Настройка системы

Анонимность в сети невозможна без контроля уникальных идентификаторов системы. В каждой системе есть уникальные идентификаторы, которые по отдельности или в купе могут точно указать на пользователя. Они могут использоваться для отслеживания системы на разных уровнях. Всего я могу выделить **3 уровня подобных настроек**:

- Уровень браузера.
- Уровень операционной системы
- Уровень оборудования.

Так же в системе и браузере есть функции, которые могут приводить к утечке реальных данных(например реального IP)

Сегодня разговор пойдёт о анонимности на последних двух уровнях - операционной системе и прикладном уровне. Их часто оставляют в стороне и делают акцент только на безопасности браузера, что сильно упрощает настройку, но создаёт большую потенциальную дыру в безопасности. На самом деле первые шаги в сторону безопасности операционной системы были уже нами предприняты: мы её переустановили на чистую версию, чтобы быть уверенным, что в системы изначально нет вирусов, и зашифровали. Шифрованием преследуются сразу две цели: 1) Защита всех данных, в том числе и системных логов, паролем. 2) Шифрование всего диска защищает данные от подмены или добавления. Если зашифрован весь диск, то трюк с закидыванием кем-то вредоносного ПО на не зашифрованный раздел становится неактуальным.

На данный момент система хорошо защищена от воздействий извне. Теперь можно не бояться за данные пока система в выключенном состоянии: что бы там не лежало, оно под надёжной защитой пароля. Текущая цель - защитить уникальные идентификаторы во время работы в системе.

Уровень операционной системы

Какие основные идентификаторы есть в операционной системе?

Mac address -- уникальный идентификатор сетевой карты. Используется для определения сетевого устройства, содержит в себе данные о производителе компонента и его уникальный ID. Виден всем устройствам в локальной сети и провайдеру.

GUID -- уникальное значение в реестре windows. Оно генерируется при установке системы и приложения имеют свободный доступа к нему.

Компоненты -- в системе есть информация о всех её компонентах и подключённых устройствах. У многих компонентов есть серийные номера, которые могут использоваться для отслеживания

Hostname и **Username** -- задаются при установки системы и используются в большом количестве программ для идентификации пользователя.

Модель процессора и материнской платы -- это своего рода mac address. Много компонентов в системе имеют уникальные номера. В VirtualBox эта проблема решена виртуальными компонентами.

Ключ активации windows -- при регистрации windows в системе остаются такие уникальные параметры как ключ и имя владельца. Ситуация усугубляется, если активировать оформленным на себя ключом.

Это далеко не полный список. Основная проблема заключается в том, что контролировать абсолютно всё в реальной системе невозможно, поэтому для работы будет использоваться виртуальная машина. Но произвести базовую настройку самой системы надо, чтобы обезопасится от основных угроз анонимности.

Основные угрозы анонимности

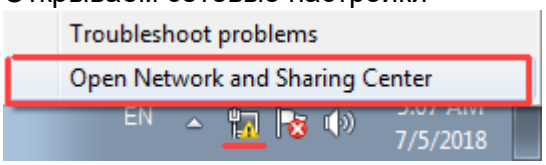
Настройки безопасности, связанные с интернетом, надо обновлять при обновлении способа подключения машины к сети. Например, если поменялся VPN, то надо обновить и DNS к нему. Если на данный момент конфига пока нет, настройки сети надо отложить до его появления.

DNS LEAK

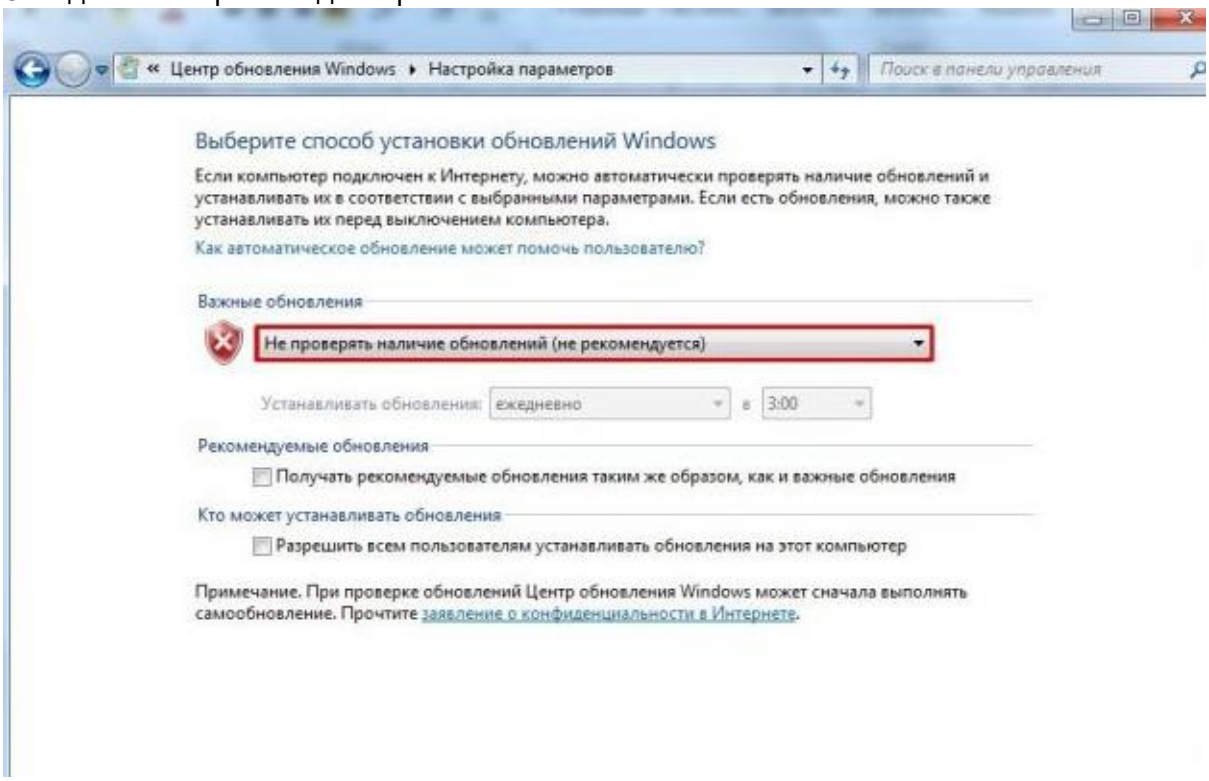
Или по простому *утечка DNS*. В понимании многих людей DNS - это просто сервер, который сопоставляет доменные имена, -- facebook.com, например, -- с IP адресами серверов, на которых эти сайты размещаются. Это не полная картина. DNS это целая сеть серверов, и иногда запрос на получение доменного имени не заканчивается на первом сервере(данных для ответа на нём может не быть), а передаётся на сервера более высокого порядка. И в чём тут подвох? Да в том, что если запрашивается поддомен какого-то сайта, то для ответа о его IP запрос может быть перенаправлен на DNS сервер самого сайта. На основе этого и работает DNS leak: он направляет браузер на свой поддомен, ссылку на которой генерирует отдельно для каждого запроса. Таким образом IP поддомена точно нет в кешах и DNS запрос доходит до DNS сервера сайта, на котором происходит отслеживает, с какого IP был запрос. В редких случаях в роли DNS сервера первого порядка выступает роутер(про такую возможность надо просто знать, на практике без настроек таких эпичных огрех в безопасности не добиться), тогда утекает основной IP машины. В подавляющих большинстве случаев получается узнать только DNS сервер, которым пользуется человек. Мало того, что это раскроет страну, так еще и для идентификации пользователя использоваться может.

При использовании обычного прокси без remote DNS(его только прокси типа socks5 поддерживают), машина уязвима к DNS leak. Более того, DNS leak иногда случается и с включённым VPN. Самый надёжный способ победить его -- использовать виртуализацию, но об этом потом. А на основной машине надо настроить используемый DNS сервер:

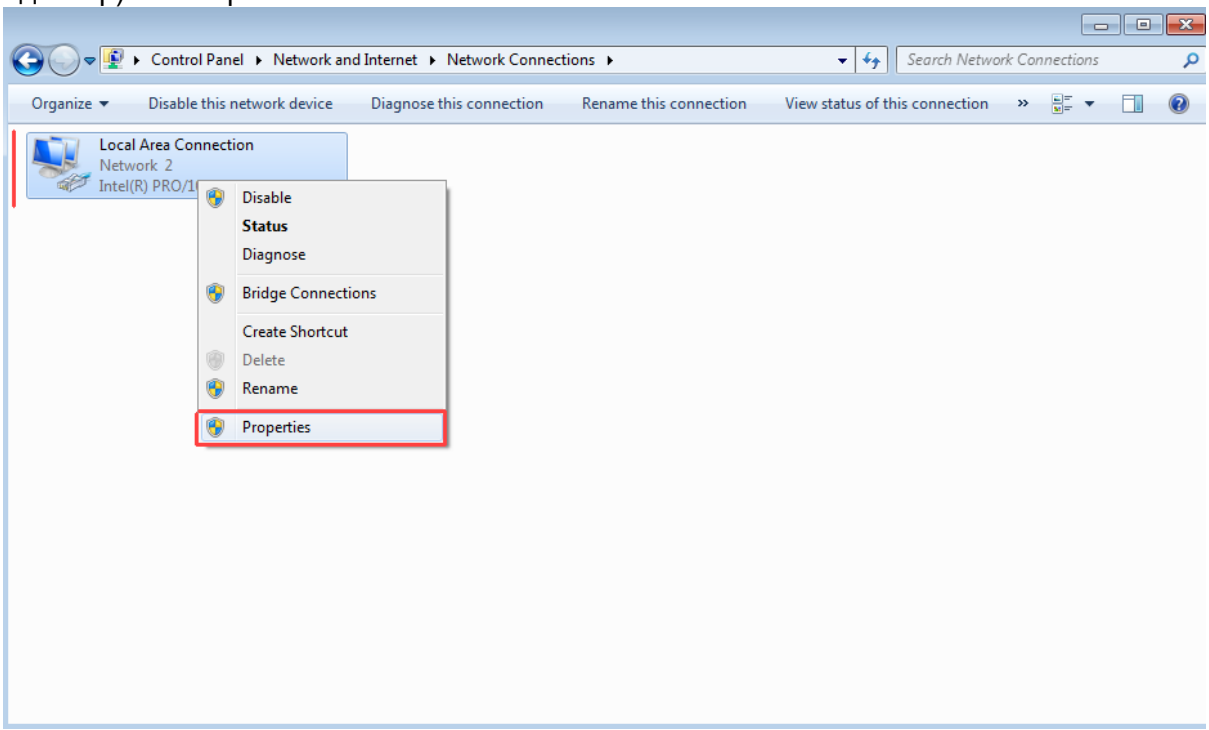
- Открываем в браузере https://whoer.net чтобы узнать в какой стране находится выход VPN
- Заходим на https://public-dns.info. Выбираем страну из предыдущего пункта и из списка внизу и подбираем 2 любых DNS с хорошим рейтингом
- Открываем сетевые настройки



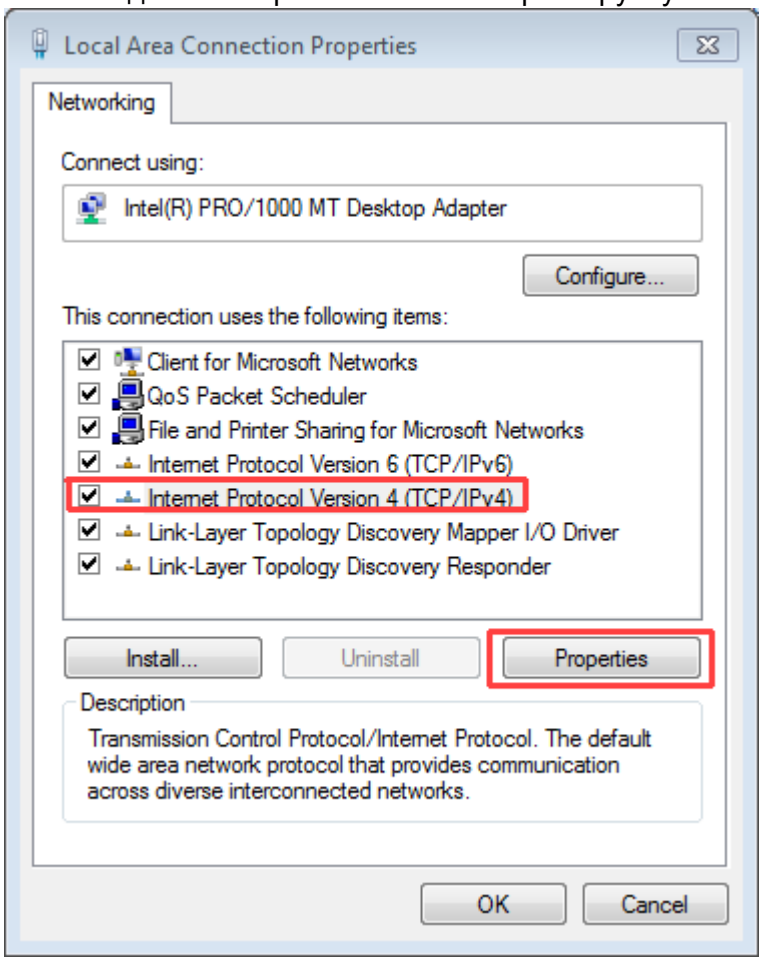
- Заходим в настройки адаптера



- Кликаем правой кнопкой мыши по адаптеру со словом tap в описании(это VPN адаптер) и выбираем свойства

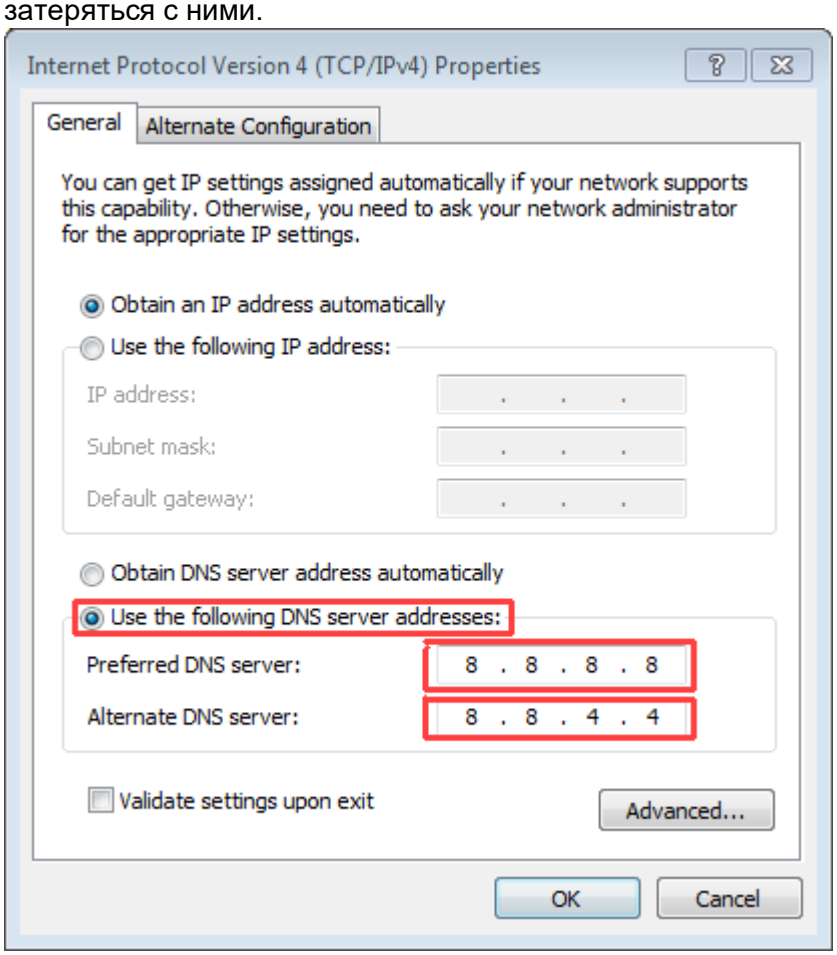


- Там заходим в настройки IPv4 и выбираем ручную настройку DNS.



- Вводим туда данные двух DNS серверов из шага выше.
- Для адаптера модема который был изначально ставим первый DNS сервер 8.8.8.8, а второй 8.8.4.4. Это сервера google, они самые популярные и проще

затеряться с ними.



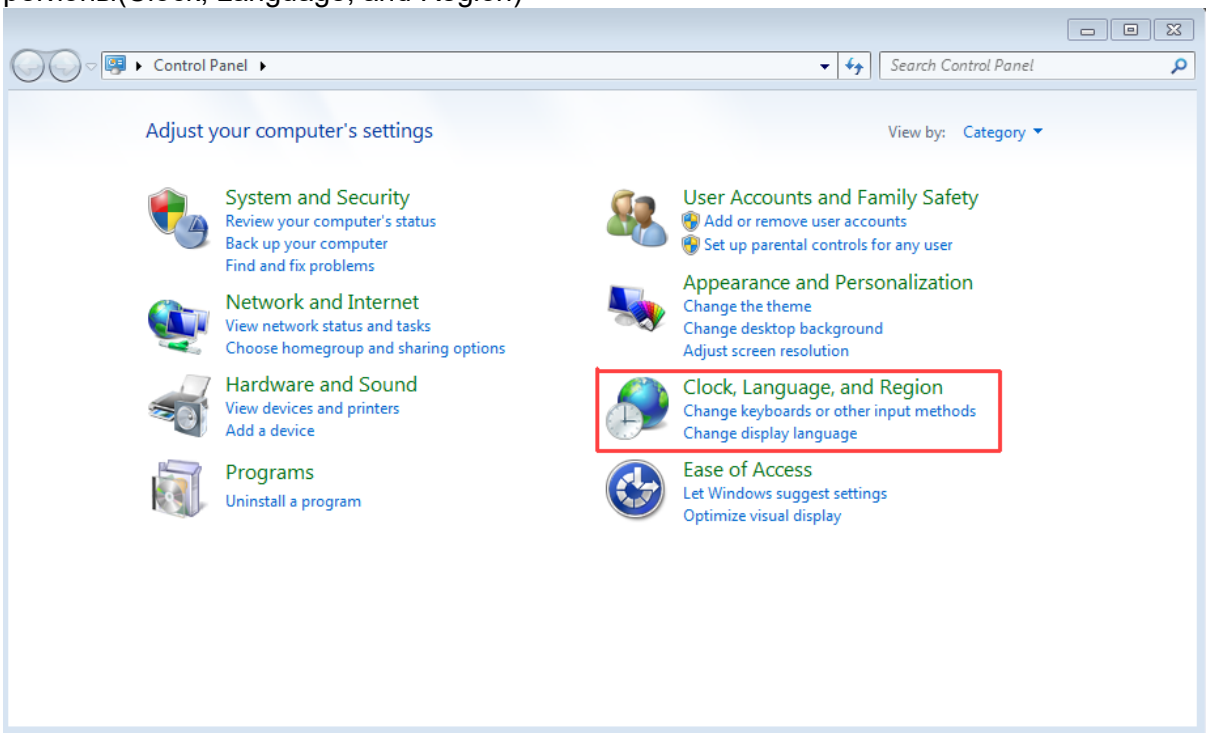
Time и **timezone**

Во многих сетевых протоколах(и в браузере) на сервере доступны такие параметры как системное время и часовой пояс. Вычислять человека по часовому поясу в голову никому не придёт, но если время отличается от установленного часового пояса или часовой пояс не соответствует стране по IP, то некоторые сайты могут заподозрить в использовании средств анонимизации. А вот часы в системе имеют свойства спешить или отставать. Можно хоть 100 раз IP поменять и переустановиться раз 200, но если есть значимое отклонение от эталонного времени, то на небольшом сайте с можно будет с большой точностью собрать все запросы одного пользователя.

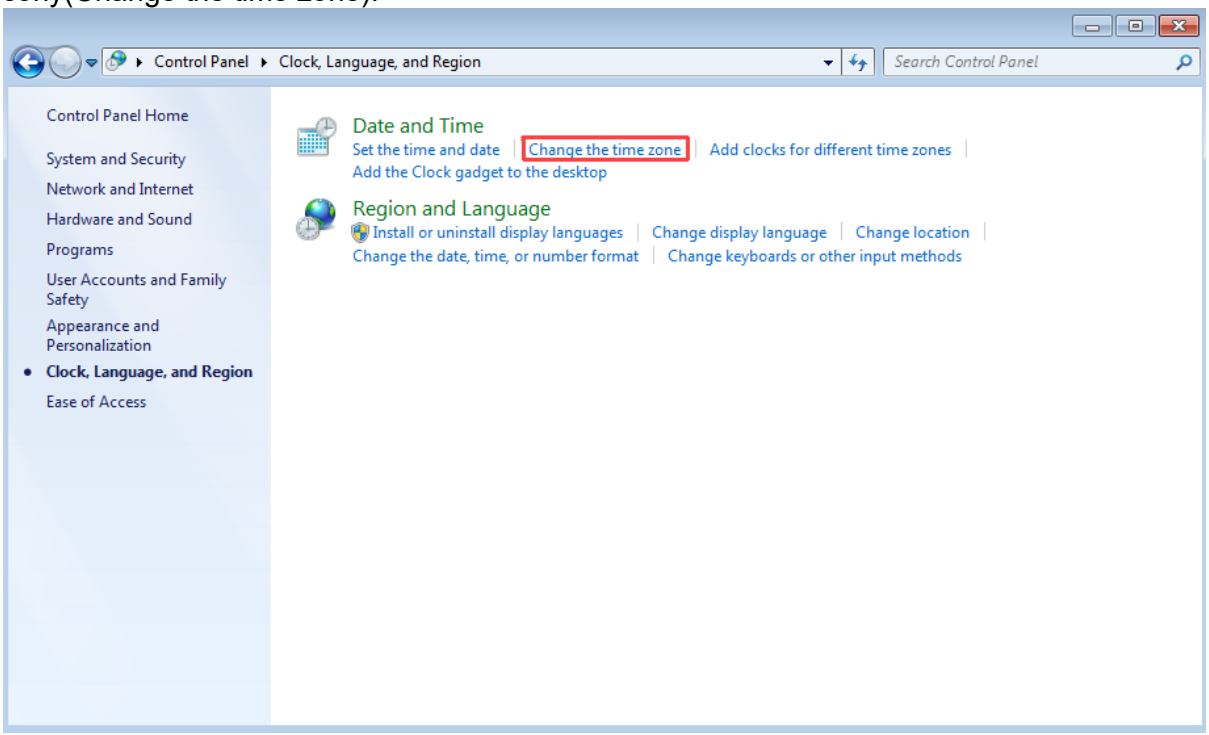
Решение -- настроить системные часы по часовому поясу VPN и синхронизировать время с интернетом, чтобы не было ярко выраженной разницы с интернет часами.

- По сайту https://whoer.net определяем страну выхода VPN.

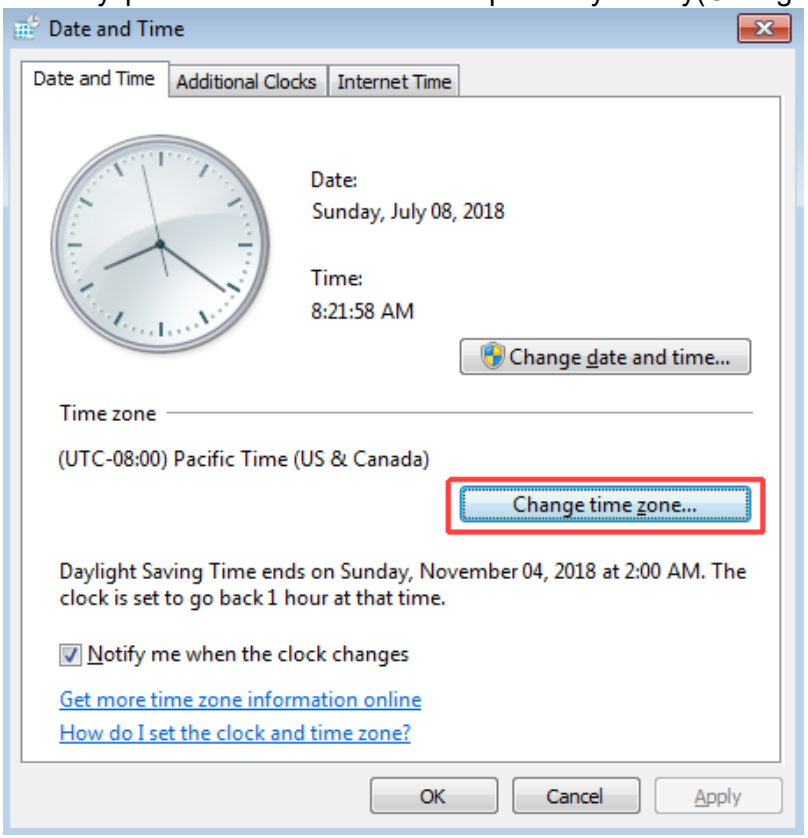
- В панели управления(control panel) windows открываем пункт Часы, языки и регионы(Clock, Language, and Region)



- Там в секции Дата и Время(Date and Time) нажимаем на Изменить временную зону(Change the time zone).



- Там внутри есть кнопка Изменить временную зону(Change time zone)



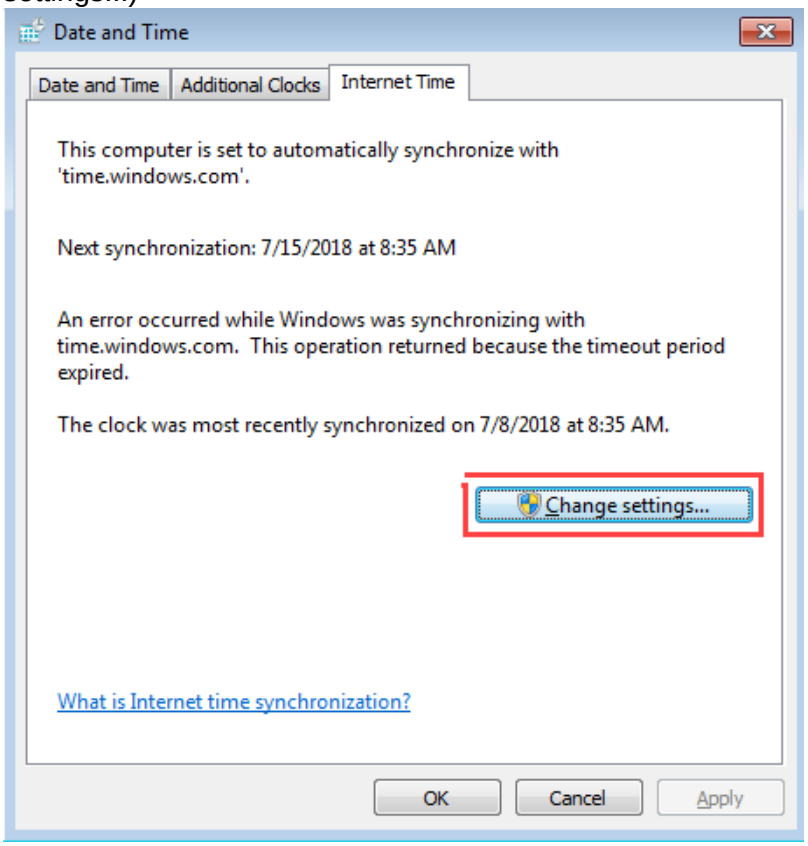
- Из списка выбираем страну, которую показывает как страну нахождения с включенным VPN. Галочка автоматического перехода на зимнее/летнее время должна стоять

Системное время

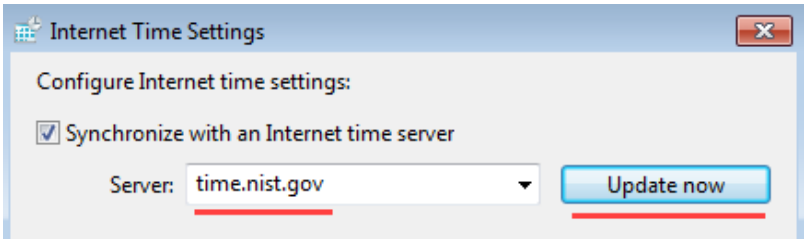
Оно должно быть синхронизировано через ntp сервер чтобы устранить большие расхождения. В windows такой функционал есть, но без настройки синхронизироваться нормально не получится.

- Опять заходим в панель управления - Clock, Language, and Region - Change the time zone как в шагах выше.

- Переходим во вкладку Internet Time и жмём там Изменить настройки(Change settings...)



- Туда вводим любой NTP сервер(time.nist.gov, например) и нажимает Обновить сейчас.



Камера

Если для работы камеры требуются дополнительные драйвера, то для отключения достаточно их просто не устанавливать.

Иногда настройки встроенной в ноутбуки камеры находятся в BIOS. Надо проверить там, нет ли пункта для отключения камеры.

Если методами выше не удалось отключить камеру, тогда в пуске ищем Device Manager(Диспетчер Устройств), в нём во вкладке Imaging devices(Устройства обработки изображений) должна быть камера. Надо правой кнопкой мыши выбрать её и нажать Disable(Отключить).

Проверить, доступна ли камера в системе можно на этом сайте https://webcamera.io/

Для linux камера и микрофон отключается через блокировку соответствующих драйверов. При этом на сайте эти устройства всё ещё продолжает определять.

Микрофон

Из пуска открываем Control Panel(Панель управления), там переходим в Hardware and Sound(Оборудование и Звук), там открываем Sound(Звук) и во вкладке Recording(Запись) будет микрофон. Нажимаем правой кнопкой мыши по нему и выбираем Disable(Отключить). Проверить результат можно на том же сайте https://webcamera.io/

При правильной настройке там должно быть написано

No camera or microphone found. Unable to continue.

Микрофон и камеру было бы неплохо еще заклеить непрозрачным скотчем.

Firewall

Это страховка на случай, если с VPN что-то будет не так. Разрывы связи бывают всегда, нельзя исключать и программных ошибок. Поэтому к падением VPN надо подготовится заранее. Обычно в таких ситуациях трафик продолжает идти напрямую в интернет, что является громадной угрозой для анонимности. Firewall - решение, которое предотвратит утечку и перекроет интернет трафик, который попытается пойти в обход VPN.

Скачайте архив с конфигуратором firewall.

[скачать]

В архиве 2 файла, их для удобства лучше разархивировать на рабочий стол.

Файл **firewall.bat** служит для активации блокировки трафика в обход firewall. Его достаточно запустить один раз, действие сохраняется и после перезапуска системы. После запуска скрипта появится напоминание, что требуются админ-права. Надо просто нажать enter, по окончанию конфигурации окно с firewall само закроется.

Любой из этих двух скриптов надо запускать от имени администратора

Файл **disable_firewall.bat** нужен для разрешения трафика в обход VPN. Если надо отключиться от VPN или не удаётся соединиться с VPN и надо осознанно выйти в сеть для решения проблемы, тогда запускается этот скрипт от имени администратора, и доступ в сеть без VPN возобновляется. Лучше держать этот файл у себя на рабочем столе, чтобы не потерять его на случай проблем с подключением.

Для нормальной работы firewall надо установить у текущего подключения тип сети как "Домашняя сеть". Для этого открываем **Центр Управления Сетями Windows(Network and Sharing Center)**, там есть раздел **Просмотр активных сетей**, в котором есть одна сеть. Если там написано **Home network(Домашняя сеть)**, то тип сети уже выставлен правильно. Иначе надо нажать по надписи с типом сети и выбрать из списка домашнюю сеть. Для windows 10 процесс отличается, о нём можно прочитать здесь.

Если не получается установить тип сети домашняя сеть, значит надо установить драйвера для модема, через который сейчас осуществляется выход в интернет, в систему.

Телеметрия в windows

Для отключения телеметрии есть решение с открытым кодом DWS. Надо его загрузить и установить. В результате его работы отключается все известные на данный момент подозрительные функции window. Чтобы избежать ошибку при настройке надо во второй вкладке Settings активировать снизу галочку **Enable professional mode**. После чего снять галочку напротив **Delete GWX**. Это рекламный модуль windows, который они использовали для агитации установки windows 10(да-да и такое было), но они прекратили его распространение, и сейчас его уже нет в системах.

После этой настойки можно запустить программу главной кнопкой с первой вкладки **Main**. Перед этим лучше убедиться, что бекап самых важных файлов уже создан где-то. В систему вносятся достаточно агрессивные изменения, и есть небольшой шанс поломки системы. Программа применительна как для win7 так и для win10.

Настройка требуется только для основной windows системы. Виртуальные системы отдельно не настраиваются.

Выглядит это таким образом:

Уровень оборудования

Доступ в интернет может осуществляться через модем или роутер. И то, и то является последним звеном в интернет цепочки перед компьютером. К модему может подключиться только одно устройство, а роутер может держать много подключений(как по проводу, так и через wi-fi). Обычно отличить можно так: если можно раздавать сеть по wi-fi -- роутер(или модем-роутер), нельзя -- модем.

Почему это важно? -- потому что в случае использования роутера именно он поддерживает соединение и обрабатывает поступающие данные. Так же он решает, что делать с входящими соединениями(модем просто передаёт всё на компьютер). В этом есть свои плюсы(можно на уровне роутера отсекать все входящие соединения) и минусы(с безопасностью у них проблемы. Стандартные пароли типа admin-123456 не редкость, и ошибки в прошивках регулярно обнаруживаются).

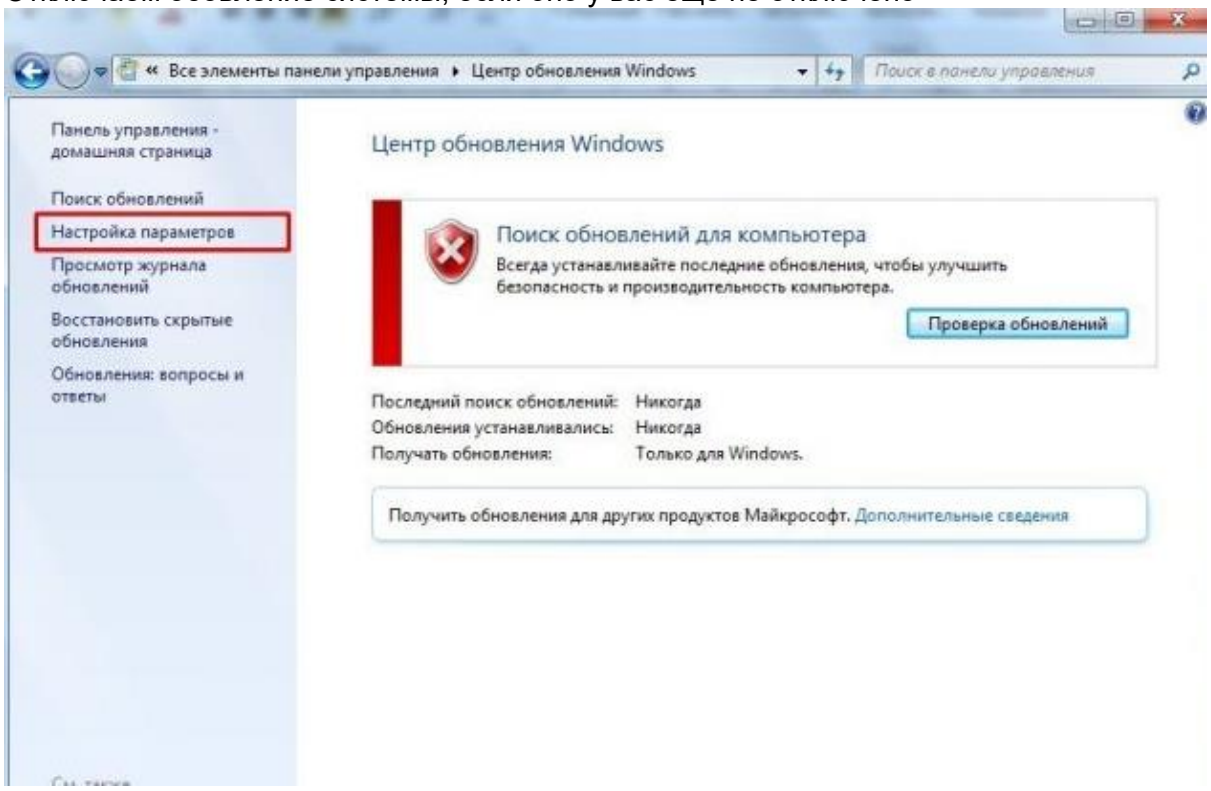
Поскольку в модеме который подключается напрямую, никаких дополнительных функций в нём нет, и его дополнительная настройка не требуется.

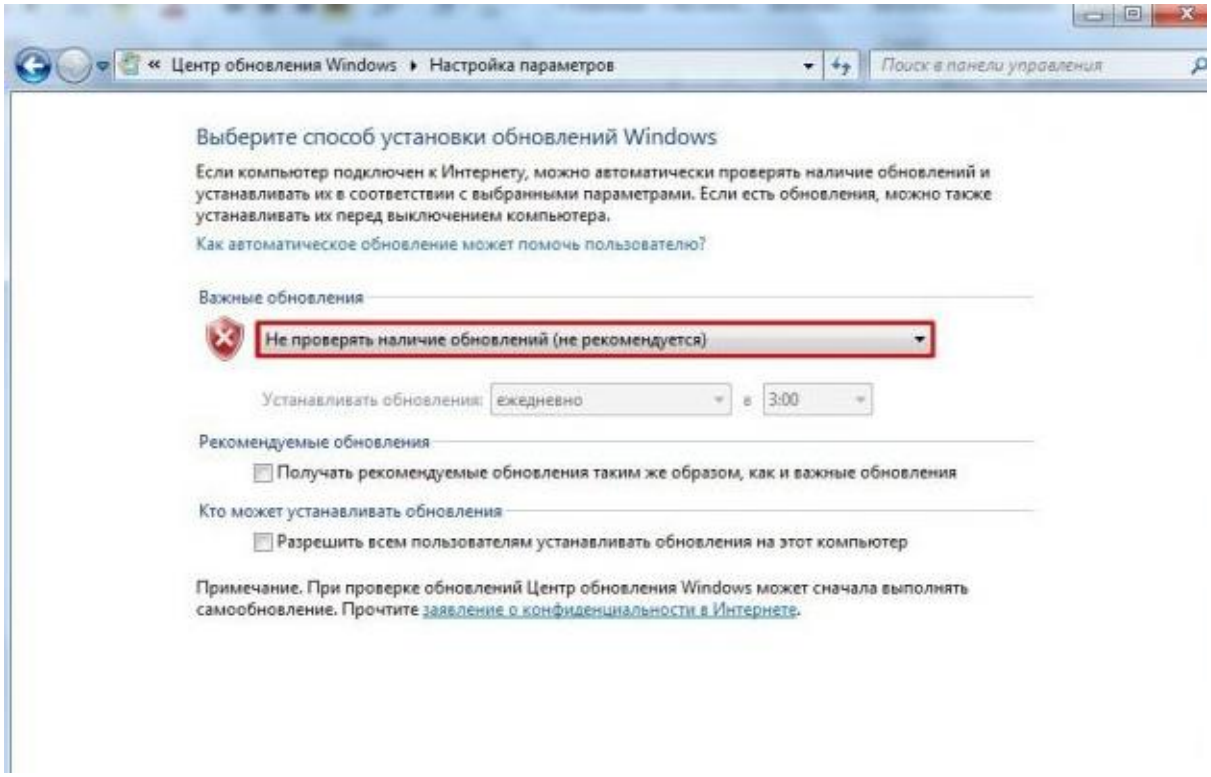
В случае с роутером надо убедиться, что он обновлён и не выставлено лишних настроек. Для этого надо зайти в его настройки(они доступны через браузер, обычно адрес и данные для входа пишут на коробке или в мануале). Первое, что нужно сделать - проверить наличие обновлений и обновиться, если они есть. Затем надо поменять стандартный пароль(даже если это не admin - admin, всё равно лучше сменить. Зачастую заводские пароли не до конца случайные). И надо настроить DNS на роутере. Если там можно его задать, то следует вписать в качестве DNS серверов DNS google - 8.8.8.8 и 8.8.4.4. Затем надо просто просмотреть пункты настроек на предмет нежелательных функций. Это может быть, например, отправка статистики провайдеру, доступ к админке через интернет, любое логирование и т.п.

Продолжая настройку системы, необходимо будет прозвести некоторые действия дляотключения телеметрии и слежки. Это делается для тех целей, чтоб не оставлять нигде свои следы. Вся работа в любом случае будет реализована через виртуальные машины и настоящие параметры засвечены не будут, но в любом случае основная машина тоже будет использоваться для разных целей, к примеру браузер для поиск какой либо информации, возможно переписки с партнерами и так далее.

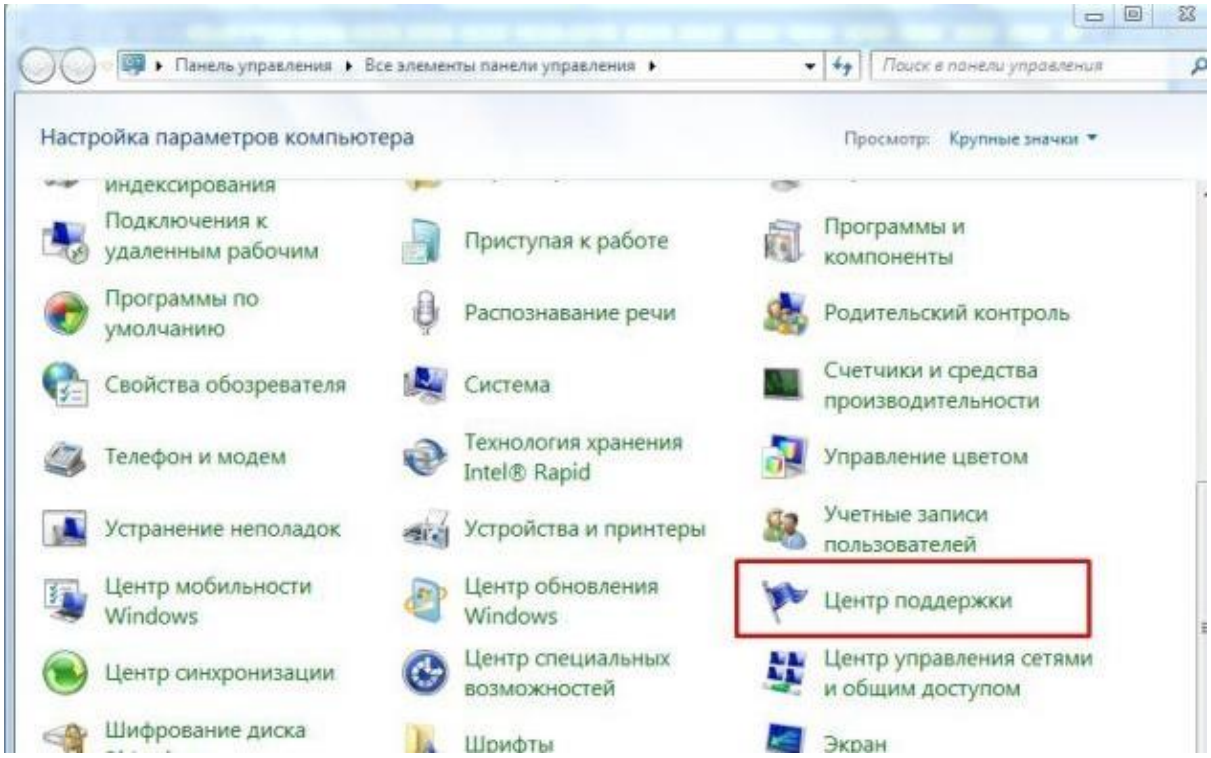
Телеметрия – это процесс сбора различной информации об активностях пользователя и его программ. Такой процесс уже давно используется в различных операционных системах. Однако для пользователей Windows 7 он представляет некую опасность. Во-первых, телеметрия сразу после установки операционной системы включается без явного уведомления пользователя. Во-вторых, собирая пользовательские данные, она тормозит ПК. В третьих, отключить её не так просто.

Переходим в панель управления и выбираем **"Центр обновления Windows"**.
Отключаем обовление системы, если оно у вас еще не отключено

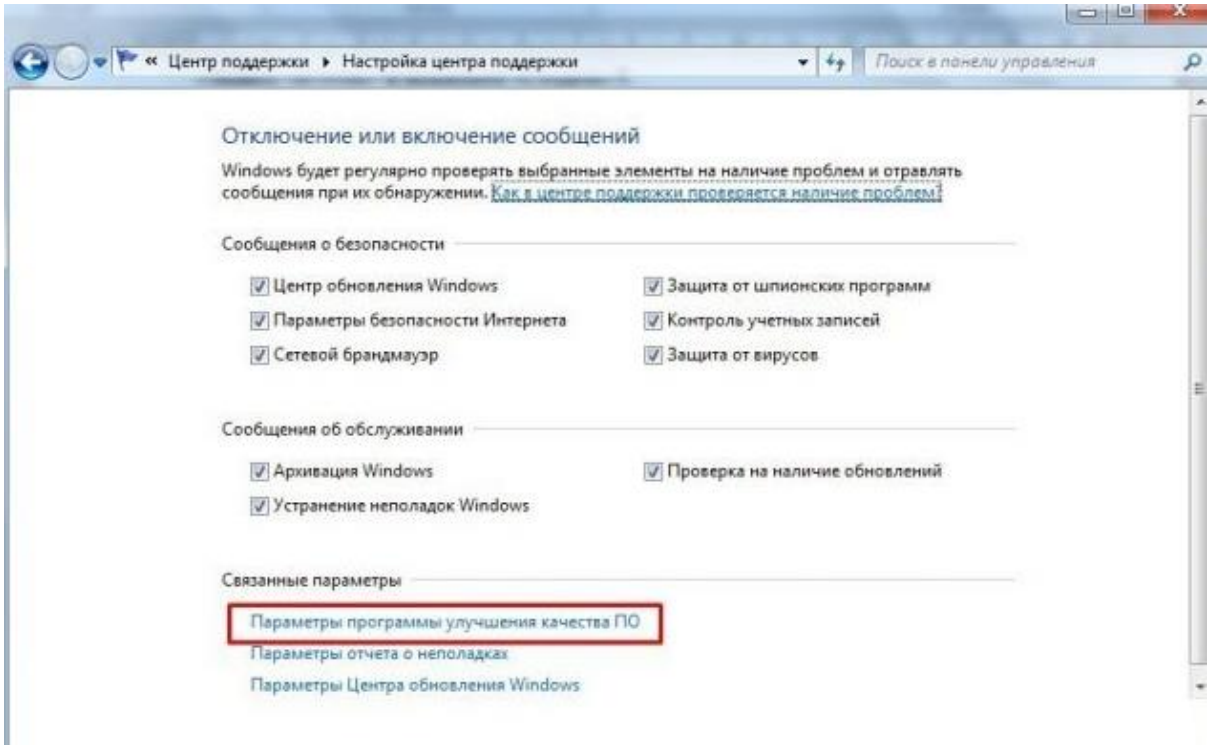




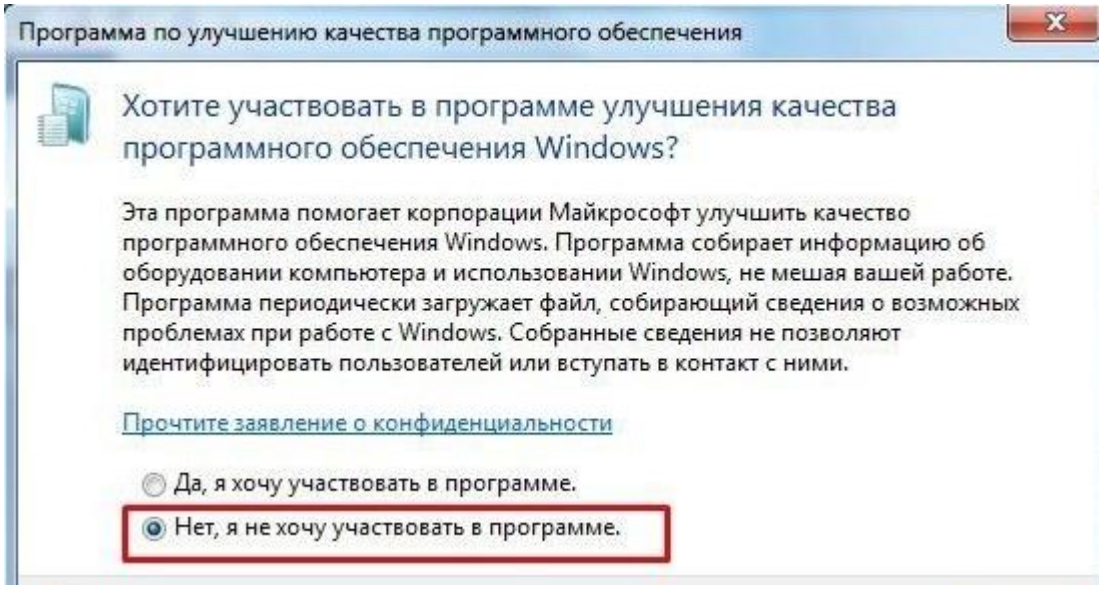
Возвращаемся в **Панель управления** и выбираем **"Центр поддержки"**



В меню слева выбираем **«Настройка центра поддержки»**. Здесь нажимаем на ссылку **«Параметры программы улучшения качества ПО».**

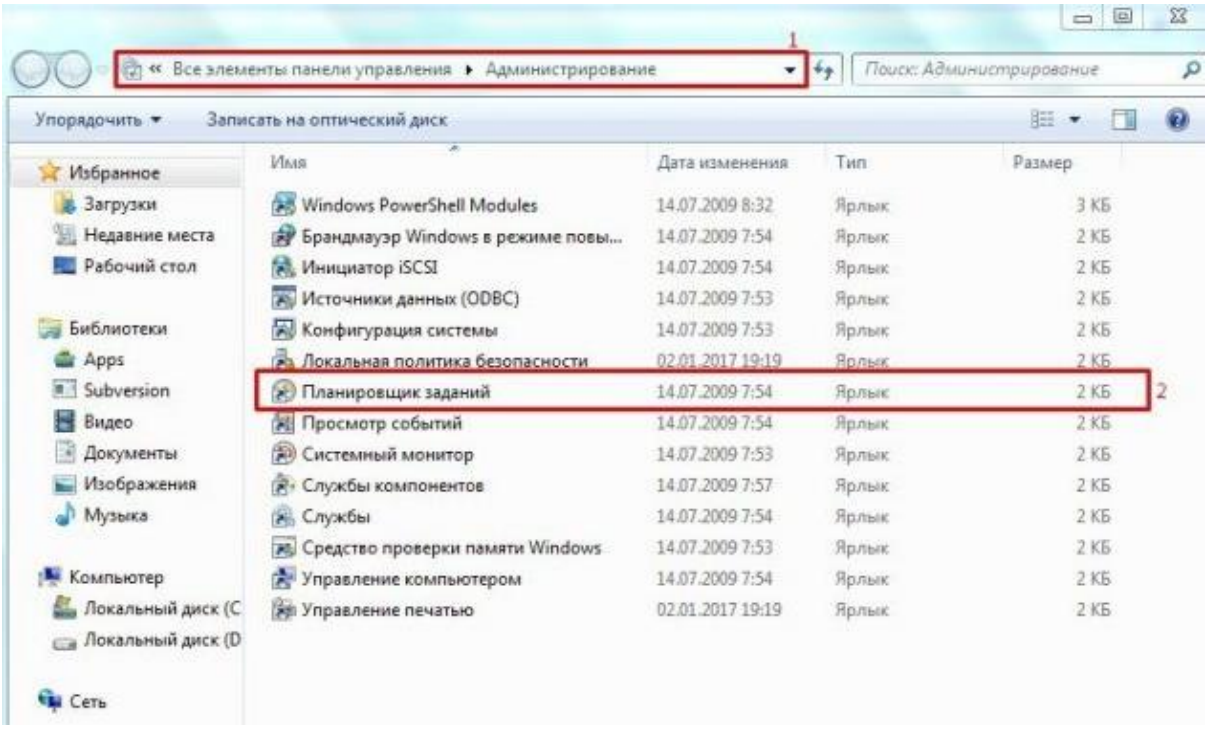


Ставим галочку **"Не участвовать"**



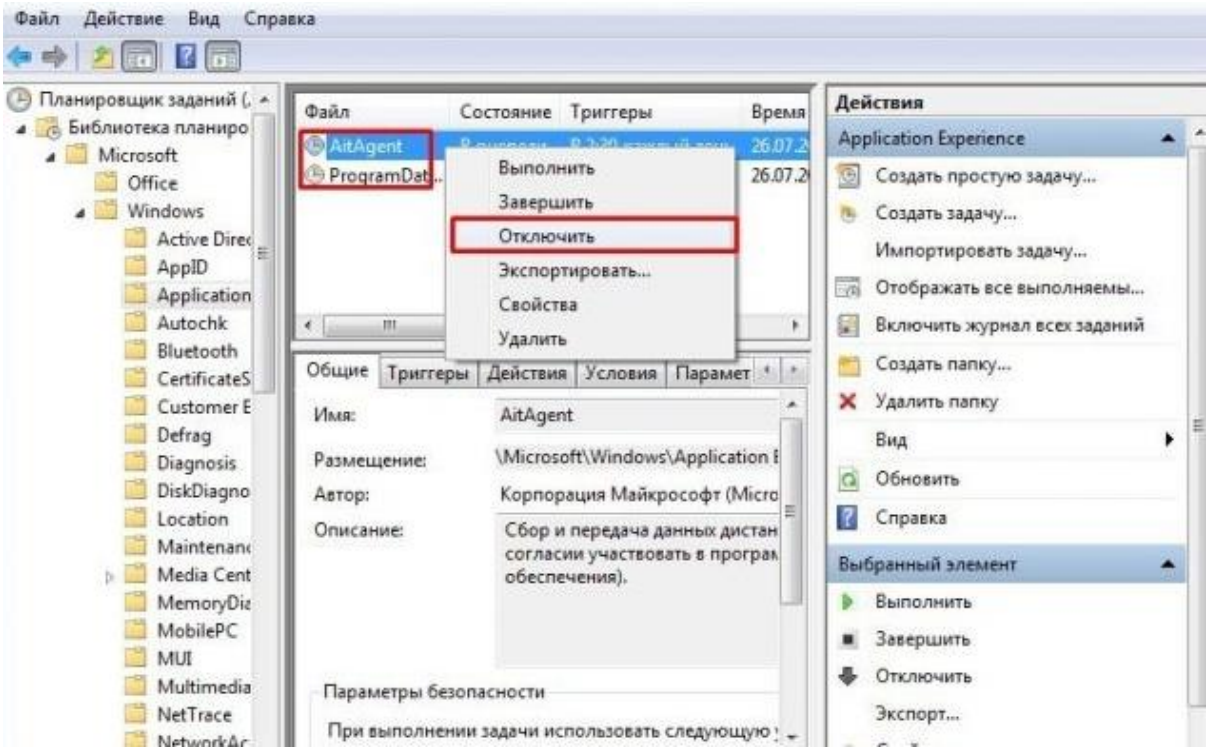
Теперь нужно отключить несколько заданий в **Планировщике**. Для этого стоит выполнить следующие действия:

Открываем **Панель управления**. Выбираем **«Администрирование»**, а далее **«Планировщик заданий».**

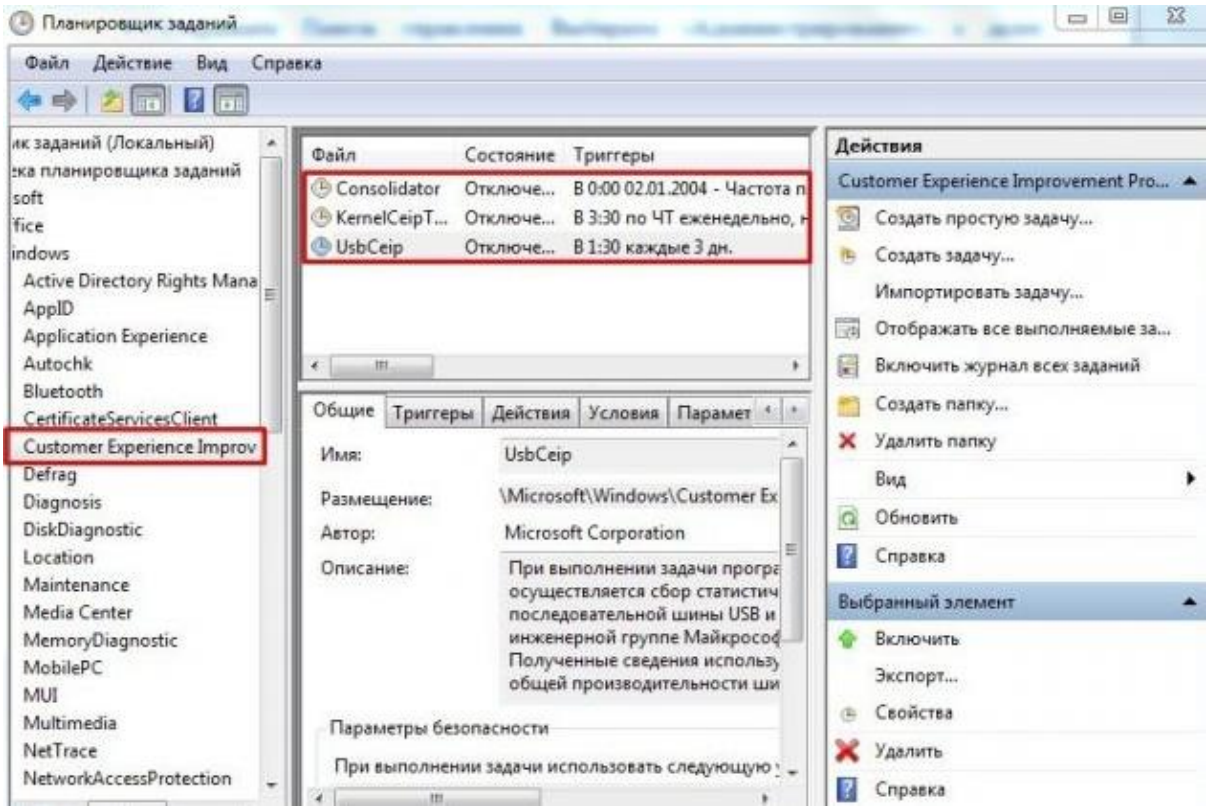


Откроется новое окно. В древовидном меню слева переходим по адресу: «Microsoft», «Windows», «Application Experience».

Здесь будет несколько задач. Отключаем **«AITAgent», «ProgramDataUpdater» и «Microsoft Compatibility Appraiser»** (если есть). Для отключения задач нажимаем на них правой кнопкой мыши и выбираем «Отключить».



И последний раздел, в котором нужно отключить все задачи, это **«Customer Experience Improvement Program».** Здесь нужно деактивировать **«Consolidator», «KernelCEIPTask», «UsbCEIP».**



Немного комментариев по вышеперечисленным пунктам.

Consolidator (Если пользователь изъявил желание участвовать в программе по улучшению качества программного обеспечения Windows, эта задача будет собирать и отправлять сведения о работе программного обеспечения в Майкрософт) — с 12/08/2015

KernelCeipTask (При выполнении задачи программы улучшения качества ПО, выполняющейся в режиме ядра (Kernel CEIP), осуществляется сбор дополнительных данных о системе, которые затем передаются в корпорацию Майкрософт. Если пользователь не дал своего согласия на участие в данной программе, то эта задача не выполняет никаких действий.) — с 12/08/2015

UsbCeip (При выполнении задачи программы улучшения качества ПО шины USB (USB CEIP) осуществляется сбор статистических данных об использовании универсальной последовательной шины USB и сведений о компьютере, которые направляются инженерной группе Майкрософт по вопросам подключения устройств в Windows. Полученные сведения используются для повышения надежности, стабильности и общей производительности шины USB в Windows. При отсутствии согласия пользователя на участие в программе улучшения программного обеспечения Windows задача не выполняет никаких действий.) — с 15/08/2015

Прогон задачи CEIP-консолидатора под procmon'ом показал, что, как минимум, отсылаются:

1. Языковые параметры

2. Конфигурация оборудования из подразделов HKLM\System\CurrentControlSet\ и HKLM\HARDWARE\DEVICEMAP\VIDEO\

3. Производитель мат.платы и всего компа (если есть), версия BIOS

4. Результаты проверки всех файлов из System32

5. Настройки интернет-соединения (HKLLonB7UtV97nMVRn1w2bM656PLog19npoEentVersion\Internet Settings\Connections*)

6. Источник установки (HKLLonB7UtV97nMVRn1w2bM656PLog19npoEentVersion\Setup\SourcePath и HKLLonB7UtV97nMVRn1w2bM656PLog19npoEentVersion\DevicePath)

Эти данные не к чему отсылать, по этой причине мы их блокируем.

Следующий этап – это отключение службы, которая также отвечает за телеметрию. Для этого выполняем следующее:

Жмём «Win+R» и вводим «services.msc»

Откроется новое окно. Находим в списке служб «Diagnostics Tracking Service» и отключаем её. Для этого используем варианты правой кнопки мыши или выделяем службу и нажимаем на соответствующую кнопку «Отключить».

После выполнения данных манипуляций, стоит перезагрузить систему.

Эти общеизвестные методы избавляют нас от нежелательных последствий и решают проблему слежки и телеметрии.