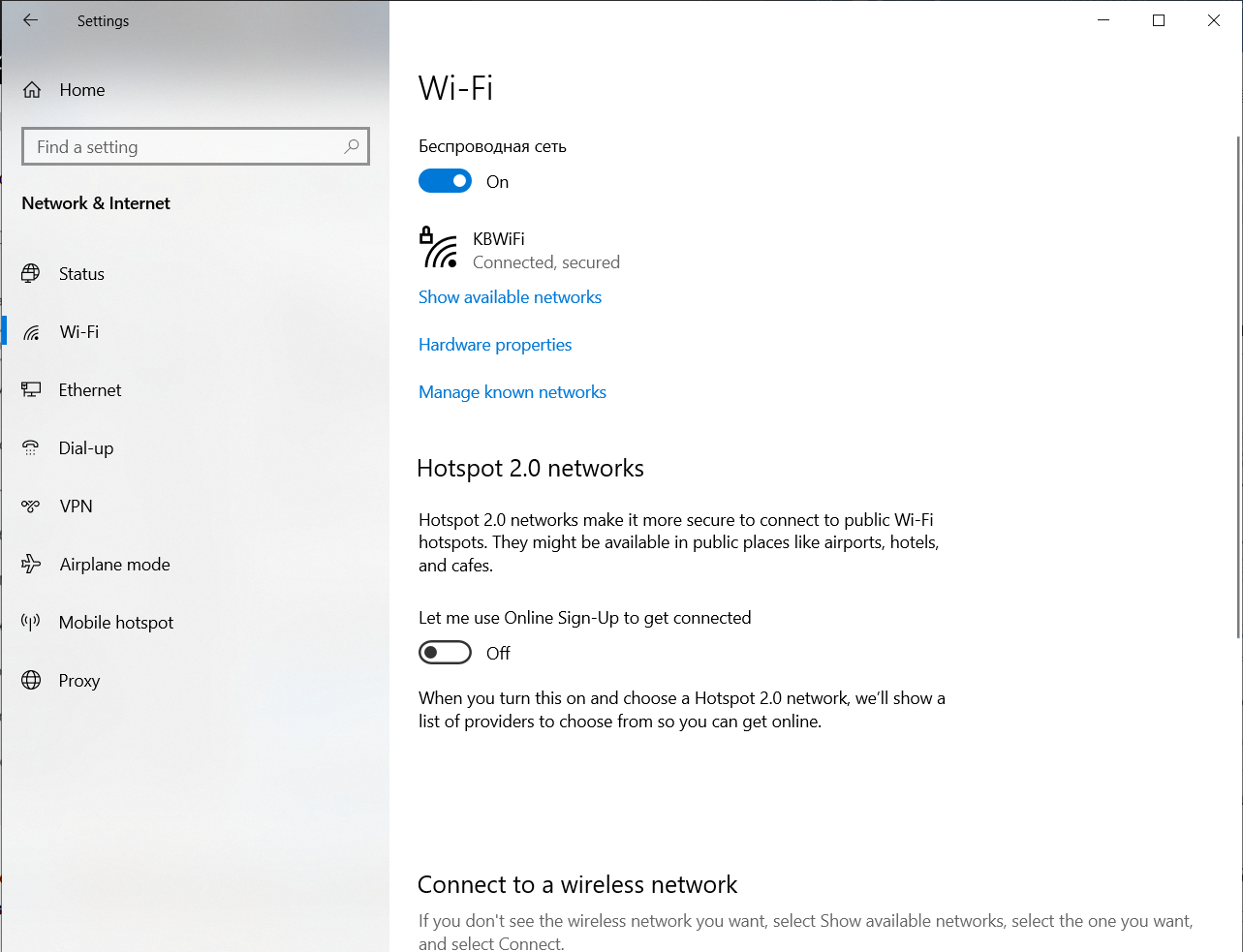


Аналогично поступаем с настройками микрофона

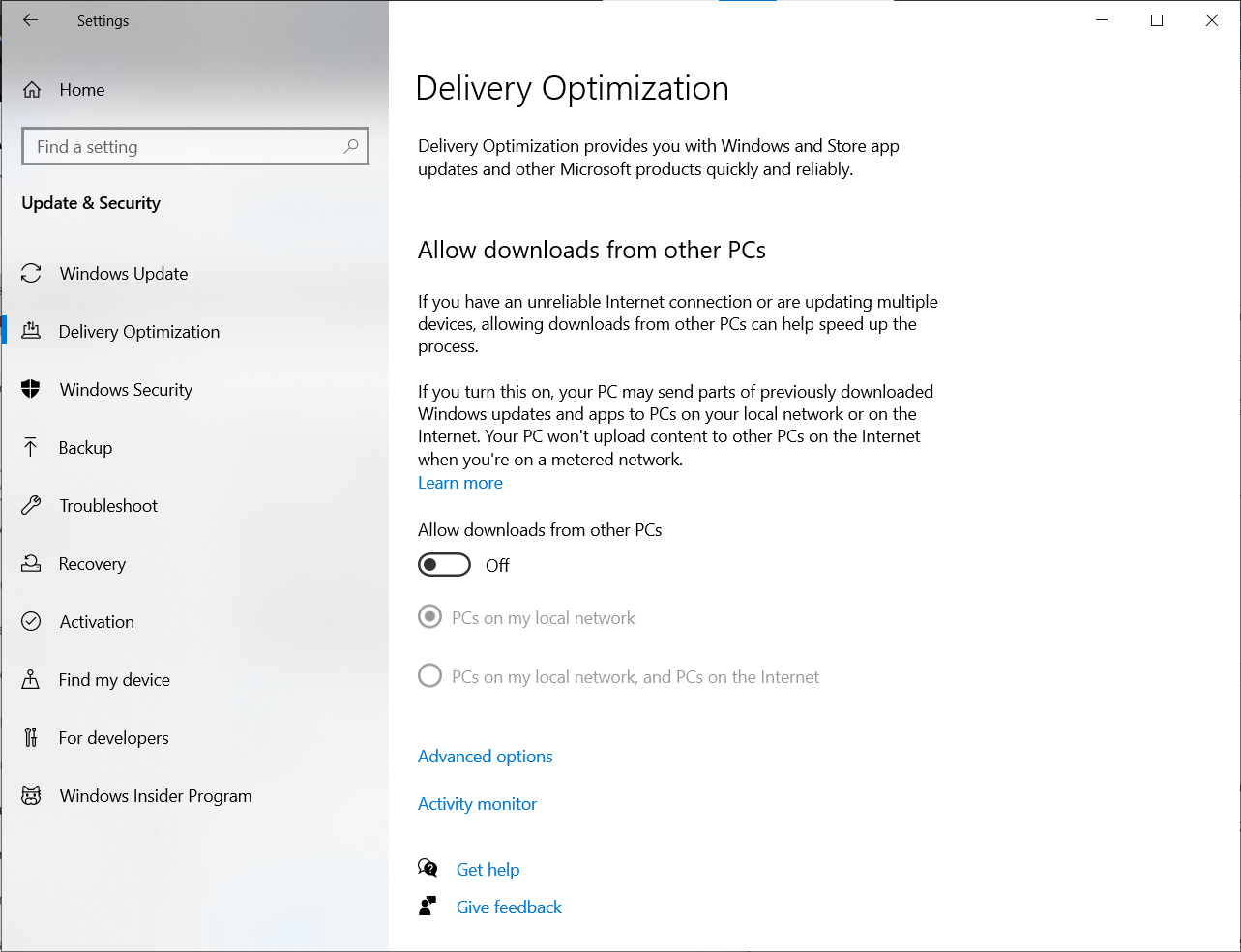


В последующих разделах также запрещаем доступ

В разделе Параметры –> Сеть и Интернет отключаем настройку Разрешить использовать веб-службу регистрации для подключения:



В разделе «Обновление и безопасность» нужно перейти на вкладку «Оптимизация доставки» и отключить настройку Разрешить загрузки с других компьютеров



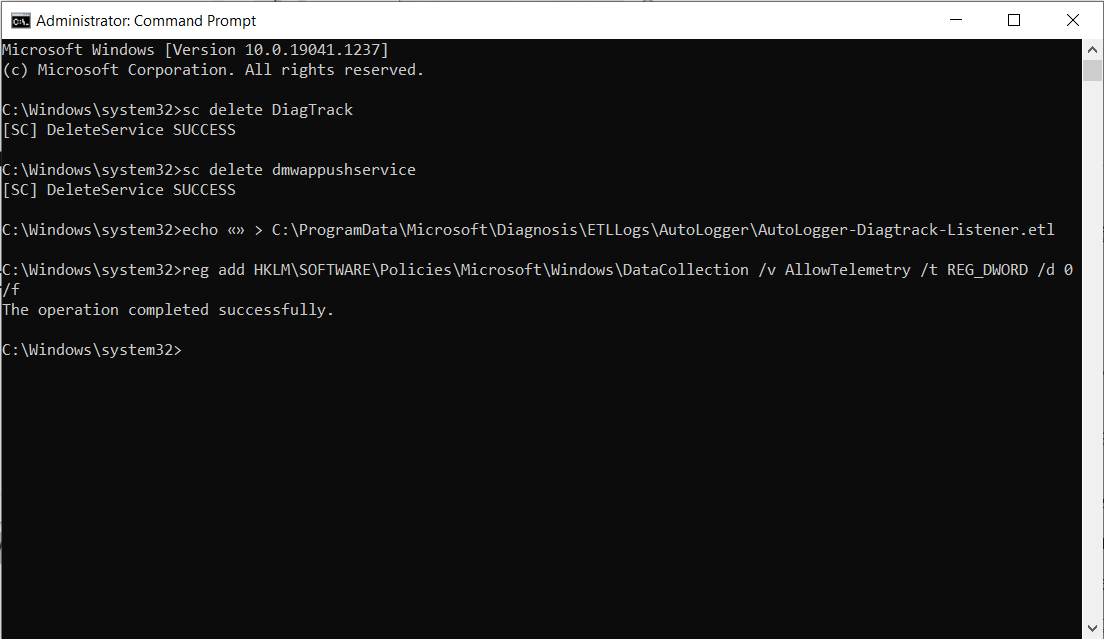
Отключим телеметрию. Для этого воспользуемся Командной строкой, запущенной от имени Администратора и введем следующие команды

sc delete DiagTrack

sc delete dmwappushservice

echo«»>C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl

reg add HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection /v AllowTelemetry /t REG\_DWORD /d 0 /f



Также отредактируем файл C:\Windows\System32\drivers\etc\hosts для блокировки доступа к серверам Microsoft. По причине того, что данный файл имеет приоритет в разрешении доменных имен перед DNS, то мы можем перенаправлять все запросы к серверам Microsoft обратно. Для этого в конец файла добавим следующие строки:

0.0.0.0 statsfe2.update.microsoft.com.akadns.net

0.0.0.0 fe2.update.microsoft.com.akadns.net

0.0.0.0 s0.2mdn.net

0.0.0.0 survey.watson.microsoft.com

0.0.0.0 view.atdmt.com

0.0.0.0 watson.microsoft.com

0.0.0.0 watson.ppe.telemetry.microsoft.com

0.0.0.0 vortex.data.microsoft.com

0.0.0.0 vortex-win.data.microsoft.com

0.0.0.0 telecommand.telemetry.microsoft.com

0.0.0.0 telecommand.telemetry.microsoft.com.nsatc.net

0.0.0.0 oca.telemetry.microsoft.com

0.0.0.0 sqm.telemetry.microsoft.com

0.0.0.0 sqm.telemetry.microsoft.com.nsatc.net

0.0.0.0 watson.telemetry.microsoft.com

0.0.0.0 watson.telemetry.microsoft.com.nsatc.net

0.0.0.0 redir.metaservices.microsoft.com

0.0.0.0 choice.microsoft.com

0.0.0.0 choice.microsoft.com.nsatc.net

0.0.0.0 wes.df.telemetry.microsoft.com

0.0.0.0 services.wes.df.telemetry.microsoft.com

0.0.0.0 sqm.df.telemetry.microsoft.com

0.0.0.0 telemetry.microsoft.com

0.0.0.0 telemetry.appex.bing.net

0.0.0.0 telemetry.urs.microsoft.com

0.0.0.0 telemetry.appex.bing.net:443

0.0.0.0 settings-sandbox.data.microsoft.com

0.0.0.0 watson.live.com

0.0.0.0 statsfe2.ws.microsoft.com

0.0.0.0 corpext.msitadfs.glbdns2.microsoft.com

0.0.0.0 compatexchange.cloudapp.net

0.0.0.0 a-0001.a-msedge.net

0.0.0.0 sls.update.microsoft.com.akadns.net

0.0.0.0 diagnostics.support.microsoft.com

0.0.0.0 corp.sts.microsoft.com

0.0.0.0 statsfe1.ws.microsoft.com

0.0.0.0 feedback.windows.com

0.0.0.0 feedback.microsoft-hohm.com

0.0.0.0 feedback.search.microsoft.com

0.0.0.0 rad.msn.com

0.0.0.0 preview.msn.com

0.0.0.0 ad.doubleclick.net

0.0.0.0 ads.msn.com

0.0.0.0 ads1.msads.net

0.0.0.0 ads1.msn.com

0.0.0.0 a.ads1.msn.com

0.0.0.0 a.ads2.msn.com

0.0.0.0 adnexus.net

0.0.0.0 adnxs.com

0.0.0.0 az361816.vo.msecnd.net

0.0.0.0 az512334.vo.msecnd.net

0.0.0.0 ssw.live.com

0.0.0.0 ca.telemetry.microsoft.com

0.0.0.0 i1.services.social.microsoft.com

0.0.0.0 i1.services.social.microsoft.com.nsatc.net

0.0.0.0 df.telemetry.microsoft.com

0.0.0.0 reports.wes.df.telemetry.microsoft.com

0.0.0.0 cs1.wpc.v0cdn.net

0.0.0.0 vortex-sandbox.data.microsoft.com

0.0.0.0 oca.telemetry.microsoft.com.nsatc.net

0.0.0.0 pre.footprintpredict.com

0.0.0.0 spynet2.microsoft.com

0.0.0.0 spynetalt.microsoft.com

0.0.0.0 fe3.delivery.dsp.mp.microsoft.com.nsatc.net

0.0.0.0 cache.datamart.windows.com

0.0.0.0 db3wns2011111.wns.windows.com

0.0.0.0 settings-win.data.microsoft.com

0.0.0.0 v10.vortex-win.data.microsoft.com

0.0.0.0 win10.ipv6.microsoft.com

0.0.0.0 ca.telemetry.microsoft.com

0.0.0.0 i1.services.social.microsoft.com.nsatc.net

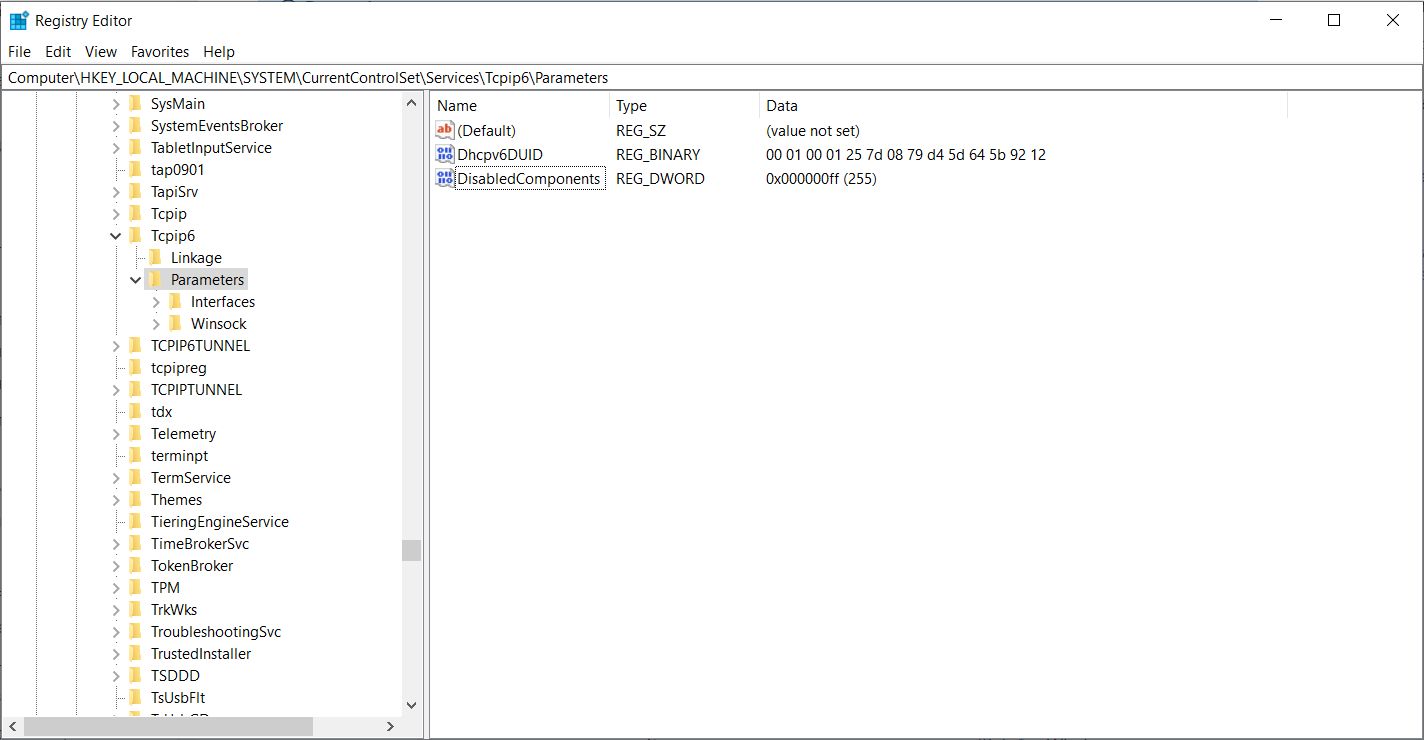
После сохранения файла очистим DNS-кэш. Для этого запустим Командную строку и выполним команду: ipconfig /flushdns

Также отключим использование IPv6 с помощью реестра. Для этого необходимо перейти по ключу HKEY\_LOCAL\_MACHINE\SYSTEM\ CurrentControlSet\Services\Tcpip6\Parameters\ и добавить следующий параметр

Имя: DisabledComponents

Тип: REG\_DWORD

Значение: 0xFF (отключено IPv6)



Продолжим настройку доверенной среды сторонними средствами. Для решения данной задачи была выбрана программа Dr.Web Security Space 12.0, так как она предоставляет все возможности, необходимые для создания доверенной среды, имеет удобный интерфейс и позволяет экспортировать заданные настройки для дальнейшего их переиспользования.

После включения интерактивного режима появляются события (рисунок 1). В уведомлении о событии отображается название самого процесса, путь до исполняемого файла, название удаленного процесса, дата создания, размер, цифровая подпись и предлагается выбор действия.

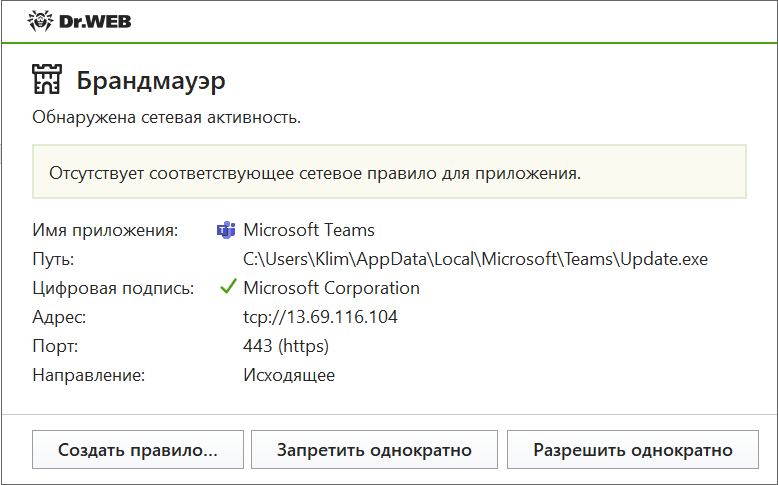


Рисунок 1. Пример события

Для приложений WinWord.exe. Outlook.exe и Excel.exe были созданы системные запреты (рисунок 2).

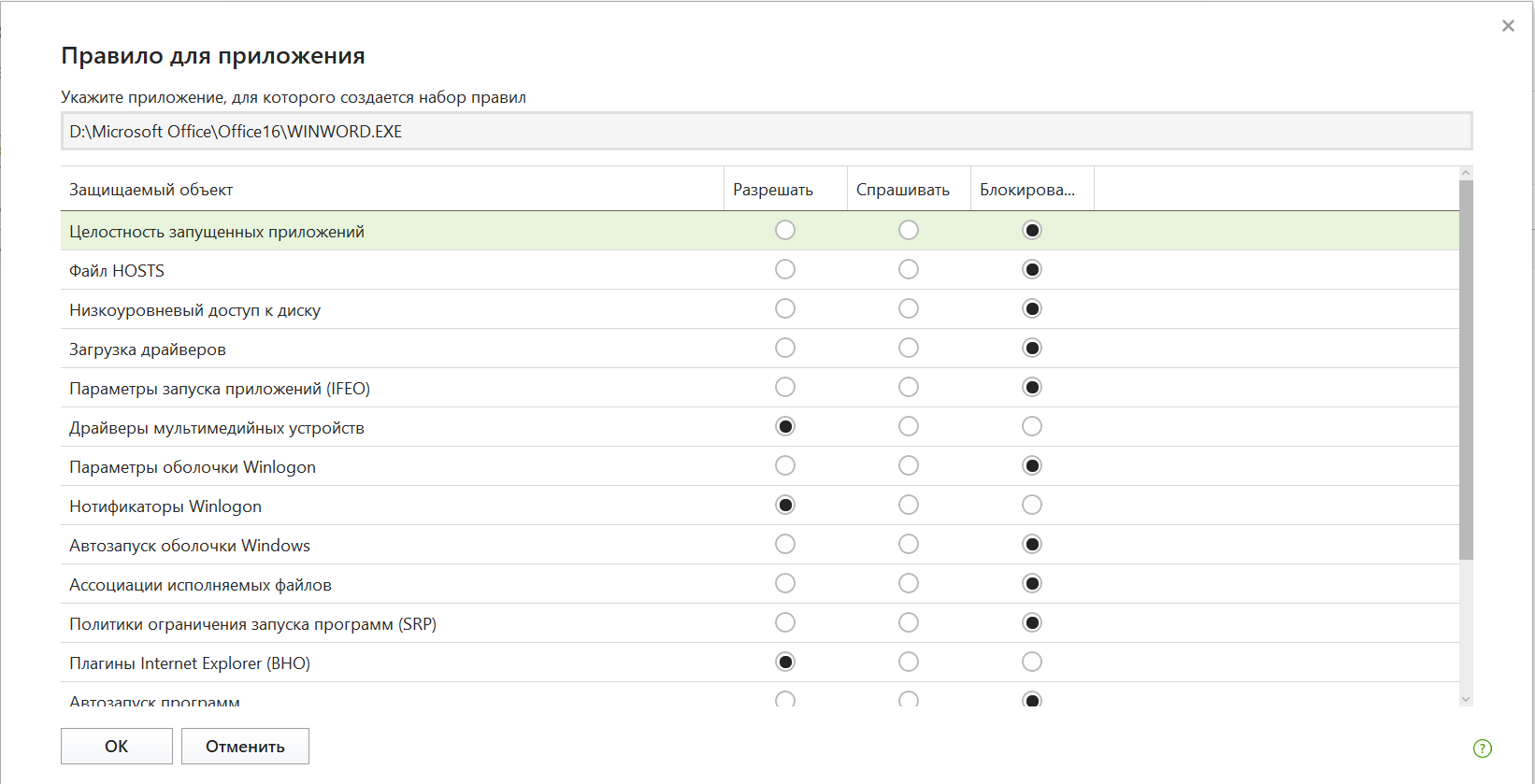


Рисунок 2. Создание системных запретов

Часть таблицы с описанием настроенных сетевых правил и системных запретов приведена в приложении А, полная таблица в отдельном файле.

**Вывод**

В процессе выполнения лабораторной работы была создана доверенная среда на АРМ, посредством настройки операционной системы и задания сетевых правил и системных запретов для исполняемых процессов с помощью стороннего программного обеспечения. Был получен опыт настройки служб Windows, сетевых правил операционной системы, ключей реестра Windows, параметров аккаунта и создания доверенной среды с помощью программного обеспечения Dr.Web Security Space 12.0. При отключении ненужных служб и настройке параметров пользователя на отключение сбора статистик, данных и телеметрии значительно сократилось количество сетевых соединений и возросла производительность АРМ.

Приложение А



