Хакер - Прокачай десятку! Настраиваем Windows 10 для безопасной и комфортной работы

nopaywall

https://t.me/nopaywall

Андрей Васильков

Содержание статьи

В своем развитии Windows прошла долгий путь от графической надстройки над MS-DOS до клиентской надстройки над облачным сервисом Microsoft. Превратить ее в полноценную операционку вряд ли удастся, но, если подкрутить глубокие настройки, она станет чуточку безопаснее и не такой своенравной.

WARNING

Прежде чем экспериментировать с реестром и службами, советуем создать точку восстановления, а еще лучше — сделать полный бэкап системного раздела.

Бэкапим реестр

Один из способов сделать бэкап реестра — это запустить в консоли REG EXPORT.

```
reg export HKLM hklm_backup.reg
```

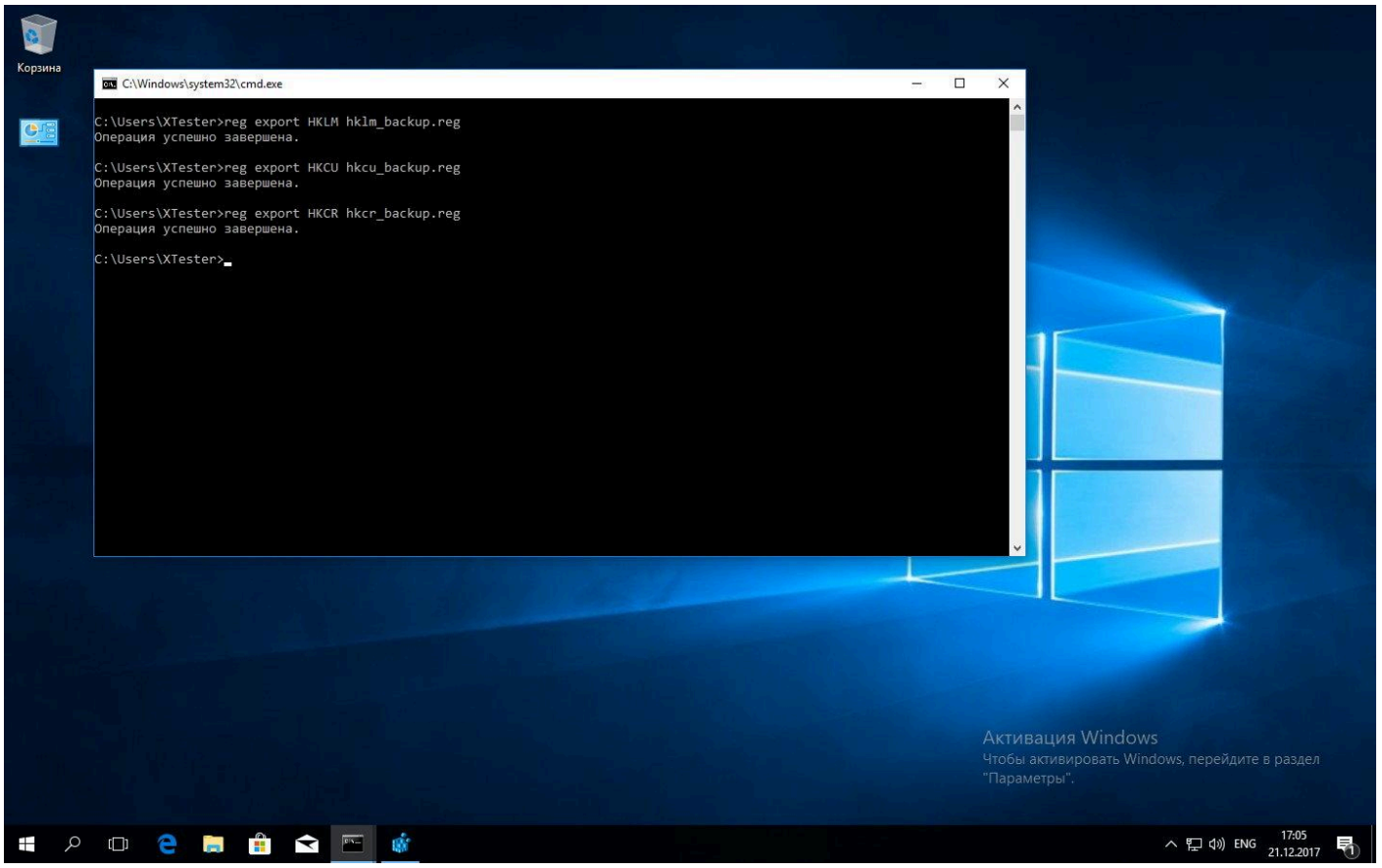
Такой командой мы задаем создание файла

```
hklm_backup.reg
```

со всей информацией из ветки

```
HKEY_LOCAL_MACHINE
```

. Аналогично повторяем команду для других веток реестра (см. скриншот).



Создаем бэкап реестра

Так же можно бэкапить отдельные ключи перед их изменением. Если что-то пойдет не так, ты всегда откатишь изменения простым запуском .reg-файла.

Получаем доступ к реестру

Программисты наклепали десятки разных твикеров системы. Все они обещают чудеса и работают непрозрачно, но реально все их функции сводятся к трем простым вещам:

- изменению отдельных ключей реестра;
- остановке невостребованных служб;
- удалению или добавлению заданий планировщика.

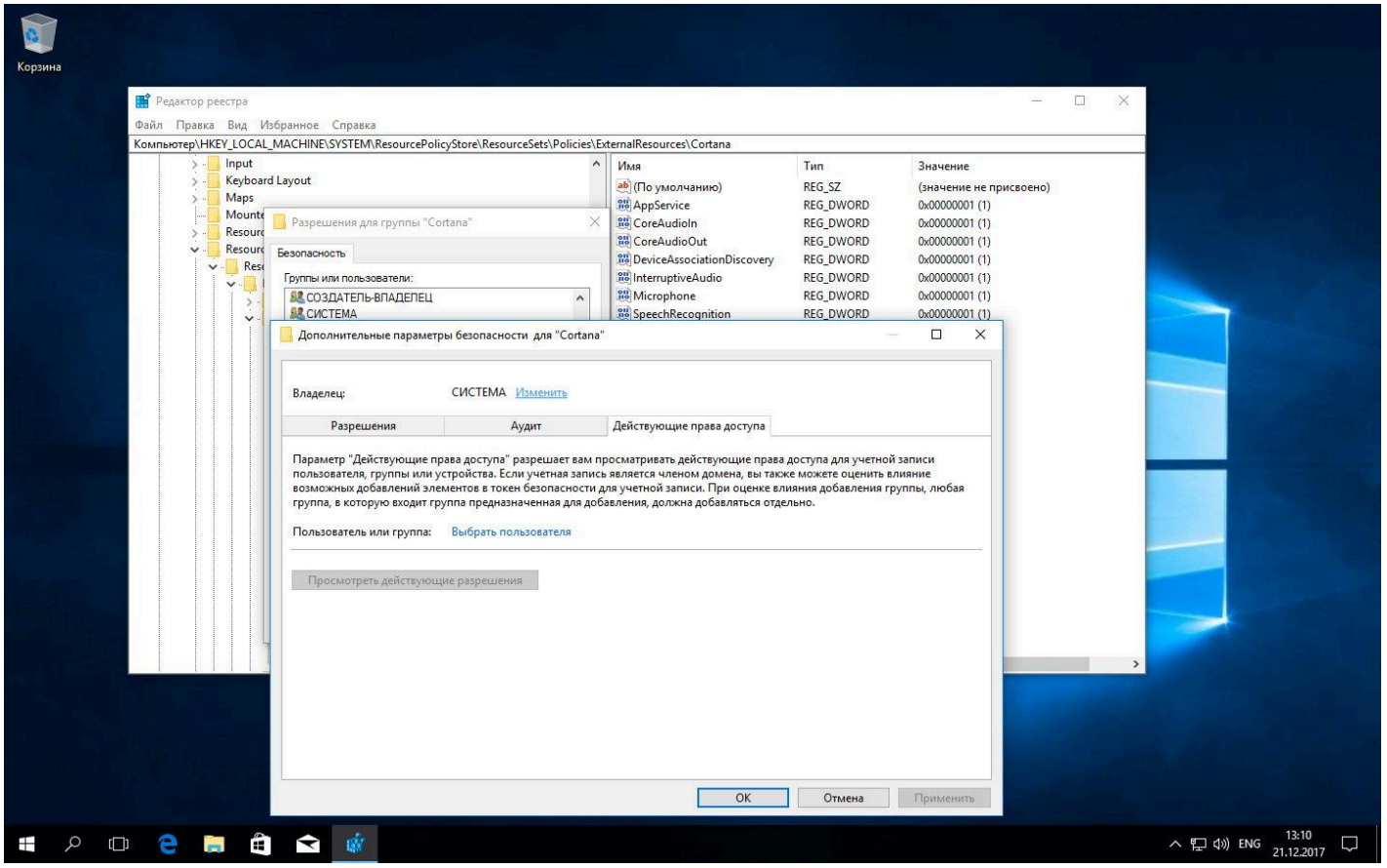
Часто эти процедуры взаимосвязаны. Например, запущенная служба не даст удалить свой ключ реестра или автоматически восстановит отмененное задание в планировщике. Поэтому мы рассмотрим каждую задачу подробно, не ограничиваясь стандартными рекомендациями.

Начнем с получения доступа к реестру. Это отдельная проблема в новых Windows, особенно десятой версии. По умолчанию администратор не может изменить значения ключей во многих ветках реестра или удалить файлы по своему усмотрению. Он вроде как хозяин, но не совсем.

Типичная схема управления привилегиями доступа Windows удивляет линуксоида тем, что система имеет более высокие полномочия, чем любой аккаунт в группе админов. В дефолтных настройках SYSTEM может все, а Administrators — только дозволенное. Исправить это недоразумение можно разными «хакерскими» способами, но большинство из них оставляют брешь в системе и снижают безопасность вместо того, чтобы ее повышать. Поэтому рассмотрим более аккуратные методы. Независимо от объекта (ключа реестра, файла, каталога) сначала придется стать его владельцем и лишь затем назначать себе права доступа.

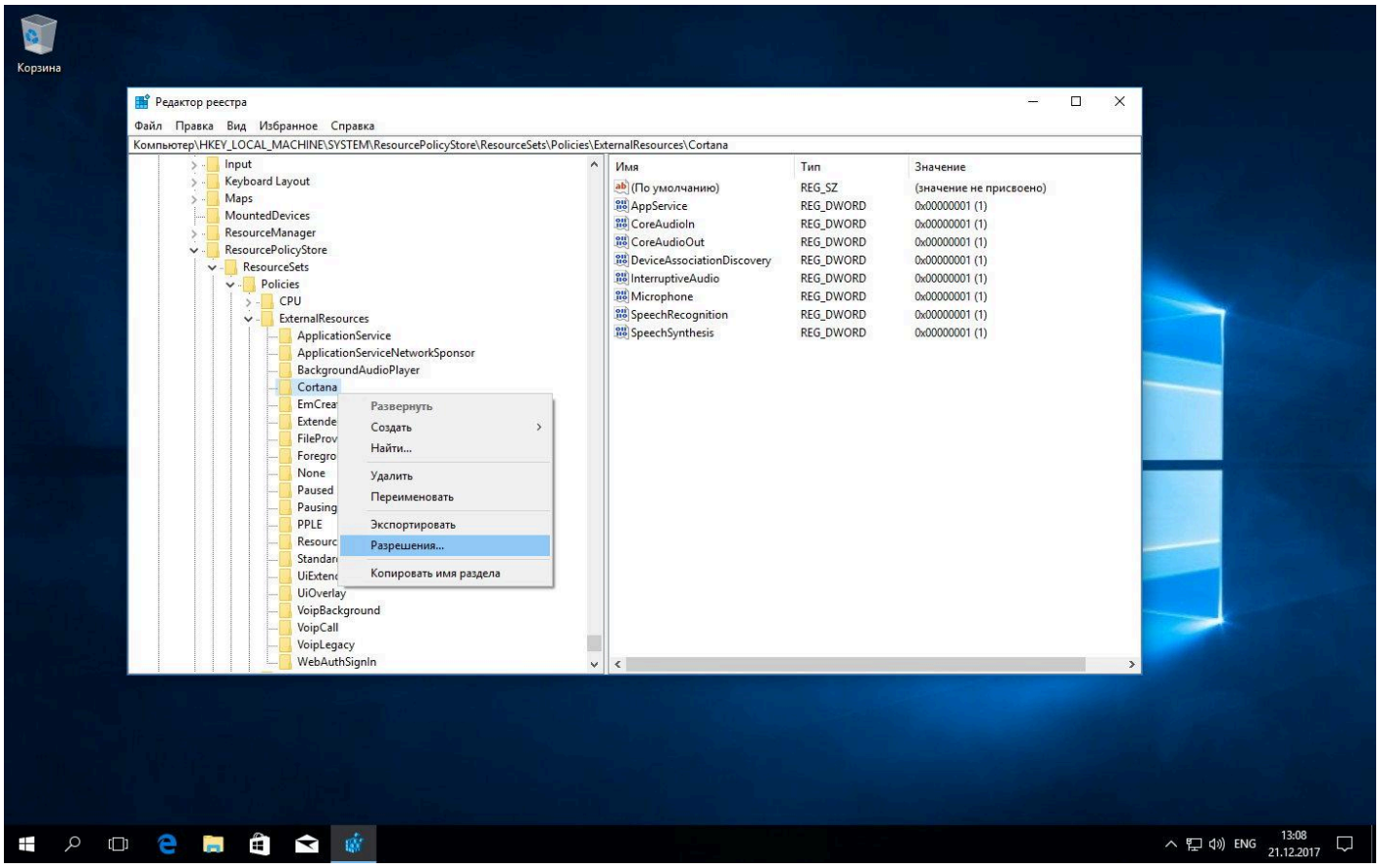
Метод 1 — через regedit

Удобство этого метода в том, что в нем не требуется дополнительно устанавливать какой-либо софт. Неудобство — в необходимости задавать разрешения для каждого конкретного ключа через графическую оболочку. Хотя кому-то это, наоборот, покажется удобным.



Меняем владельца для Кортаны

Просто запускаем от админа regedit, выделяем желаемый ключ и в контекстном меню (вызывается правым кликом мыши) переходим в параметр «Разрешения» (Permissions), где меняем владельца и затем прописываем любые разрешения.



Задаем разрешения для изменения настроек Кортаны

Метод 2 — через штатную утилиту SubInACL

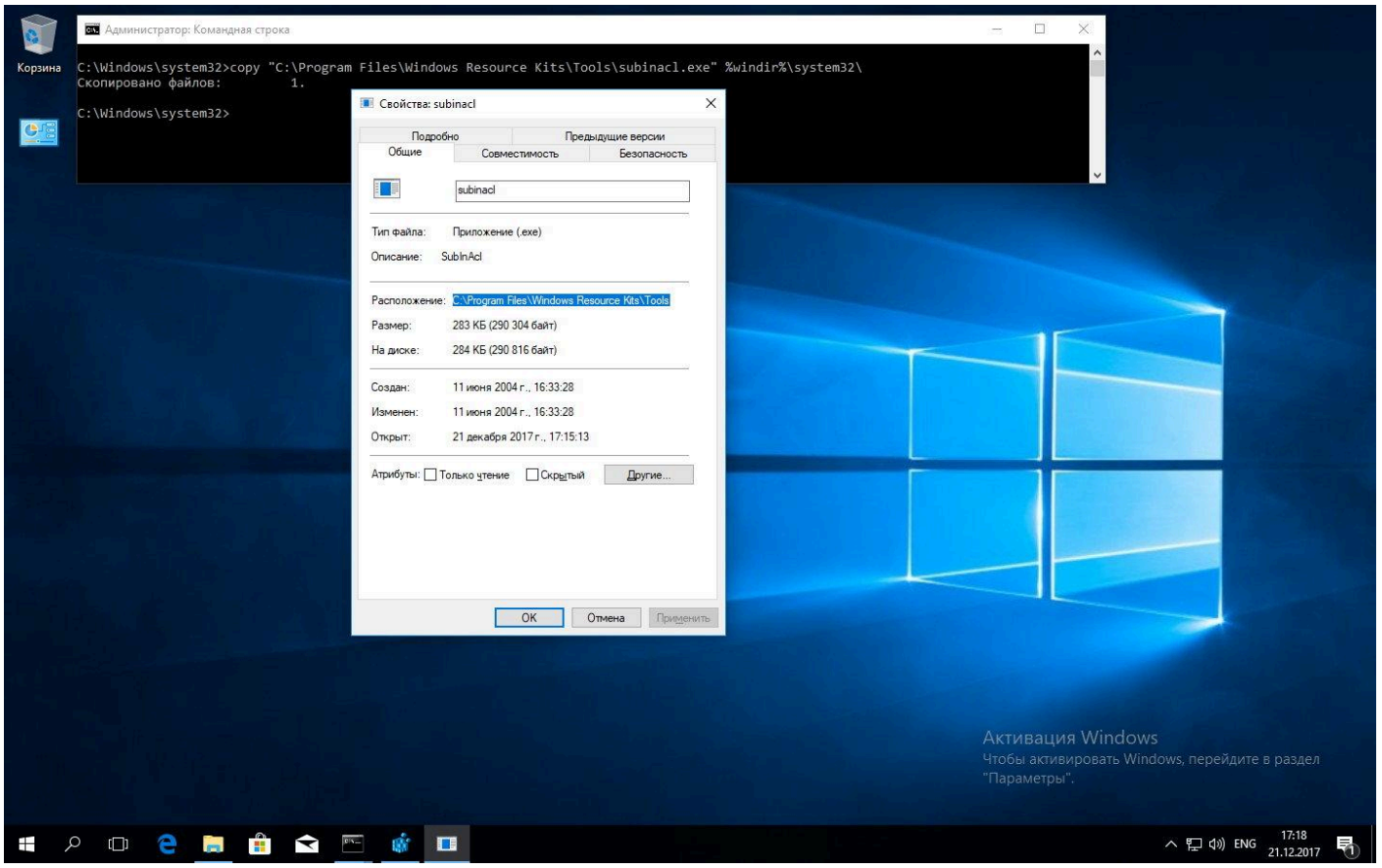
Скачиваем утилиту SubInACL с сайта Microsoft. В списке поддерживаемых ОС нет Windows 10, но пусть тебя это не смущает. Проверяли, работает. Просто помни, что программу надо запустить из консоли от имени администратора. Для этого удобнее сначала скопировать

```
SubInACL.exe
```

в системный каталог Windows (

```
%Windir%\System32\
```

), чтобы не вбивать каждый раз путь до исполняемого файла.



Копируем SubInACL в системный каталог
Далее для

```
SubInACL
```

нужно указать имя модифицируемого объекта, его тип и желаемое действие. Объект может быть одного из следующих типов: файл (file), каталог (folder), определенный ключ реестра (keyreg) или запись реестра со всеми ее дочерними ключами (subkeyreg).
Как обычно: прежде чем назначать права объекту, нужно стать его владельцем. Два действия легко объединить в одну команду, перечислив их через пробел. Например, следующая команда сначала сделает группу «Администраторы» владельцем ключа AutoLogger (он отвечает за трассировку событий, происходящих на начальных этапах загрузки ОС), а затем предоставит админам полный доступ к нему.

```
SUBINACL /keyreg "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\AutoLog
ger" /setowner=XTester /grant=XTester=f
```

Вместо

```
XTester
```

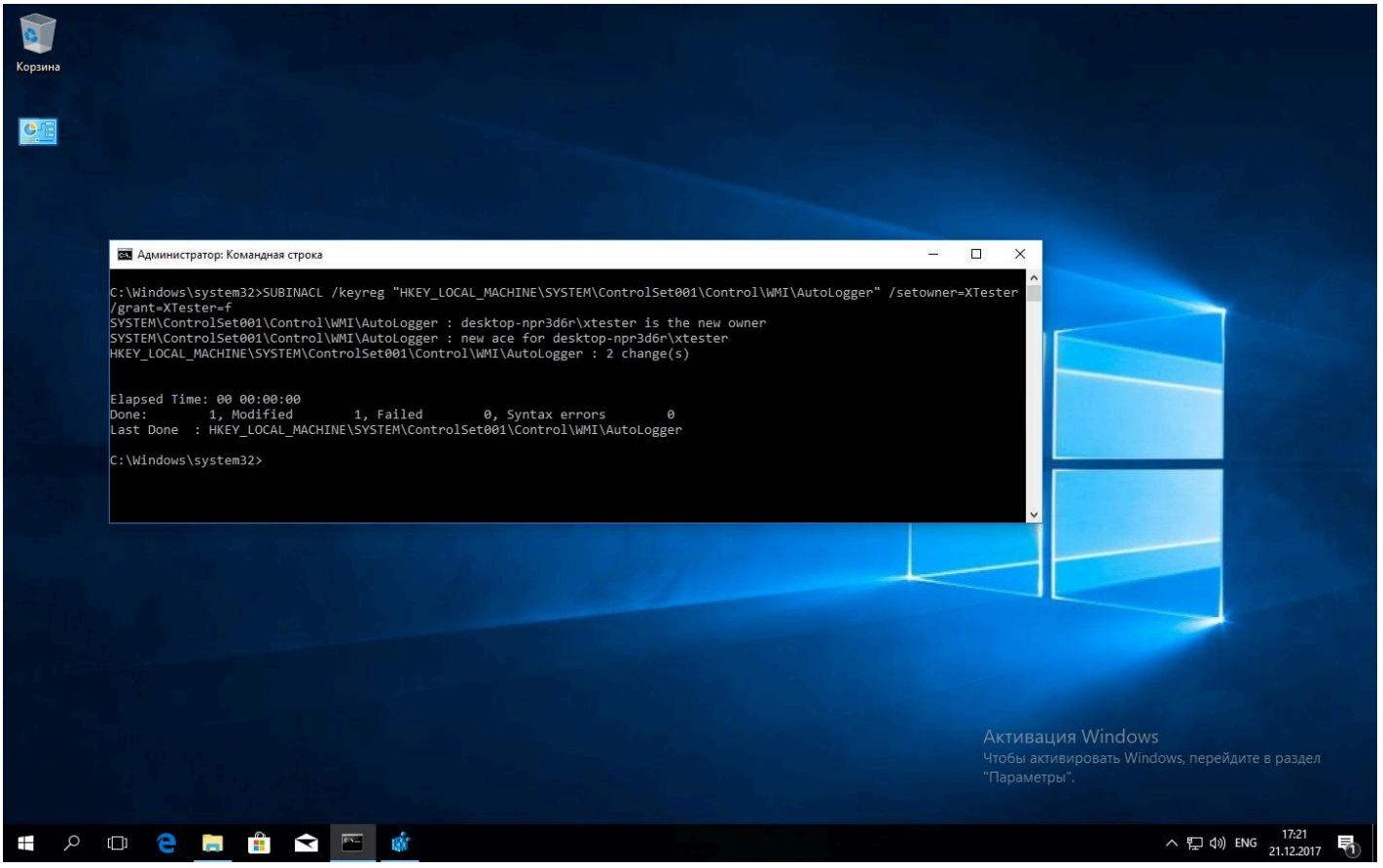
подставь везде имя своей учетной записи.
Используя объекты типа

```
subkeyreg
```

, легко полностью разблокировать реестр. Просто перечисли его корневые ветки по образцу ниже:

```
subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=XTester=f subinacl /subkeyreg H
KEY_CURRENT_USER /grant=XTester=f
```

И так далее.



Пример использования SubInACL

Аналогично в одну команду становимся владельцами всех файлов и каталогов на указанном диске.

```
subinacl /subdirectories %SystemDrive% /grant=XTester=f
```

Метод 3 — через стороннюю бесплатную утилиту SetACL

В целом метод аналогичен использованию штатной утилиты SubInACL. Отличия — минимальные.

Сначала скачиваем фриварную софтину.

Распаковываем архив и копируем из него файл

```
SetACL.exe
```

в каталог

```
%Windir%\System32
```

(или 64). Потом запускаем консоль от админа и вызываем SetACL. Полный синтаксис использования этой утилиты описан в руководстве. Краткая справка вызывается при запуске с ключом

```
help
```

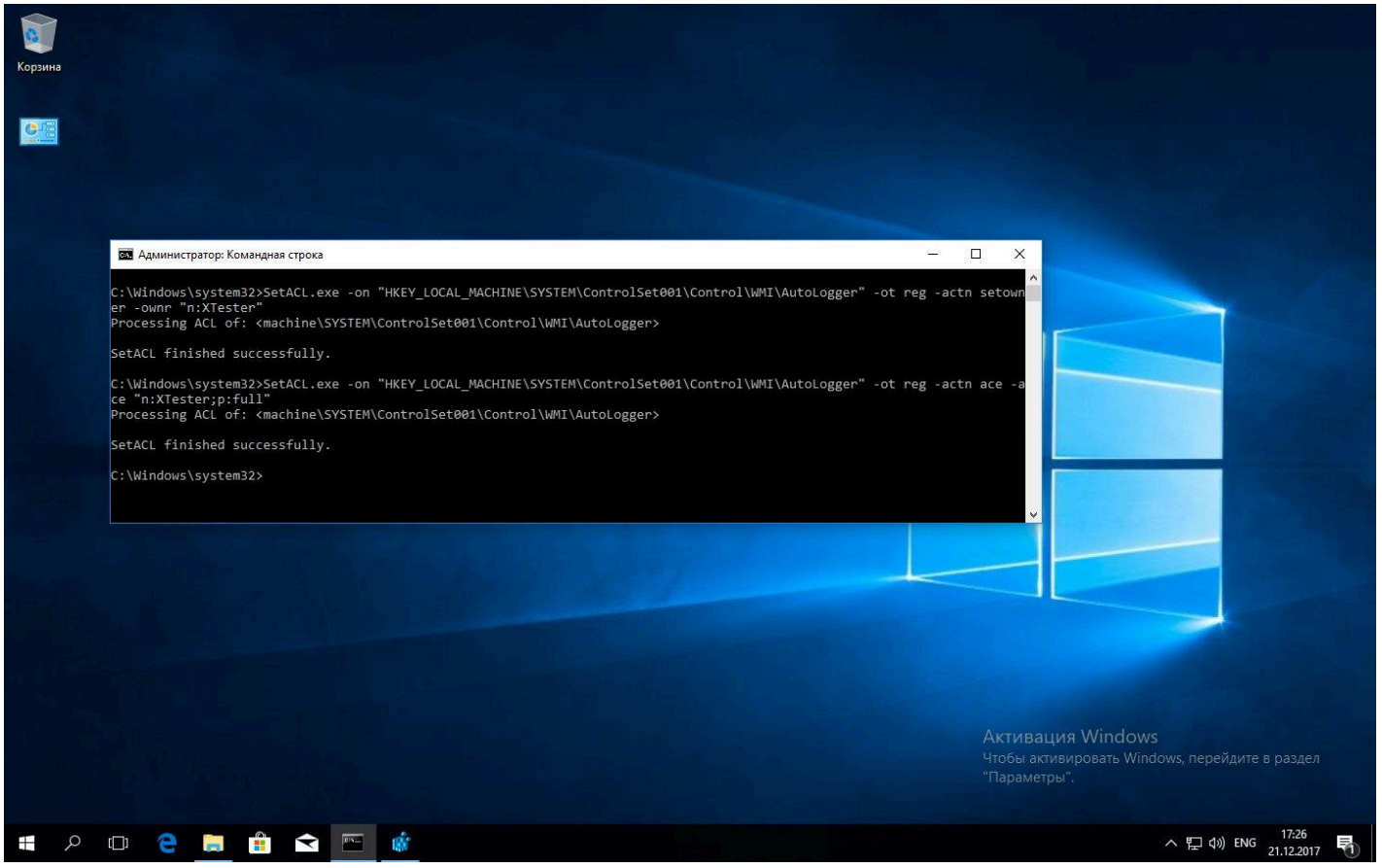
.

Логика утилиты та же, что и у SubInACL: нужно указать имя объекта, его тип и действие. Только в случае SetACL это лучше делать отдельными командами. Например, команда ниже сделает указанного пользователя (XTester) владельцем ключа автологгера.

```
SetACL.exe -on "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\AutoLogge
r" -ot reg -actn setowner -ownr "n:XTester"
```

Следующая же команда предоставит указанной учетке полный доступ к этому ключу реестра, то есть позволит изменять его.

```
SetACL.exe -on "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\WMI\AutoLogge
r" -ot reg -actn ace -ace "n:XTester;p:full"
```



Используем SetACL для задания прав доступа

После того как ты получил возможность менять любые ключи реестра, самое время приступить к его модификации.

Отключаем Кортану

Кортана сильно интегрирована в систему. Она связана со службой поиска, политиками приватности и так далее. Поэтому записей о ней в реестре много, и с каждым билдом Windows 10 их становится все больше.
После «разблокировки» реестра любой ключ легко менять через regedit. Когда их много, удобнее создать батник и поменять их все скопом из консоли.

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search" /v "AllowCo
rtana" /t REG_DWORD /d 0 /f reg add "HKLM\SOFTWARE\Microsoft\PolicyManager\de
fault\Experience\AllowCortana" /v "value" /t REG_DWORD /d 0 /f reg add "HKLM
\SOFTWARE\Microsoft\Windows\CurrentVersion\Search" /v "CortanaEnabled" /t REG
_DWORD /d 0 /f reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Searc
h" /v "CortanaEnabled" /t REG_DWORD /d 0 /f reg add "HKCU\SOFTWARE\Microsoft
\Windows\CurrentVersion\Search" /v "CanCortanaBeEnabled" /t REG_DWORD /d 0 /f
```

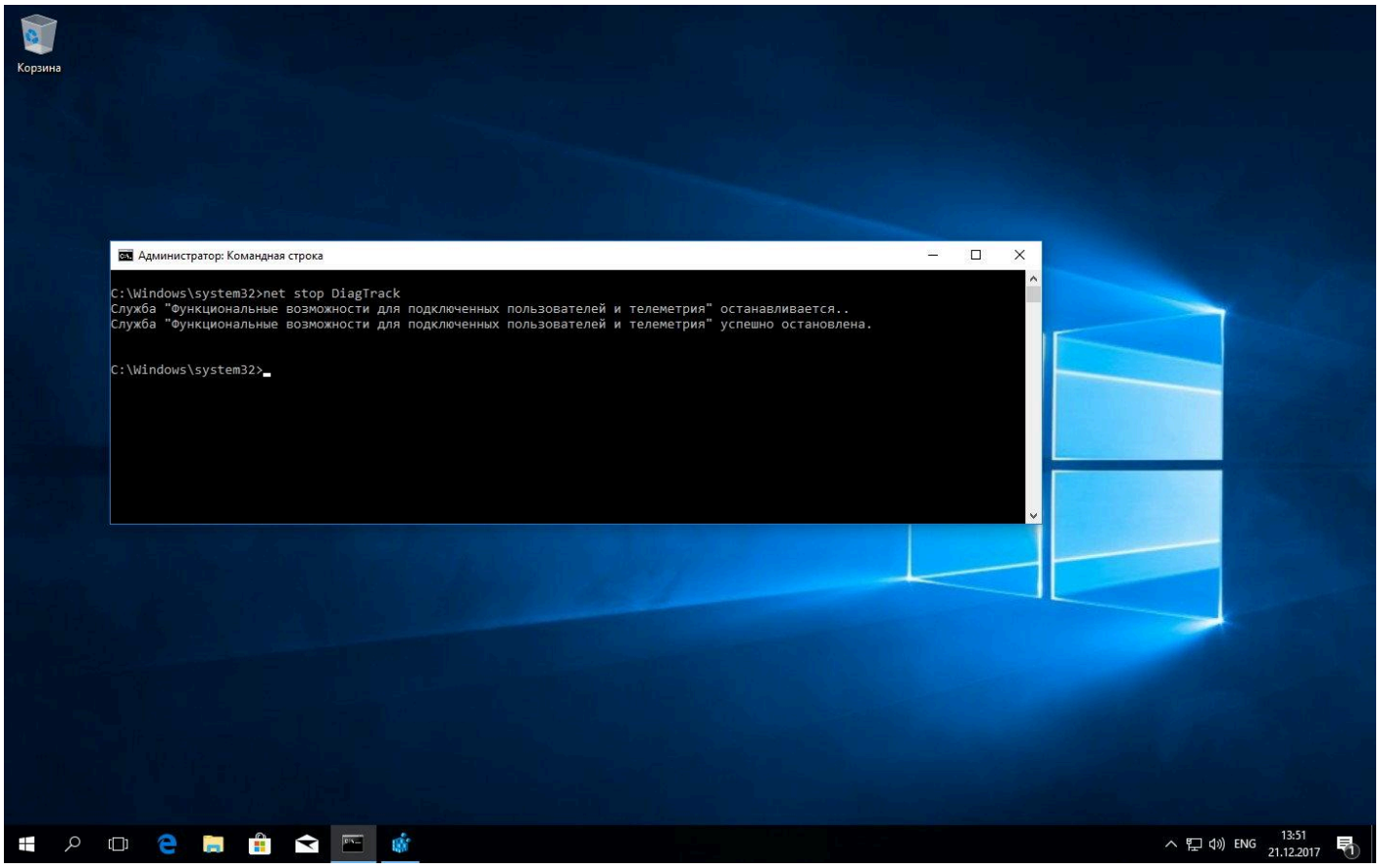
Отключаем сбор данных

Под видом сбора «диагностических» данных Windows 10 передает в Microsoft гигабайты данных, среди которых могут оказаться и конфиденциальные. По сути это что-то вроде встроенного кейлоггера.
Чтобы избавиться от этой пакости, сначала останавливаем фоновые службы. Это можно сделать через оснастку

```
services.msc
```

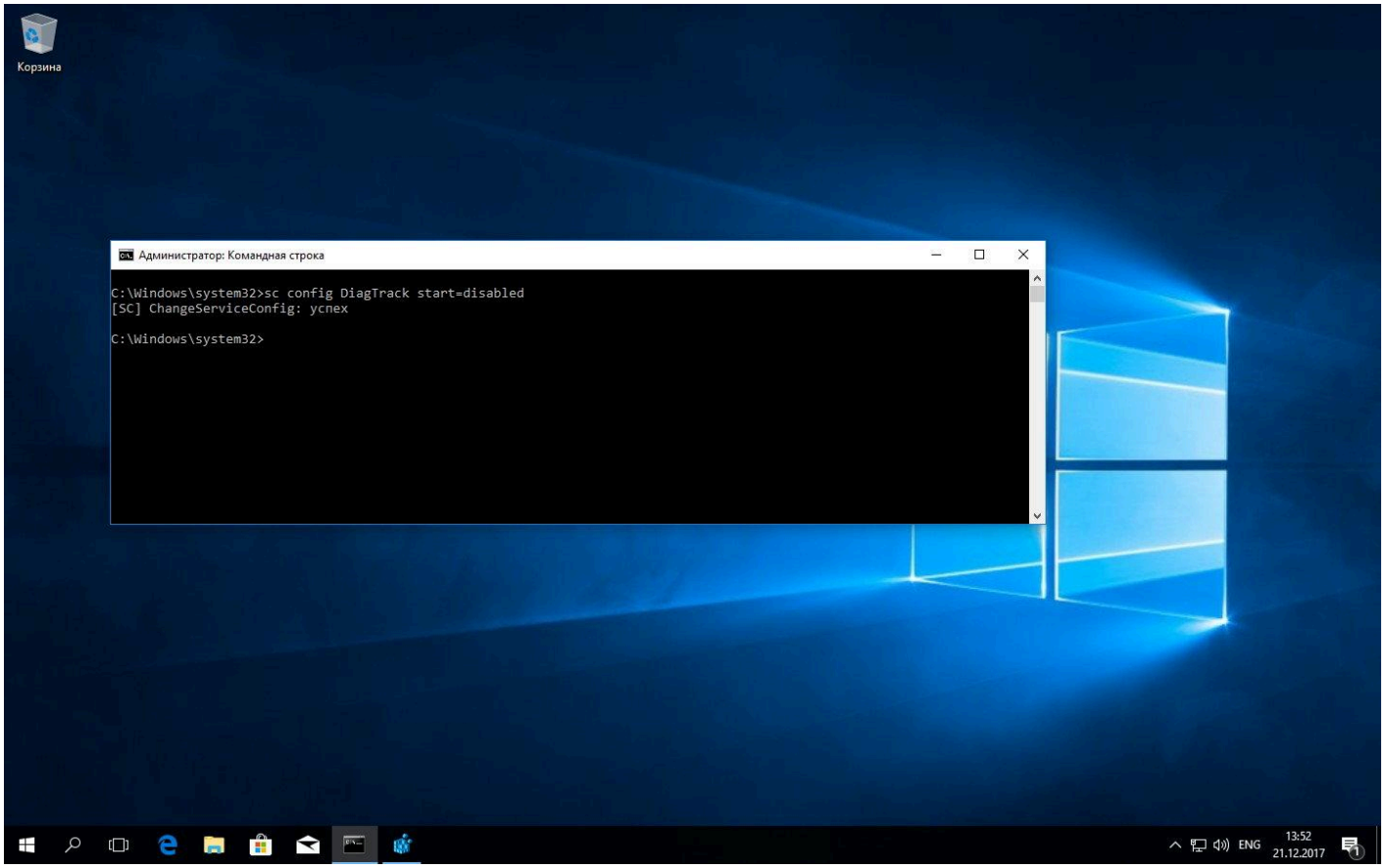
или прямо из консоли.

```
net stop DiagTrack
```



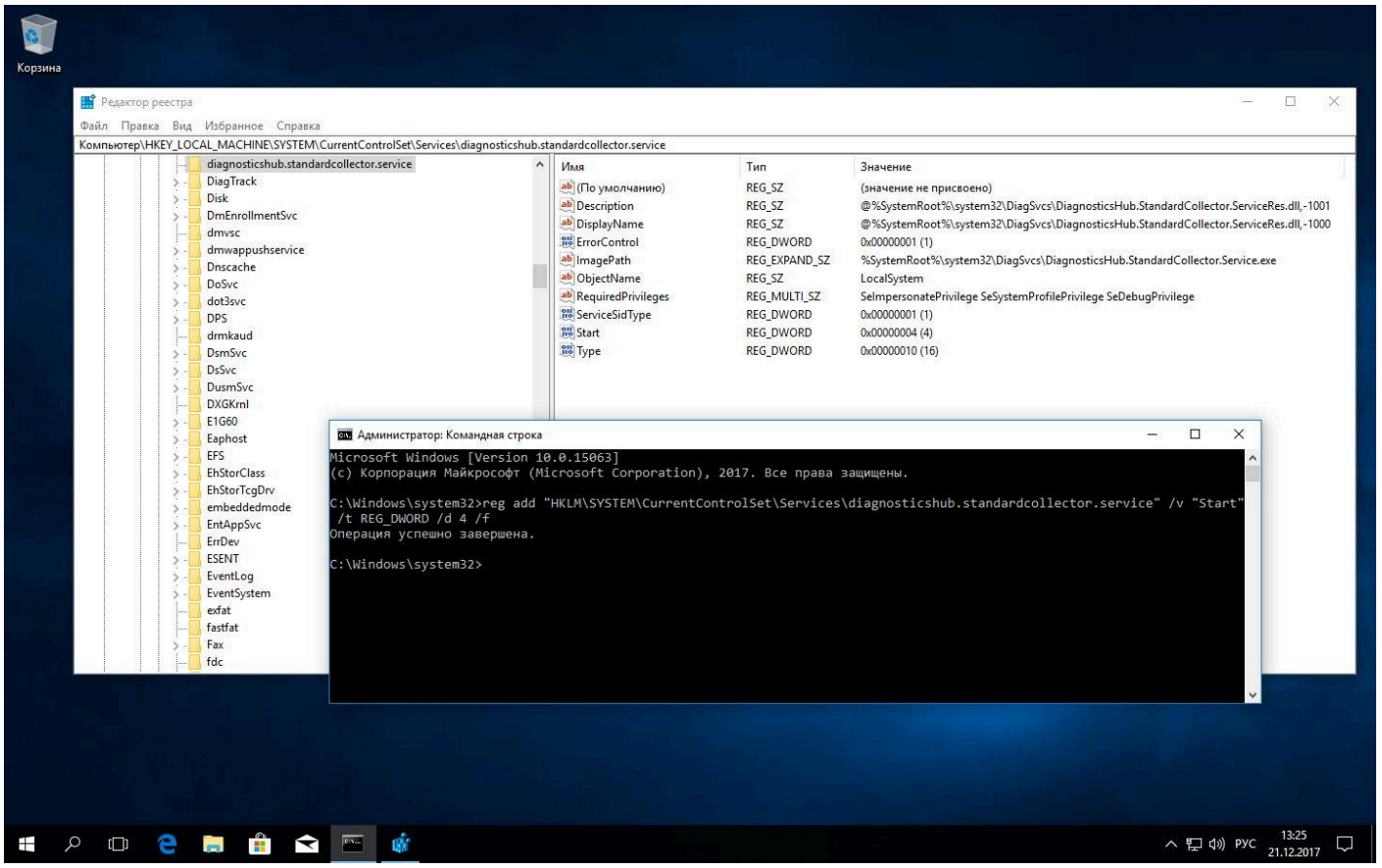
Останавливаем службу телеметрии

```
sc config DiagTrack start=disabled
```



Отключаем автостарт службы телеметрии

```
net stop dmwappushservice sc config dmwappushservice start=disabled
```



Изменяем любые ключи реестра через консоль или regedit
Далее по аналогии останавливаем службы и запрещаем их автозапуск:

- diagnosticshub.standardcollector.service;
- DcpSvc;
- WerSvc;
- PcaSvc;
- DoSvc;
- WMPNetworkSvc.

Список служб всегда подбирается индивидуально, но в первую очередь мы последовательно отключаем:

- DiagTrack (служба отправки «диагностических» данных);
- Diagnostics Hub Standard Collector (служба сборщика центра «диагностики» Microsoft);
- dmwappushservice (служба маршрутизации push-сообщений WAP).

Теперь пора править реестр.

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection" /v AllowTel
emetry /t REG_DWORD /d 0 /f reg add "HKLM\SYSTEM\CurrentControlSet\Services\d
iagnosticshub.standardcollector.service" /v "Start" /t REG_DWORD /d 4 /f reg
add "HKCU\SOFTWARE\Microsoft\Personalization\Settings" /v "AcceptedPrivacyPol
icy" /t REG_DWORD /d 0 /f reg add "HKLM\SYSTEM\ControlSet001\Control\WMI\Auto
```

```
Logger\AutoLogger-Diagtrack-Listener" /v "Start" /t REG_DWORD /d 0 /f reg add
"HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger\AutoLogger-Diagtrack-Li
stener" /v "Start" /t REG_DWORD /d 0 /f reg add "HKLM\SYSTEM\CurrentControlSe
t\Control\WMI\AutoLogger\SQMLogger" /v "Start" /t REG_DWORD /d 0 /f reg add
"HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" /v "AITEnable" /t REG_DW
ORD /d 0 /f reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" /v
"DisableUAR" /t REG_DWORD /d 1 /f reg add "HKCU\SOFTWARE\Microsoft\InputPerso
nalization" /v "RestrictImplicitInkCollection" /t REG_DWORD /d 1 /f reg add
"HKCU\SOFTWARE\Microsoft\InputPersonalization" /v "RestrictImplicitTextCollec
tion" /t REG_DWORD /d 1 /f reg add "HKCU\SOFTWARE\Microsoft\InputPersonalizat
ion\TrainedDataStore" /v "HarvestContacts" /t REG_DWORD /d 0 /f reg add "HKLM
\SOFTWARE\Policies\Microsoft\Windows\TabletPC" /v "PreventHandwritingDataShar
ing" /t REG_DWORD /d 1 /f reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\H
andwritingErrorReports" /v "PreventHandwritingErrorReports" /t REG_DWORD /d 1
reg add "HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows" /v "CEIPEnable"
/t REG_DWORD /d 0 /f reg add "HKLM\SOFTWARE\Policies\Microsoft\SQMClient" /v
"CorporateSQMURL" /t REG_SZ /d "0.0.0.0" /f reg add "HKCU\SOFTWARE\Policies\M
icrosoft\Office\16.0\osm" /v "Enablelogging" /t REG_DWORD /d 0 /f reg add "HK
CU\SOFTWARE\Policies\Microsoft\Office\16.0\osm" /v "EnableUpload" /t REG_DWOR
D /d 0 /f reg add "HKCU\SOFTWARE\Microsoft\MediaPlayer\Preferences" /v "Usage
Tracking" /t REG_DWORD /d 0 /f reg add "HKCU\SOFTWARE\Microsoft\Siuf\Rules" /
v "NumberOfSIUFInPeriod" /t REG_DWORD /d 0 /f reg add "HKCU\SOFTWARE\Microsof
t\Siuf\Rules" /v "PeriodInNanoSeconds" /t REG_DWORD /d 0 /f reg add "HKLM\SOF
TWARE\Policies\Microsoft\Windows\DataCollection" /v "DoNotShowFeedbackNotific
ations" /t REG_DWORD /d 1 /f reg add "HKCU\SOFTWARE\Policies\Microsoft\Assist
ance\Client\1.0" /v "NoExplicitFeedback" /t REG_DWORD /d 1 /f reg add "HKLM\S
OFTWARE\Microsoft\Input\TIPC" /v "Enabled" /t REG_DWORD /d 0 /f reg add "HKCU
\SOFTWARE\Microsoft\Input\TIPC" /v "Enabled" /t REG_DWORD /d 0 /f
```

Просто сохрани все в виде скрипта (.bat или .cmd) и закомментируй те строки, которые считаешь лишними на конкретном компьютере.

WWW

Если хочешь узнать больше о шпионских замашках Windows 10, прочти эти статьи:

- Тайная жизнь Windows 10. О чем Windows 10 стучит в Microsoft и как заставить ее прекратить
- Обзор Windows 10 Anniversary Update: снова отучаем «десятку» следить и шпионить

Отключаем небезопасные сервисы

Любой сервис теоретически небезопасен, но есть известный перечень служб, которые оставляют в Windows 10 зияющие дыры. Остановить и отключить их автозагрузку можно также через

```
net stop
```

и

```
sc config
```

. Я просто перечислю их здесь, чтобы не перегружать статью командами с повторяющимся синтаксисом:

- RemoteRegistry;
- TermService;
- TrkWks;
- DPS.

Если ты используешь Windows 10 на компьютере, то лучше отключить и бесполезный сбор информации с датчиков мобильных устройств:

- SensorDataService;
- SensorService;
- SensrSvc.

Если не пользуешься Xbox, то стоит отключить и связанные с Xbox сервисы:

- XblAuthManager;
- XblGameSave;
- XboxNetApiSvc.

Опционально через реестр отключаем удаленного помощника:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance" /v "fAllowT
oGetHelp" /t REG_DWORD /d 0 /f reg add "HKLM\SYSTEM\CurrentControlSet\Control
\Remote Assistance" /v "fAllowFullControl" /t REG_DWORD /d 0 /f
```

При необходимости отключаем административные шары.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v
"AutoShareWks" /t REG_DWORD /d 0 /f
```

Задаем автоматическую очистку файла подкачки

Во избежание утечки паролей и прочих конфиденциальных данных лучше регулярно очищать файл подкачки при перезагрузке и выключении.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Managem
ent" /v " ClearPageFileAtShutdown " /t REG_DWORD /d 1 /f
```

Отключаем автозапуск со сменных носителей

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v
"NoDriveTypeAutoRun" /t REG_DWORD /d 255 /f reg add "HKLM\SOFTWARE\Microsoft
\Windows\CurrentVersion\Policies\Explorer" /v "NoAutorun" /t REG_DWORD /d 1 /
f
```

Стираем историю

Отключаем сохранение списков последних открытых файлов:

```
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /v "ShowRec
ent" /t REG_DWORD /d 0 /f reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\F
ileHistory" /v "Disabled" /t REG_DWORD /d 1 /f
```

Отключаем ведение истории поисковых запросов:

```
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Search" /v "DeviceHis
toryEnabled" /t REG_DWORD /d 0 /f
```

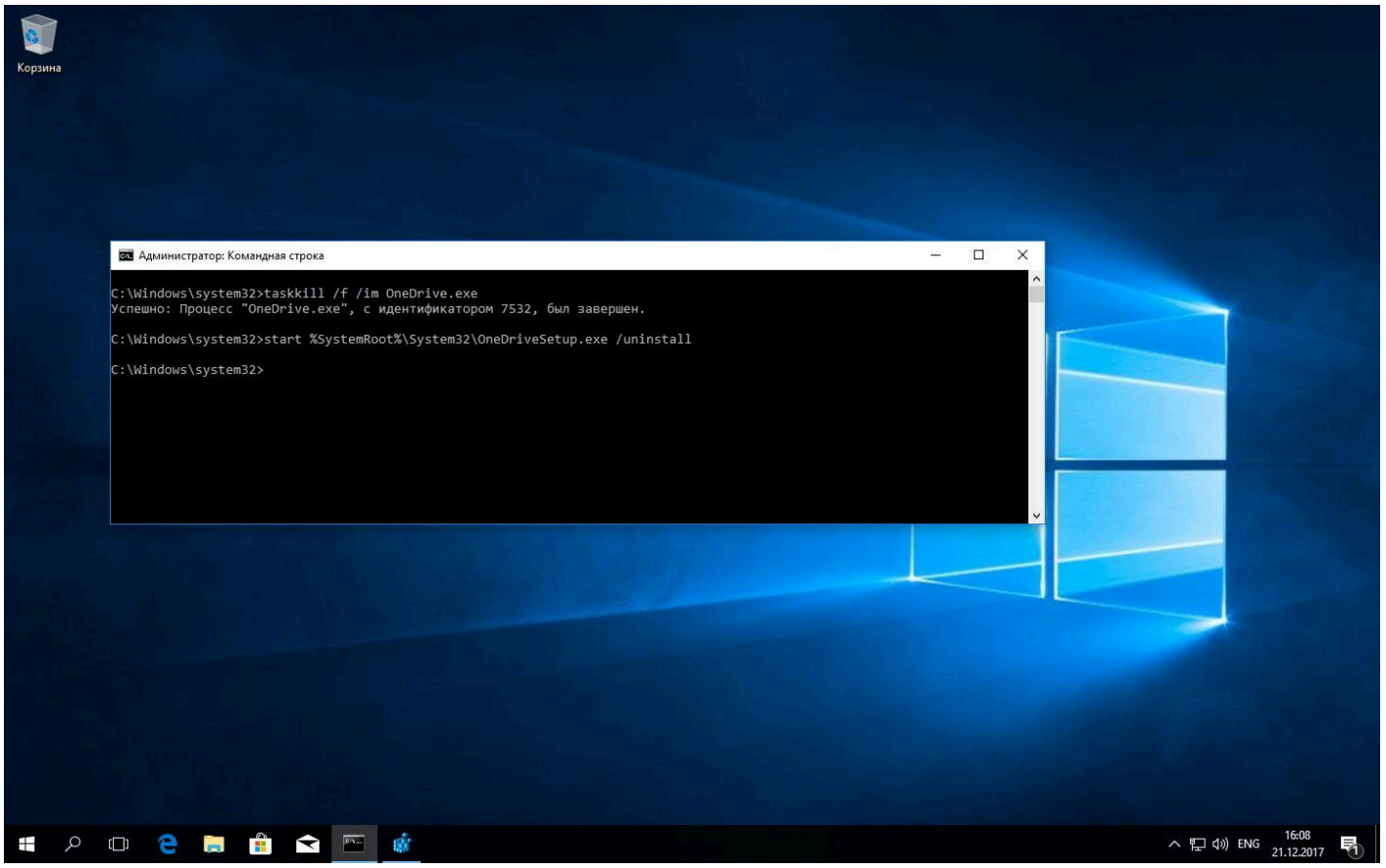
Отключаем историю для приложений:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\AppPrivacy" /v "LetAppsAcce
ssCallHistory" /t REG_DWORD
```

Удаляем предустановленные приложения

Удаление встроенных компонентов в Windows 10 не всегда происходит очевидным образом, но любая задача решается через консоль. Сначала мы прибиваем процесс ненужного нам приложения, а затем деинсталлируем его. На примере OneDrive это выглядит так:

```
taskkill /f /im OneDrive.exe start %SystemRoot%\System32\OneDriveSetup.exe /u
ninstall
```



Удаляем OneDrive

Настраиваем автоматическое создание точек восстановления

Точки восстановления удобно создавать автоматически при помощи утилиты командной строки WMI (Windows Management Instrumentation).
Просто настрой восстановление системы один раз, а затем создай батник, в котором будет следующая строка:

```
Wmic.exe /Namespace:\\root\default Path SystemRestore Call CreateRestorePoint
"%DATE%", 100, 1
```

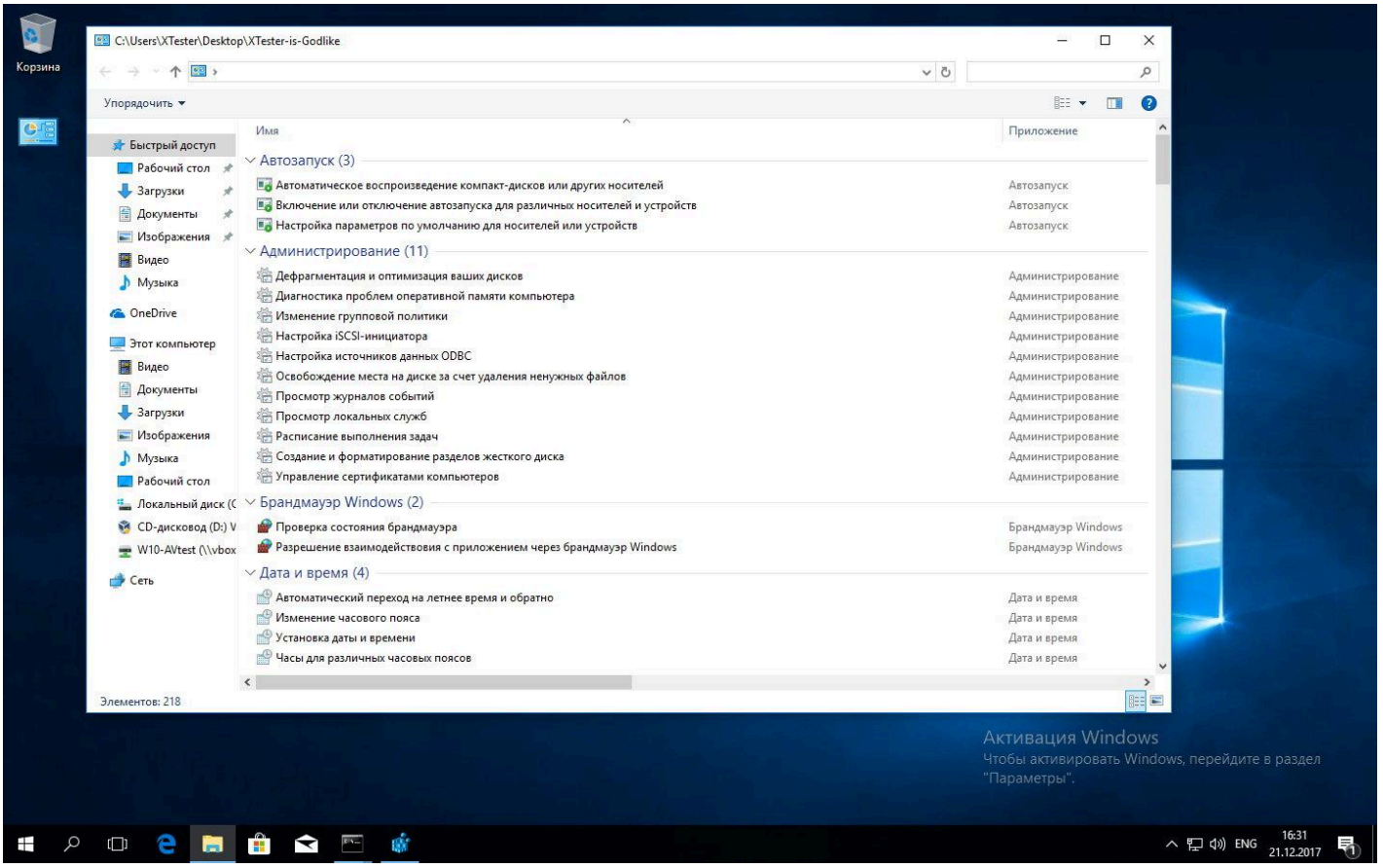
Повесь его в планировщик заданий, и он будет запускаться по указанному расписанию и автоматически создавать новые точки восстановления согласно настройкам, заданным тобой на первом этапе.

Режим бога (делаем быстрый вызов любых настроек)

Настройки многих параметров Windows 10 упрятаны так глубоко, что лазить по графическим меню можно полдня. Гораздо удобнее вызывать их все одним кликом через единственный ярлык. Такой прием получил название «режим бога» и выполняется элементарно: достаточно из-под админа создать на рабочем столе новую папку с именем

```
НапишиЗдесьЧтоУгодно.{ED7BA470-8E54-465E-825C-99712043E01C}
```

Это всё!



Добавляем «режим бога»

После нажатия на Enter значок папки изменится на системный и его имя скроется. При клике на него загрузится список из более чем двухсот настроек в алфавитном порядке. Красота!

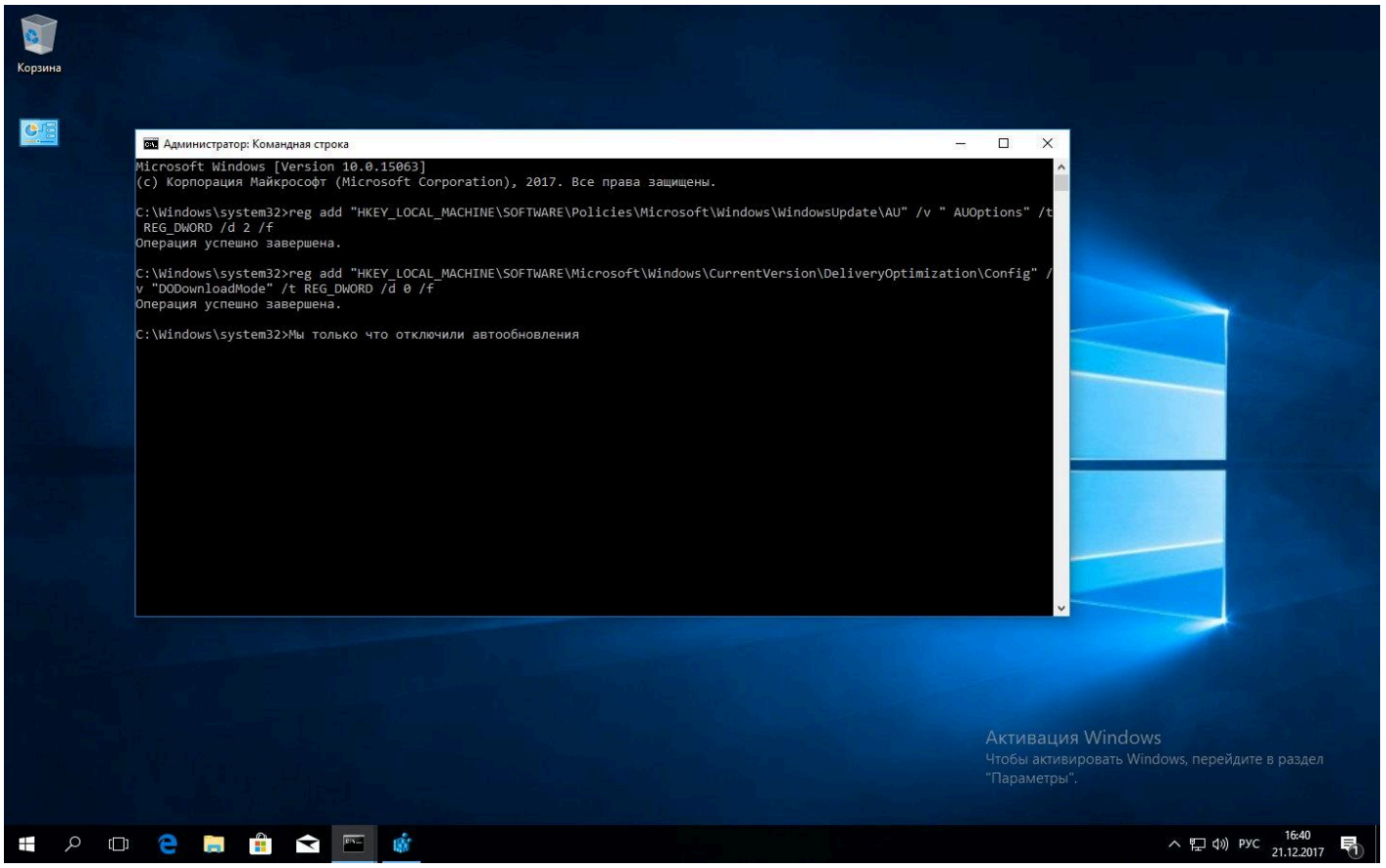
Отключаем автообновления

Избавить Windows от привычки загружать и ставить обновления, когда вздумается системе, а не тебе, тоже можно через реестр.

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
\AU" /v " AUOptions" /t REG_DWORD /d 2 /f
```

После этого остается возможность получать апдейты вручную.

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Deliver
yOptimization\Config" /v "DODownloadMode" /t REG_DWORD /d 0 /f
```



Автообновление отключено

Убираем из планировщика запланированные задачи телеметрии

Они состоят из секций «Клиентский опыт», «Облачный опыт», «Статистика приложений», «Файловая статистика», «Диагностика диска», «Диагностика энергоэффективности», «Монитор семейной безопасности», «Сбор сведений о сети» и множества других.
Все они доступны через консольную команду

```
schtasks
```

, которую сперва нужно запустить с ключом

```
end
```

для остановки задачи. Затем повторно запускаем уже с ключом

```
change
```

, указав после

```
tn
```

(task name) соответствующее название.

К примеру, команда

```
schtasks /end /tn "\Microsoft\Windows\FileHistory\File History (maintenance m
ode)"
```

завершит задачу «Сбор статистики использования файлов», а следующая команда отключит ее:

```
schtasks /change /tn "\Microsoft\Windows\FileHistory\File History (maintenanc
e mode)" /disable
```

Вот список остальных задач телеметрии:

- Microsoft\Windows\AppID\SmartScreenSpecific
- Microsoft\Windows\Application Experience\AitAgent
- Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser
- Microsoft\Windows\Application Experience\ProgramDataUpdater
- Microsoft\Windows\Application Experience\StartupAppTask
- Microsoft\Windows\Autochk\Proxy
- Microsoft\Windows\CloudExperienceHost\CreateObjectTask
- Microsoft\Windows\Customer Experience Improvement Program\Consolidator
- Microsoft\Windows\Customer Experience Improvement Program\BthSQM
- Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask
- Microsoft\Windows\Customer Experience Improvement Program\UsbCeip
- Microsoft\Windows\Customer Experience Improvement Program\Uploader
- Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector
- Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver
- Microsoft\Windows\DiskFootprint\Diagnostics
- Microsoft\Windows\FileHistory\File History (maintenance mode)
- Microsoft\Windows\Maintenance\WinSAT
- Microsoft\Windows\NetTrace\GatherNetworkInfo
- Microsoft\Windows\PI\Sqm-Tasks
- Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem
- Microsoft\Windows\Shell\FamilySafetyMonitor
- Microsoft\Windows\Shell\FamilySafetyRefresh
- Microsoft\Windows\Shell\FamilySafetyUpload
- Microsoft\Windows\Windows Error Reporting\QueueReporting

Заключение

В интернете ты найдешь массу программ, авторы которых обещают «улучшить работу Windows». Обычно они действуют по принципу черного ящика, выполняя неведомые действия. Все их функции можно заменить набором батников, создание которых описано в этой статье.

При создании собственного набора скриптов придется немного помучаться, но только один раз. Дальше все будет выполняться по расписанию (через планировщик) или по запросу в один клик.

Главное — ты всегда будешь знать наверняка, что именно изменяется в реестре и работе системных служб. Заодно, работая в консоли, ты углубишь свои знания о Windows 10 и сможешь выполнять аналогичные задачи голыми руками где угодно.