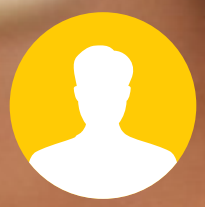
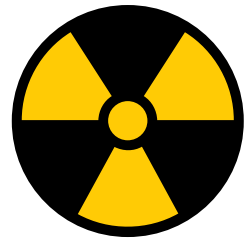
ВЕРНИТЕ ПРАВА!

КАК ОБОЙТИ ОГРАНИЧЕНИЯ НА РАБОЧЕМ КОМПЬЮТЕРЕ



84ckf1r3
84ckf1r3@gmail.com

Когда ты приходишь на работу и обнаруживаешь, что на компьютере что-то запрещено, а в Сети — заблокировано, это воспринимается практически как вызов. В своей статье я расскажу, какие бывают методы ограничений и как с ними бороться. Многие из описанных трюков мне приходилось проделывать самостоятельно — конечно же, исключительно с благими намерениями.



WARNING

Нарушение политики безопасности может повлечь административную и уголовную ответственность в зависимости от соотношения твоей наглости и удачливости. Редакция и автор не несут ответственности за любой возможный вред.

Понятно, что ограничения важны для безопасности и снижения нагрузки на эникейщиков, но обычно уровень технической подготовки у сотрудников разный, а правила одни на всех. Если ты чувствуешь, что ограничения мешают работе и личной свободе, а также здраво оцениваешь последствия, то у тебя есть все шансы собственноручно улучшить условия.

В ЧУЖОЙ МОНАСТЫРЬ СО СВОЕЙ ФЛЕШКОЙ

Получение нужных прав на рабочем компьютере в общем случае начинается с загрузки другой ОС с набором «хакерских» утилит. Мы уже писали о том, как создать мультизагрузочную флешку, а сейчас пройдемся по важным деталям.

Бывает, что загрузиться с проверенной флешки или Live CD очень непросто даже при наличии физического доступа к компьютеру. Загрузка с произвольного носителя не представляла проблем до появления EFI. Просто входишь в настройки BIOS и меняешь порядок загрузки в разделе Boot. На одних компах для этого надо было нажать Delete, на других F2 — в любом случае нужная клавиша указывалась на экране или в мануале. Сейчас же в UEFI используется список доверенных загрузчиков и два разных режима стартовой последовательности, а загрузка Windows 8, 8.1 и 10 для ускорения может происходить прямо из EFI безо всяких предложений войти в настройки.

Если ты сразу видишь загрузку Windows и не успеваешь ничего сделать, то дождись ее запуска и выполни одно из следующих действий:

1. Нажми «перезагрузить» на экране приветствия Windows, удерживая левую клавишу Shift.

2. Уже после загрузки зайди в «Параметры → Обновление и безопасность → Восстановление → Особые варианты загрузки». Нажми «Перезагрузить сейчас → Поиск и устранение неисправностей → Дополнительные параметры → Параметры загрузки».
3. Как вариант — можешь ввести shutdown.exe /R /O в командной строке.

Независимо от выбранного способа произойдет перезагрузка с выбором параметров, и ты сможешь оказаться в настройках BIOS/UEFI.

Если права жестко ограничены и войти в настройки Windows 10 софтовым методом невозможно, можешь попробовать физически отключить HDD/SSD. Тогда при следующей загрузке появится сообщение об ошибке и отобразится пункт для входа в UEFI.

Может показаться, что отключить питание HDD на рабочем компьютере сложно, особенно если корпус опечатан. Просто нажми на пластиковую заглушку слота 5,25″, которая обычно располагается на фронтальной панели. Чуть сильнее. Я сказал: «чуть»! Чувствуешь, как прогибается? Продавив ее миллиметра на три, попробуй ухватить край и вытащить заглушку. В образовавшееся отверстие спокойно пролезает рука до середины предплечья, даже если ты регулярно ходишь в качалку. Через эту амбразуру при должной ловкости можно не только кабель отключить, но и почти весь комп перебрать. Метод напоминает ремонт двигателя через выхлопную трубу, но действует в реальной жизни. Исключение составляют нестандартные корпуса — например, полностью алюминиевые.

Быстрая загрузка с флешки

Облегчить жизнь может опция быстрого выбора загрузочного устройства, реализованная в некоторых прошивках. Если она есть и активна, то при включении компьютера помимо сообщения «Press [key] to enter setup» появится еще одно: «... or [key] for boot menu». Обычно это клавиши Enter, F1 — F12, их сочетания с клавишами Alt, Ctrl, Ins и Esc. Полный список вариантов занял бы не одну страницу, так что лучше искать ответ в мануале к конкретной материнской плате.

Так или иначе, ты попадаешь в настройки BIOS. С большой вероятностью для загрузки с флешки также придется изменить параметр Boot List Option. По умолчанию он обычно стоит в новом режиме UEFI, а на флешке используется GRUB с за-

пуском через MBR. Поэтому нам нужен либо старый режим Legacy/CSM, либо оба, но с приоритетом классического: Legacy/CSM + UEFI. Иногда этот пункт отсутствует в списке. Тогда поддержку Legacy придется предварительно активировать на другой вкладке. Обычно этот пункт называется Load Legacy Option Rom. Там же отключается защищенный метод загрузки Secure Boot. При желании можно не отключать его, а добавить собственные ключи доверенных загрузчиков, но описание этого метода выходит за рамки статьи.

Другим препятствием может стать парольная защита BIOS/UEFI. Напоминаю, что пароль обычно записан с обратной стороны батарейки на материнской плате. Просто вытащи ее и переверни. Как не видишь пароля? Странно… Ладно, вставляй обратно. Пока ты крутил батарейку, он испарился вместе с другими данными CMOS. Если ветеринарные методы компьютерных операций тебе чужды или открыть корпус проблематично (например, он стоит у всех на виду), то попробуй ввести инженерный пароль. Он гуглится по производителю BIOS и общий у всех материнских плат одной серии.

Другой способ софтового сброса пароля на вход в BIOS — вызвать ошибку в контрольной сумме блоков данных. Для этого есть утилита Кристофа Гренье CmosPwd. Она прямо из Windows делает запись в CMOS. Метод не сработает, если утилиту заблокирует антивирус или если перезапись CMOS была предварительно отключена на низком уровне.

INFO

На некоторых ноутбуках, ультрабуках и неттопах временное обесточивание CMOS не приводит к сбрасыванию пароля на вход в BIOS/UEFI, поскольку он хранится в отдельной микросхеме энергонезависимой памяти. В таких случаях можно восстановить пароль по коду ошибки. Этот код отображается после трехкратного ввода неправильного пароля и представляет собой хеш от сохраненного пароля. Поскольку хеш-функции необратимы, то вычислить пароль напрямую нельзя. Однако существуют программы, подбирающие пароль с таким же значением свертки. Это может быть как заданный пароль, так и другая комбинация символов, дающая такой же хеш при проверке. Зайти в настройки можно по любому из них, так как проверяется именно хеш. Обрати внимание, что на некоторых ноутбуках Dell при вводе пароля надо нажимать Ctrl + Enter. Если ничего не помогло, то остается воспользоваться паяльником и программатором, но это уже хардкор для инженеров сервис-центров.

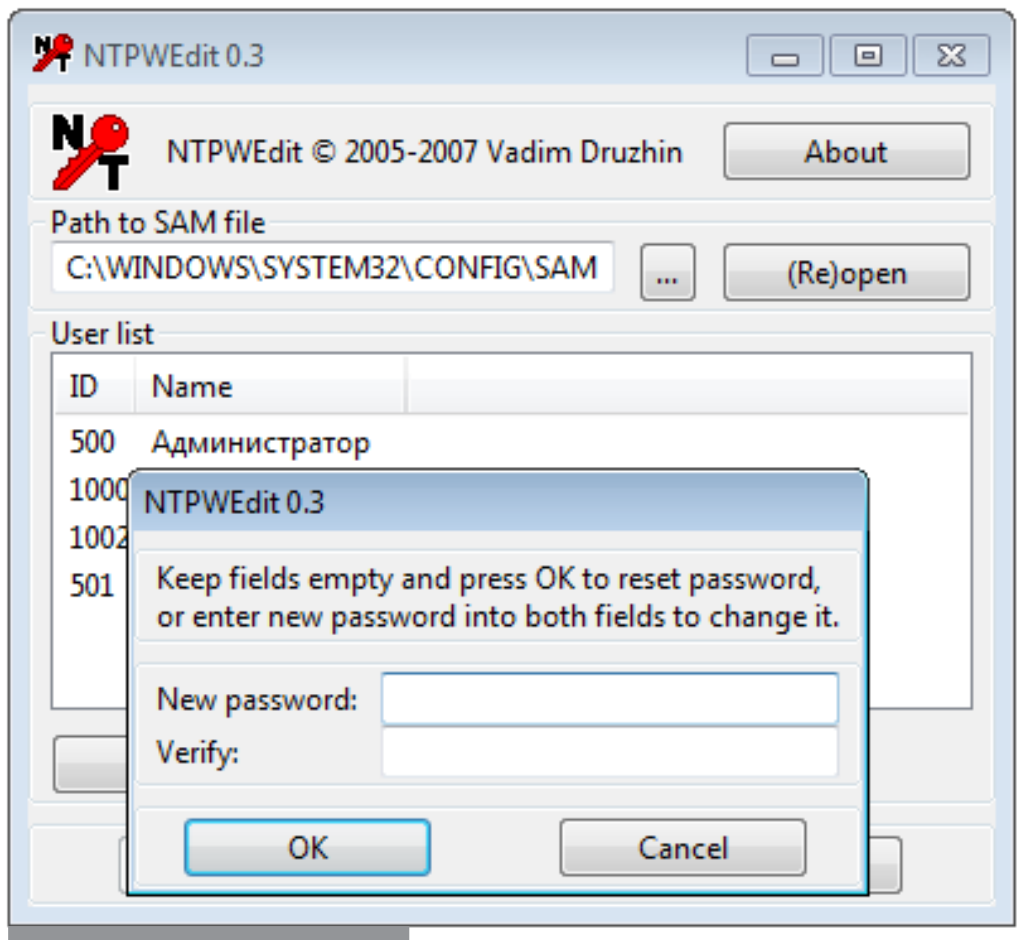
ОТКРЫВАЕМ ДОСТУП К ДИСКУ

Итак, предположим, что мы успешно загрузились с флешки и готовы к подвигам. С чего начнем? Первое ограничение, с которым сталкивается обычный пользователь, — отсутствие прав чтения и записи в определенных каталогах. Свободно использовать он может только домашнюю папку, что не слишком удобно.

Такие ограничения заданы на уровне списков управления доступом в файловой системе NTFS, но сверяться с ними обязана только сама винда. Другие ОС и отдельные утилиты способны игнорировать эти ограничения. Например, Linux и программы для восстановления данных не используют WinAPI, а обращаются к диску либо через свои драйверы, либо напрямую. Поэтому они просто не видят выставленные в NTFS атрибуты безопасности и читают все подряд.

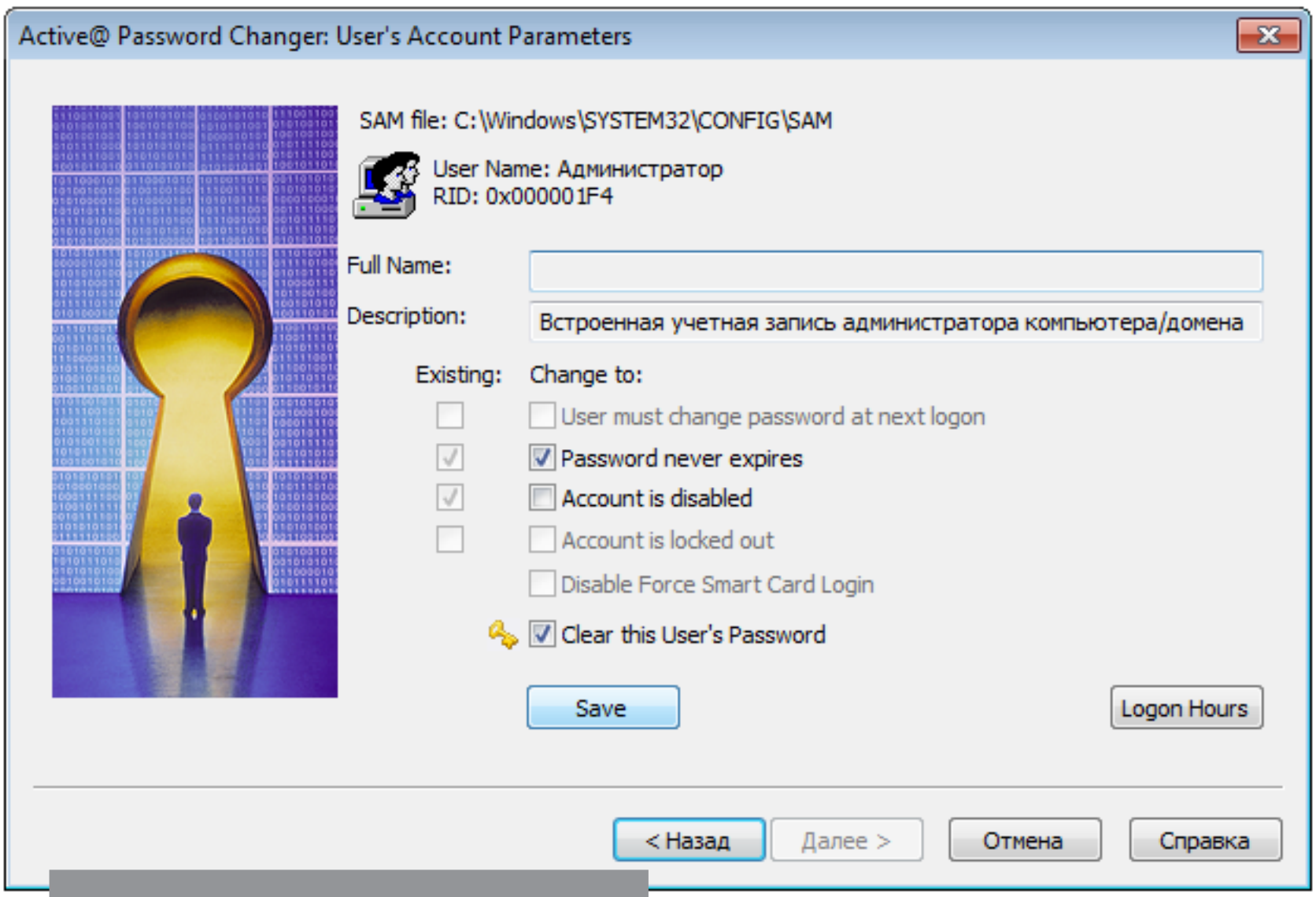
Сделать копию любых данных ты можешь уже на этом этапе. Единственное возможное препятствие — шифрование разделов. Встроенную защиту BitLocker помогут преодолеть утилиты ElcomSoft (кстати говоря, как и многие другие виртуальные заборы), а вот TrueCrypt, VeraCrypt и другие серьезные криптографические контейнеры придется вскрывать иначе. Проще всего делать это методами социального инжиниринга, поскольку техническая защита у этих средств на порядок выше, чем психологическая у владельца, — см. реальные примеры из жизни.

Заменить права доступа тоже несложно. Загрузившись с флешки, ты становишься админом в той же Windows PE и делаешь с диском что хочешь. Однако интереснее сохранить права в основной системе, для чего надо стать админом именно в ней. Для этого удобнее всего воспользоваться одной из утилит для сброса паролей. Например, простейшая программа NT Password Edit Вадима Дружина была написана более десяти лет назад, но актуальна до сих пор. С ее помощью можно удалить или задать новый пароль любой учетной записи Windows.



NT Password Edit

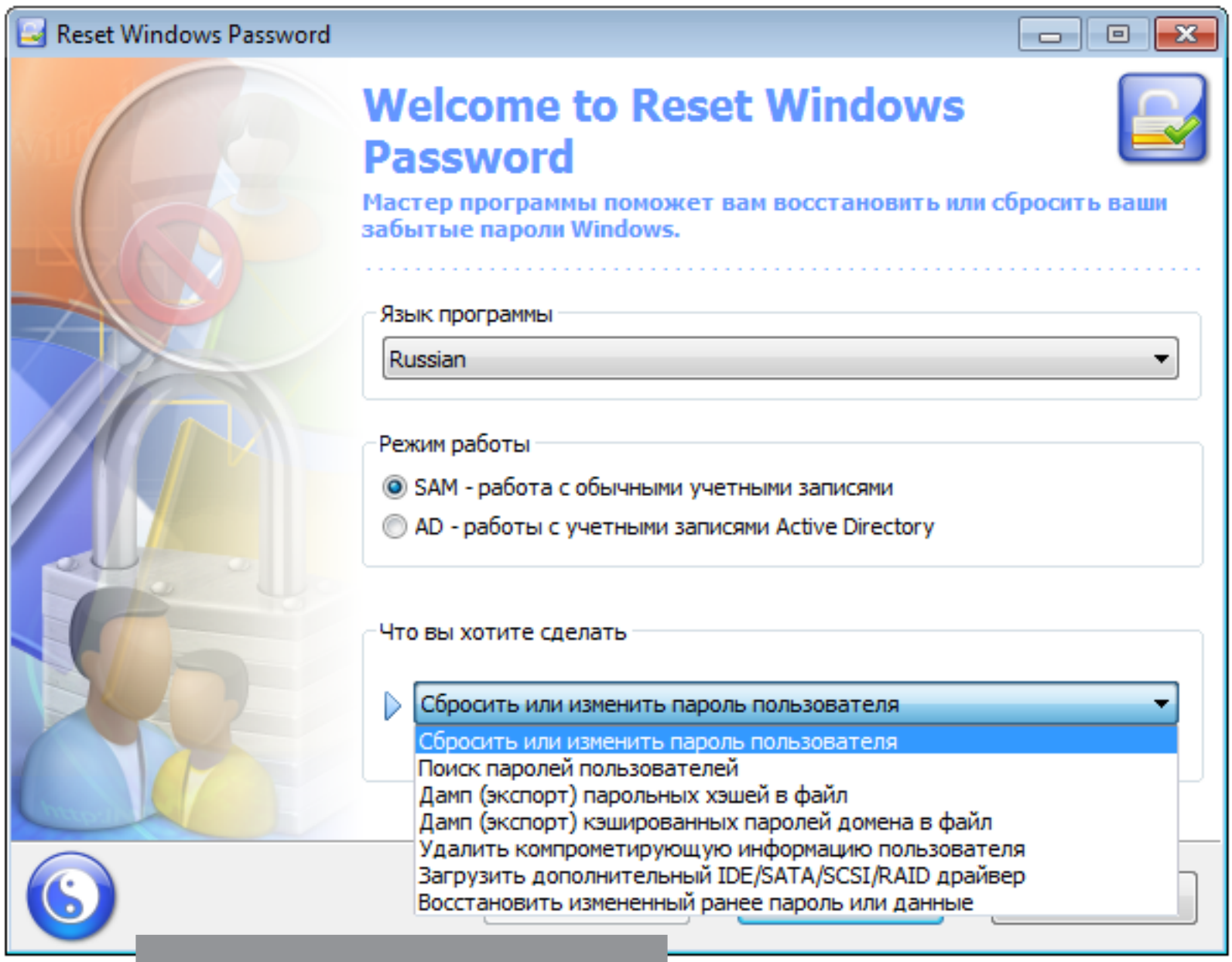
В большинстве случаев этой утилиты оказывается достаточно. Дальше остаются лишь рутинные операции вроде смены владельца и переустановки разрешений для выбранных каталогов. Чуть больше возможностей дает еще одна подобная утилита — Active@ Password Changer. Вместе с другими утилитами Active@ она добавляется на флешку как крошечный образ .ima, поэтому запуск бесплатной старой (но еще полезной) версии возможен даже без загрузки WinPE.



Активируем отключенные аккаунты

Password Changer также позволяет сбросить пароль любой учетной записи и умеет разблокировать ее, если она была отключена ранее.

Еще больше функций у программы Reset Windows Password. С ее помощью можно не только сбрасывать пароли, но и заметать следы взлома.



Сброс, дамп и заметание следов

Подобно SAMInside, она позволяет копировать пароли и хеши для их анализа на другой машине — так их проще вскрыть уже в спокойной обстановке (см. статью «Большой парольный коллайдер» в номере 194). Подобрать административный пароль куда интереснее, чем просто сбросить его: с исходным паролем ты будешь меньше светиться в логах, тогда как грубый взлом могут быстро заметить.

Еще один тонкий вариант — добавить в систему нового пользователя, наделить его желаемыми правами и скрыть эту учетную запись. Если пользователей десятки, то лишнего увидят нескоро. Проделав это, ты сможешь логиниться под обычным аккаунтом, не вызывая подозрений, а при необходимости запускать любую программу от имени одному тебе известной учетки с полным доступом. Конечно, полностью спрятать ее не удастся, но хотя бы на экране приветствия она маячить не будет. Для этого достаточно изменить подраздел UserList в реестре.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\↵
    Winlogon
```

Отыскиваем раздел SpecialAccounts или создаем его, если не нашелся. В этом разделе ищем или создаем подраздел UserList, а в нем — новый параметр типа DWORD с именем скрываемой учетки. Если присвоить ему нулевое значение, то соответствующая учетная запись не будет отображаться ни на экране приветствия, ни в общем списке из панели управления.

Можно пойти дальше и усилить конспирацию. Для этого отыскиваем ключи с говорящим названием dontdisplaylastusername и DontDisplayLockedUserId в этой ветке:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\↵
    Policies\System
```

Первому присваиваем значение 0x00000001, а второму — 0x00000002. Текущий и последний использованный аккаунт также исчезнут с экрана блокировки.

ПОТОКИ NTFS ПОМОГУТ ПОЛУЧИТЬ ДОСТУП К ФАЙЛАМ

Как уже отмечалось выше, большинство прав доступа на рабочих компьютерах с Windows задается на уровне файловой системы NTFS. Тут самое время вспомнить про файловые потоки и особенности синтаксиса. Согласно универсальному соглашению об именовании файлов (UNC), двоеточие отделяет букву диска от дальнейшего пути. В NTFS этот знак используется еще и как разделитель между собственно именем файла и связанным с ним файловым потоком.

Если настройки прав для каждого файла и каталога Windows корректны, то нет разницы, как именно обращаются к объектам файловой системы. Доступ всегда будет блокироваться при отсутствии необходимых разрешений. Однако настройка прав — долгая рутинная операция, которую в последние годы админы часто стали упрощать, используя сторонние программы. Далеко не все из них (даже сертифицированные) корректно работают с файловыми потоками. Поэтому, если не удается прочитать filename.ext, попробуй обратиться к потоку данных этого файла с помощью конструкции filename.ext:stream:$DATA или filename.ext::$DATA.

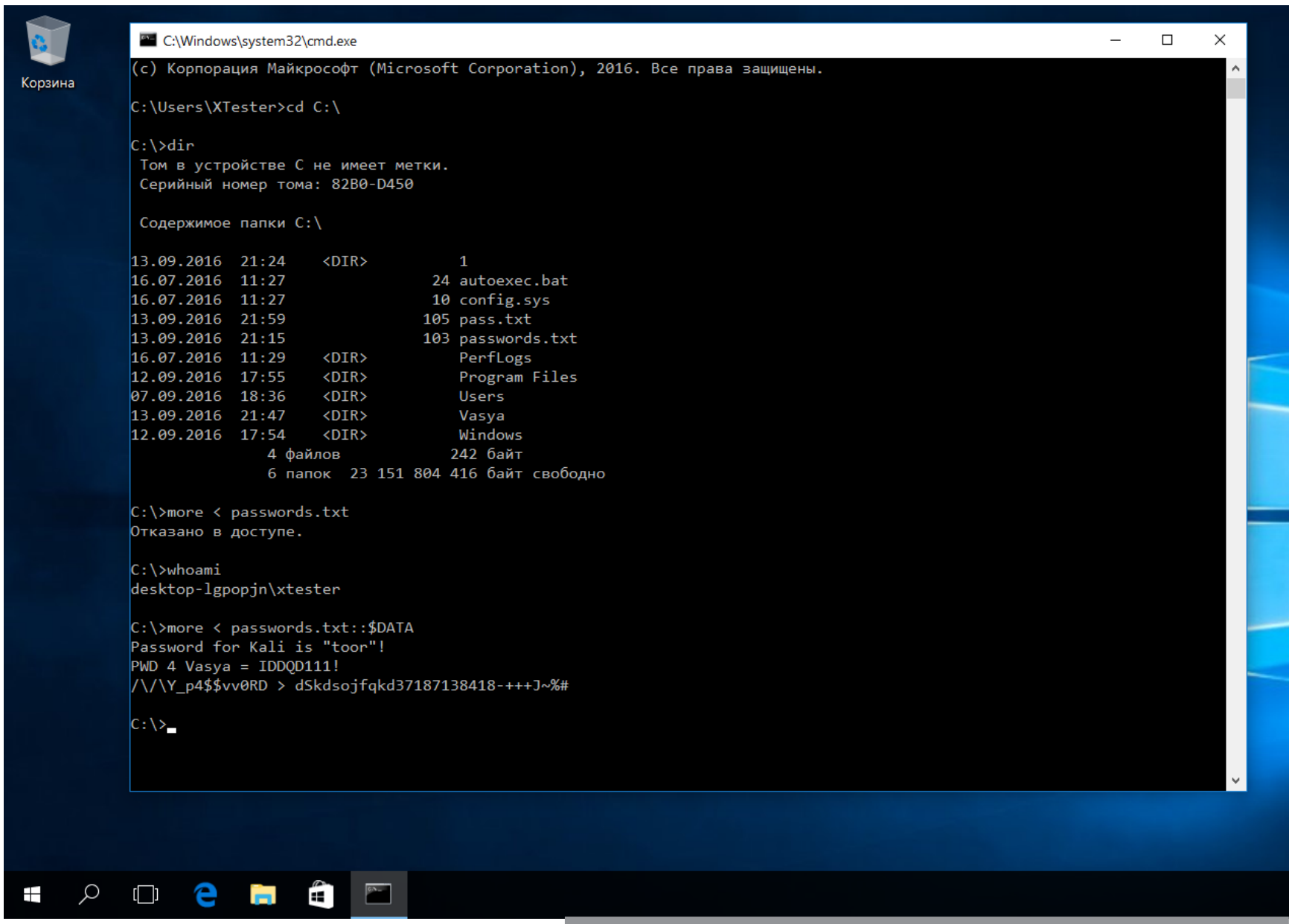
Например, если у тебя нет доступа к файлу passwords.txt, то следующая команда все равно выведет его содержимое на экран:

```
more < passwords.txt::$DATA
```

Примерно так же можно скопировать содержимое файла, перенаправив вывод команды more не на экран, а в другой файл.

```
more < passwords.txt::$DATA > pass.txt
```

Это не должно срабатывать при корректном выставлении ограничений чтения/записи, но админы частенько не утруждают себя аудитом прав доступа на каждый объект файловой системы. На реальном компьютере нередко получается гремучая смесь из явно заданных и унаследованных прав, противоречиями в которых можно воспользоваться в своих интересах..



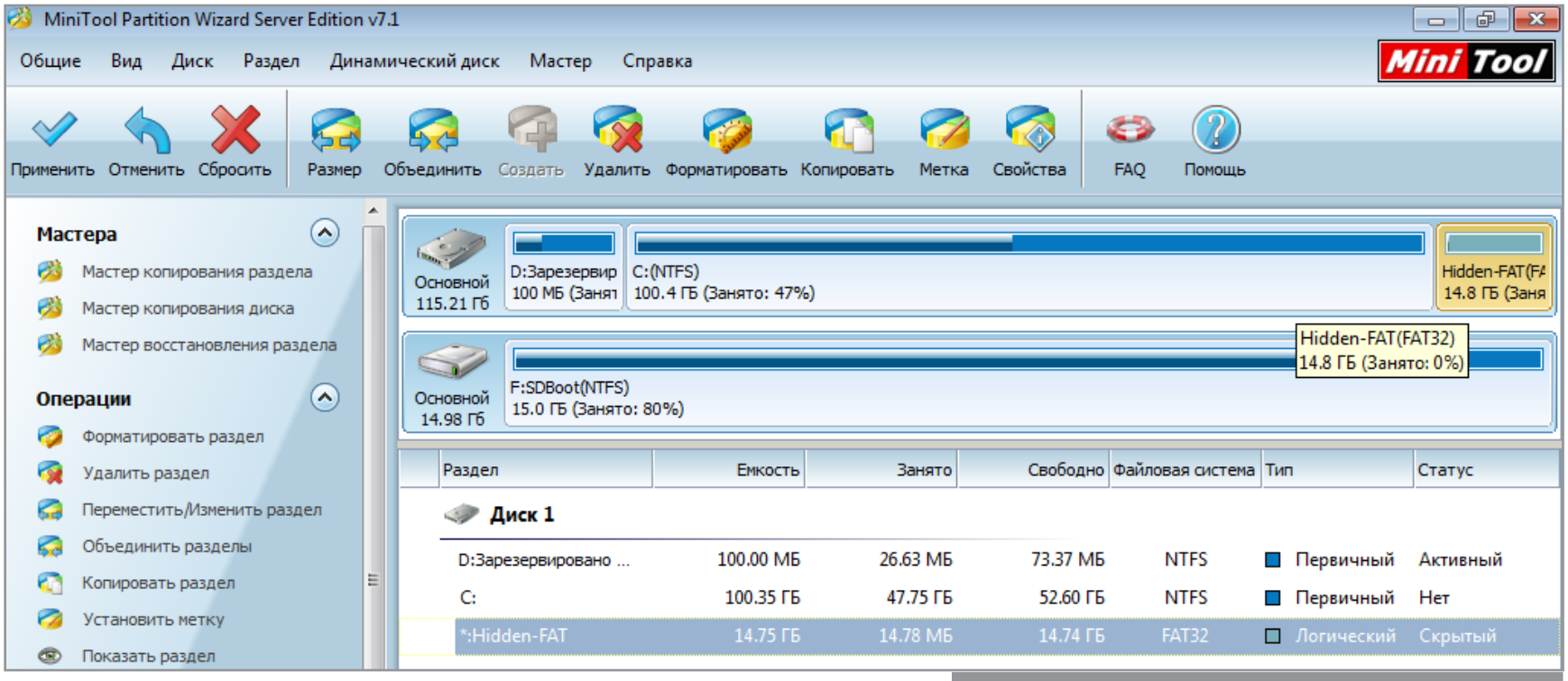
Читаем файл из потока данных прямо в консоль

Кстати, о механизмах наследования. Встречаются ситуации, когда админ запрещает доступ к подкаталогу для определенных пользователей, но оставляет для них же полный доступ к директориям верхнего уровня. При этом возникает явное противоречие, и ограничения перестают действовать. Например, отсутствие прав на чтение файла не работает, если разрешено читать список содержащего его каталога. Аналогично и с удалением.

СОЗДАЕМ СЕКРЕТНЫЙ РАЗДЕЛ БЕЗ ПОДДЕРЖКИ ПРАВ ДОСТУПА

Иногда админы запрещают только выполнение файлов. Например, чтобы пользователь не смог запустить какую-то программу. Обойти это ограничение можно, просто скопировав ее на раздел FAT32 (как вариант — на ту же флешку),

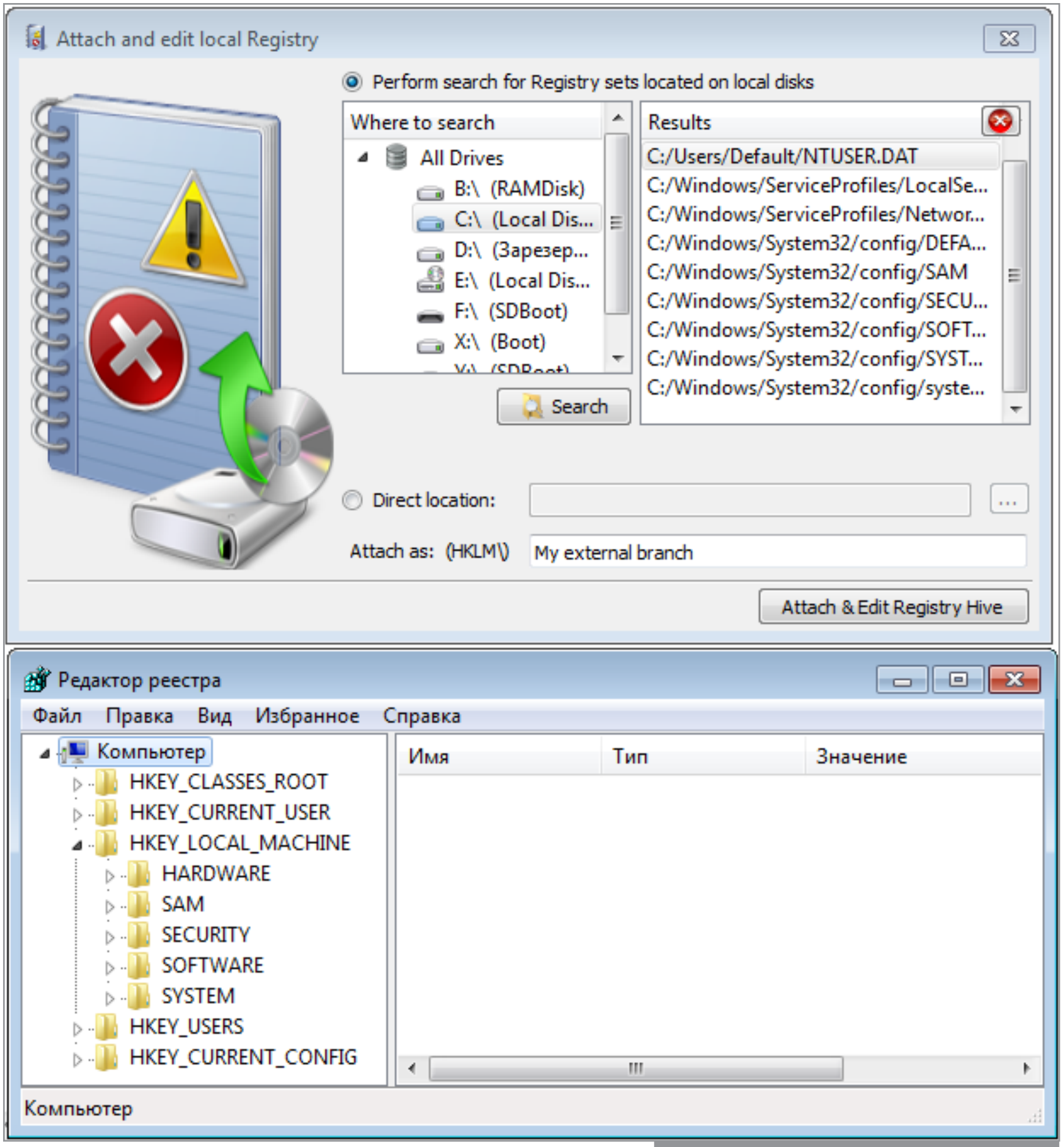
где права доступа уже задать невозможно. Их просто не поддерживает сама файловая система. Если же постоянно пользоваться флешкой слишком рискованно, то можно сделать хитрее. Один раз запустить с нее любой редактор дисковых разделов, уменьшить размер системного, а на освободившемся месте создать новый том FAT32 и (опционально) скрыть его.



Создаем скрытый раздел FAT32

Скрытым разделам не присваивается буква диска, поэтому они не отображаются в «Проводнике» и файловых менеджерах. Смонтировать его в Windows можно через «Управление дисками» — diskmgmt.msc. Необходимые права для запуска этого инструмента ты уже назначил себе на прошлом этапе, когда узнавал пароль админа или создавал нового.

Если на раздел FAT32 копировались документы, базы или медиафайлы, то они будут открываться без проблем. Ничто не помешает и запускать простой софт, который ставится распаковкой: на новом месте все будет работать, как и раньше. Вот с установленными программами не все так просто. У них придется менять пути в настройках. Это либо файлы .cfg и .ini в том же каталоге, либо ключи реестра. Изменить ключи можно при помощи удаленного редактора реестра, запускаемого с флешки в той же WinPE.



Редактируем реестр другой ОС

С таким инструментом можно обойти и другие ограничения, прописанные в реестре.

ОБХОДИМ АНТИВИРУС КАСПЕРСКОГО

Большая часть запретов на действия пользователя в Windows реализована через реестр и права доступа в NTFS. Однако есть и другой вариант: установка специализированных программ контроля.

Например, софт «Лаборатории Касперского» загружает собственные драйверы из \windows\system32\drivers\ и sysnative\drivers. С их помощью он перехватывает системные вызовы и обращения к файловой системе, контролируя как работу программ, так и действия пользователя. Обычно админ закрывает изменение настроек антивирусного софта паролем. Хорошая новость заключается в том, что есть простые процедуры сброса такого пароля.

«Антивирус Касперского SOS» и версии для Windows Workstation проверяют имя главного файла. Поэтому достаточно проделать следующее:

- переименовать avp.exe (загрузившись в WinPE или в безопасном режиме);
- запустить переименованный файл после обычного входа в систему;
- зайти в меню «Настройка → Параметры», отключить самозащиту и защиту паролем;
- сохранить настройки, выгрузить антивирь и переименовать его обратно.

При желании можно задать собственный пароль, чтобы админ понял, как ты мучился, не зная его.

Этот метод не сработает, если антивирус на твоем компе настраивается централизованно. Однако ты всегда можешь временно нейтрализовать сторожа описанным выше способом.

С новыми продуктами Касперского все еще проще. Итальянский консультант Kaspersky Lab Маттео Ривойра написал скрипт (http://media.kaspersky.com/utilities/ConsumerUtilities/KLAPR.zip), который автоматически определяет установленную версию антивируса и обнуляет заданный пароль. Из батника видно, что в 32-битных и 64-разрядных версиях винды он хранится в разных ветках реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\[имя_продукта]\settings
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\[имя_продукта]\
    settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\[имя_продукта]\
    settings
```

Поэтому либо просто запусти этот bat, либо правь реестр вручную из-под WinPE. Просто проверь эти ветки и присвой параметру EnablePasswordProtect нулевое значение DWORD.

ДОБАВЛЯЕМ ТРОЯНСКУЮ ЗАКЛАДКУ

Мультизагрузочная флешка — настоящий швейцарский нож. После загрузки с нее можно разблокировать скрытые учетные записи, сбрасывать пароли, править реестр и вообще творить что угодно. Проблема одна: ее могут заметить. Поэтому сделаем себе дополнительный лаз, который не требует внешних инструментов. Создать его можно в том числе и через консоль восстановления. Так или иначе, ты можешь сделать копию файла utilman.exe, а затем заменить его на cmd.exe. Сначала сделаем копию исходного файла.

```
copy %windir%\system32\utilman.exe %windir%\system32\utilman-new.exe
```

Затем перезаписываем исходный файл utilman.exe файлом cmd.exe:

```
copy %windir%\system32\cmd.exe %windir%\system32\utilman.exe
```

Буква диска (системного раздела) в переменной %windir% не обязательно будет C:\. Ее можно узнать при помощи утилиты diskpart — командой list volume.

После замены utilman.exe файлом cmd.exe при следующей загрузке Windows ты увидишь привычный экран приветствия. Только при клике на «Специальные возможности» теперь будет открываться командная строка.

В ней можно делать все то же, что и обычно. Например, можешь выяснить актуальный список учетных записей командой net user и поменять их параметры. Делаешь с любым аккаунтом что угодно — активируешь и деактивируешь, меняешь пароли, изменяешь сроки их действия и так далее. Подробнее интаксисе читай в справке на сайте Microsoft.

ОБХОДИМ ЛОКАЛЬНЫЕ ГРУППОВЫЕ ПОЛИТИКИ

Подробнее о политиках поговорим чуть позже (не люблю я их, политиков), а пока разберем простейший пример — ограничение на запуск программ через административные шаблоны.

Админы очень любят редактор gpedit.msc. Одна из самых востребованных настроек в нем называется «Выполнять только указанные приложения Windows». Обычно при помощи этого инструмента офисному планктону разрешают запуск только приложений из белого списка. В него вносят Word, Excel, калькулятор и прочие безобидные вещи. Все остальные имена исполняемых файлов автоматически попадают под запрет. Обрати внимание: именно имена. Поэтому берем тот же cmd.exe или totalcmd.exe, переименовываем в winword.exe и спокойно пользуемся. Посмотреть (и поменять) ограничения можно через тот же редактор удаленного реестра в WinPE. Они записаны в этой ветке:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\↵
    Policies\Explorer\RestrictRun
```

СТРЯХИВАЕМ ДОМЕННЫЕ ПОЛИТИКИ

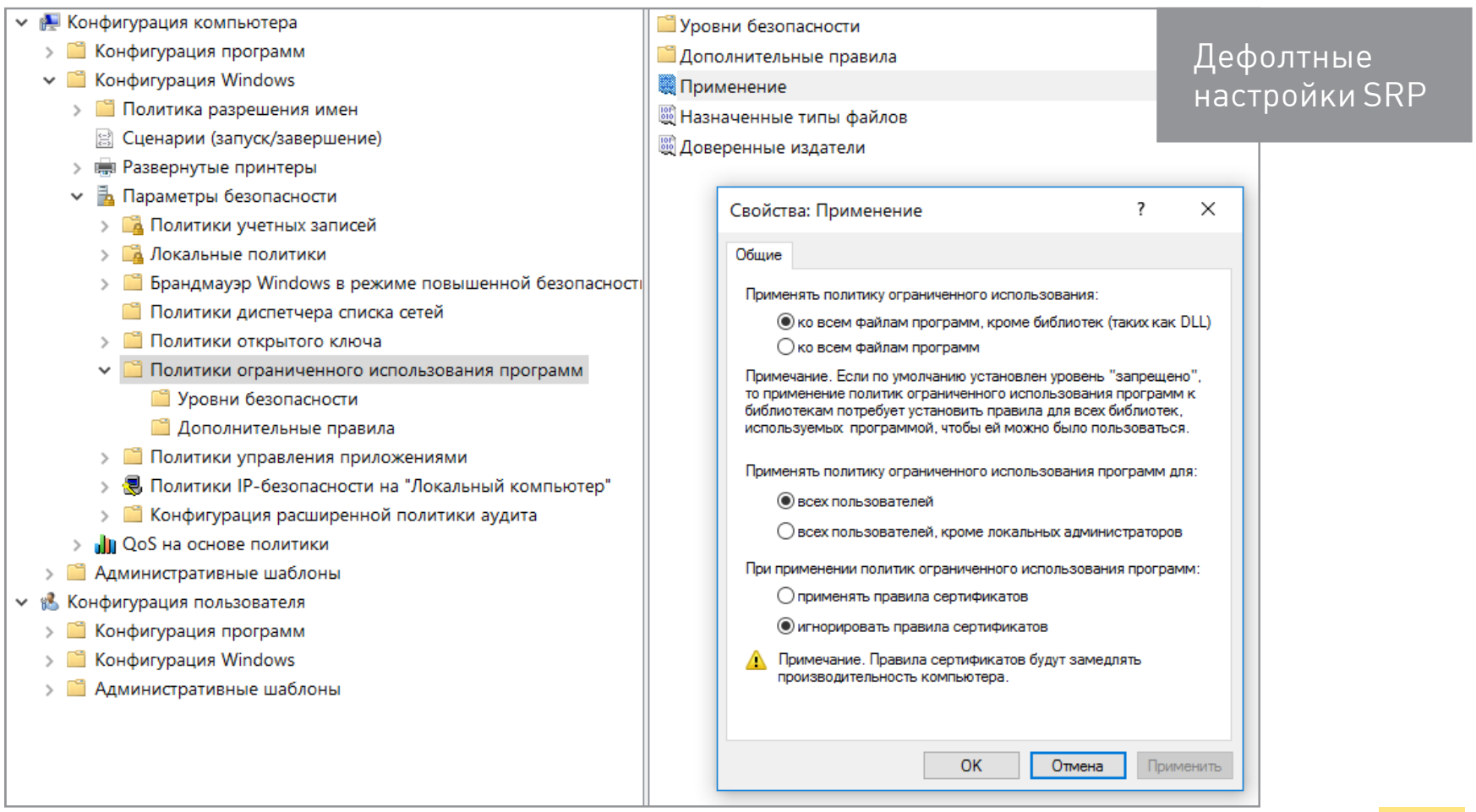
В домене компьютеры управляются централизованно через групповые политики, однако и этот заслон можно преодолеть. Самый простой способ — не дать политикам загрузиться. Для этого запускаешь Windows в безопасном режиме или просто отключаешь машину от локальной сети при включении. Во втором случае ты сможешь залогиниться в домен даже без физического подключения к нему, поскольку Windows кеширует данные предыдущего входа и при потере связи с контроллером домена выполняет проверку локально.

После входа можешь снова подключиться к локалке и работать как обычно, только уже без активных политик. Минус этого способа состоит в неизбирательном подходе. В политиках записаны не только ограничения, но и дополнительные ресурсы, вроде выделенной сетевой папки. Впрочем, к этому времени у тебя уже должны быть достаточные права, чтобы восстановить утрату самостоятельно.

ОБХОДИМ ПРОДВИНУТЫЕ ЗАПРЕТЫ НА ЗАПУСК ПРОГРАММ

В домене используется более продвинутый инструмент ограничения запуска программ — SRP. Он умеет проверять, помимо имён исполняемых файлов, их пути, хеши и сертификаты. Простым переименованием экзешника его не одурачить. Как же быть? Аналогично: просто не дать системе увидеть эти ограничения.

По умолчанию контролируется только запуск программ, но не динамических библиотек, поскольку тотальная проверка отнимает слишком много ресурсов.



Дефолтные настройки SRP

Еще в 2005 году Марк Руссинович написал утилиту Gpdisable. Она выполняет инжект библиотеки в любой процесс, и тот перестает видеть запреты групповой политики из соответствующей ветки реестра.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\↵
    CodeIdentifiers
```

Затем схожую тактику реализовал Эрик Ракнер (Eric Rachner) в своей утилите Group Policy Bypassing Tool — тогда он еще был руководителем команды Application Consulting Engineering (ACE team) в Microsoft.

Обе программы имеют одинаковый недостаток: чтобы запустить их и внедрить .dll, пользователь уже должен иметь некоторые административные привилегии. Но если они у него есть, то смысл в этих утилитах теряется. Локальному админу ничто не мешает убрать ограничения доменных политик вручную.

В блоге ACROS Security лет пять назад был описан другой способ обхода доменных ограничений, применимый в реальной ситуации с правами простого пользователя.

4. Переименовываем внедряемую библиотеку gpdisable.dll в deskpan.dll.
5. Создаем новую папку с именем `files.{42071714-76d4-11d1-8b24-00a0c9068ff3}`.
6. Помещаем в нее файл deskpan.dll и открываем папку.
7. Создаем в ней новый документ .rtf и открываем его.

При этом загружается WordPad, который подгружает в память gpdisable.dll под видом deskpan.dll. Разберём метод подробнее.

Deskpan.dll — это расширение CPL панорамирования дисплея, стандартная библиотека в Windows, на которую не распространяются ограничения SRP. В системе она зарегистрирована как COM-сервер с глобальным идентификатором класса {42071714-76d4-11d1-8b24-00a0c9068ff3}. Если мы запускаем доверенное приложение из папки, в названии которой есть ID этого класса после точки, то оно создает экземпляр COM-сервера и выполняет загрузку deskpan.dll из текущего рабочего каталога.

В изложенном варианте этот метод работает только в Windows XP, но для более свежих версий винды его несложно модифицировать. Принцип остается прежним.

Например, в Windows 7 можно использовать COM-сервер AnalogCable Class (\System32\PsisDecd.dll), зарегистрированный с идентификатором CLSID {2E095DD0-AF56-47E4-A099-EAC038DECC24}. При обращении к PsisDecd.dll загружается библиотека ehTrace.dll, поиски которой начинаются с текущего каталога. Поэтому аналогичный сценарий внедрения gpdisable.dll можно реализовать даже с помощью «Блокнота».

1. Переименовываем gpdisable.dll в ehTrace.dll.
2. Создаем новый текстовый документ.
3. Создаем каталог с именем **`files.{2E095DD0-AF56-47E4-A099-EAC038DECC24}`** и помещаем в него оба файла (библиотеку и текстовый документ).
4. Дважды кликаем на текстовый файл и открываем в «Блокноте» пункт «Сохранить как».

В этот момент в память загружается gpdisable.dll.

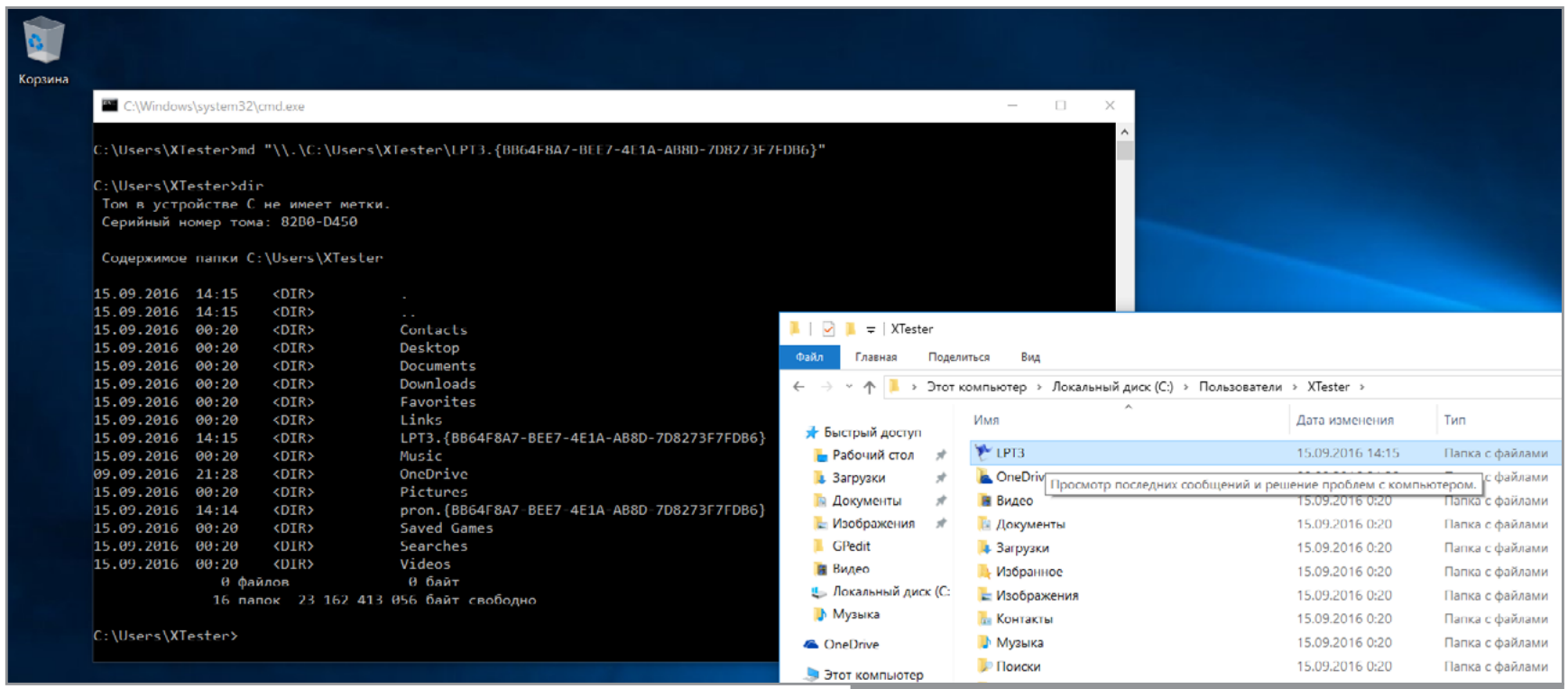
СОЗДАЕМ ХИТРЫЕ ЯРЛЫКИ

Трюки из предыдущего раздела возможны потому, что в Windows наряду с обычными папками используются папки-ярлыки с предопределенными функциями. Например, «Мой компьютер», «Панель управления» или «Принтеры». Все они реализованы как COM-серверы с известными идентификаторами класса (CLSID). Всего их больше ста, поэтому перечислю только новые в Windows 10:

- {3936E9E4-D92C-4EEE-A85A-BC16D5EA0819} — часто используемые папки;
- {018D5C66-4533-4307-9B53-224DE2ED1FE6} — OneDrive;
- {679f85cb-0220-4080-b29b-5540cc05aab6} — панель быстрого доступа;
- {BB64F8A7-BEE7-4E1A-AB8D-7D8273F7FDB6} — безопасность и обслуживание.

Любой из них можно использовать для скрытого запуска своих программ.

В примере ниже я создаю в пользовательской директории подпапку с именем LPT3.{BB64F8A7-BEE7-4E1A-AB8D-7D8273F7FDB6}. Имя до точки запрещено в Windows, поскольку совпадает с названием порта. Чтобы его создать, потребуется запутать командный интерпретатор последовательностью \\.\ и передать полный путь к создаваемому каталогу как аргумент в кавычках.



Создаем скрытую неудаляемую папку

После этой команды получаем неудаляемый штатными средствами каталог, который в проводнике отображается как LPT3. При двойном клике на нем содержимое папки не открывается. Вместо этого запускается «Центр безопасности и обслуживания». При этом лежащие внутри папки экзешники будут доступны из командных файлов (.bat и .cmd) и из реестра (например, в секции автозагрузки).

ВКЛЮЧАЕМ USB

Одним из препятствий для использования флешки может быть отключение админом портов USB на твоем компьютере. Сделать это можно разными способами, поэтому и методы противодействия требуются разные.

1. Порты физически отключены

Такое возможно только с дополнительными портами, которые подключаются кабелем к материнской плате. Задние порты распаяны на самой материнке, и их минимум две штуки. Поэтому принеси из дома копеечный хаб, воткни его вместо мышки или клавиатуры и подключай всю штатную периферию через него. Второй порт оставь для загрузочной флешки.

2. Порты отключены в BIOS/UEFI

Админ может отключить как порты вообще (редкий случай), так и отдельную опцию USB Boot. Именно она отвечает за возможность загрузки с USB-носителей. Как входить в настройки BIOS, мы уже разобрали, а отыскать нужную опцию не составит труда.

3. Удалены драйверы контроллера USB

Хитрые админы просто сносят драйверы USB через диспетчер устройств, но тебя это не остановит. Загрузиться с флешки отсутствие драйверов не помешает. Став локальным админом, ты легко доустановишь отсутствующие драйверы — Windows сама предложит это сделать.

4. Заблокированы отдельные устройства USB

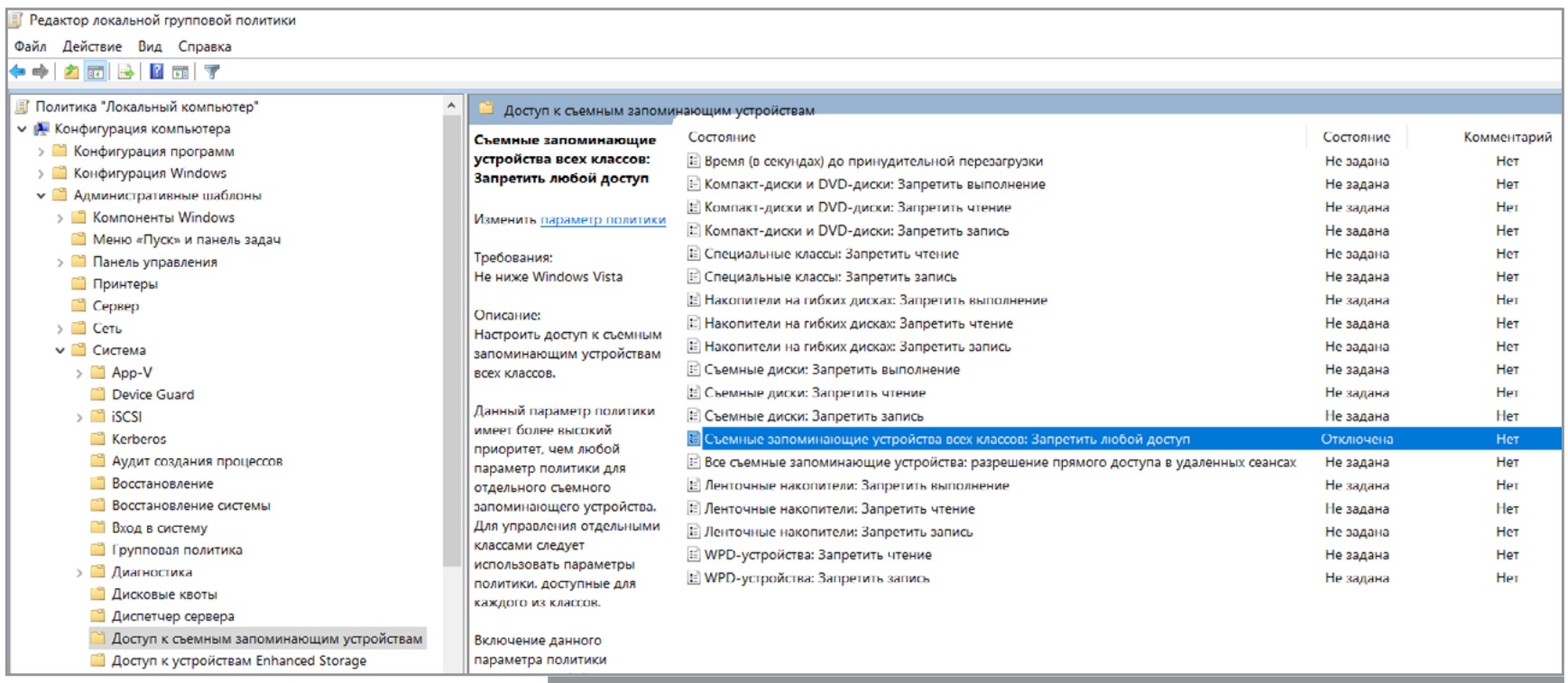
Более тонкий метод — запрет использования именно USB-накопителей. При этом другие типы устройств с интерфейсом USB продолжают работать. Задается ограничение через ветку реестра

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
```

При значении параметра Start 0x00000004 использование флешек и внешних дисков запрещено, а при 0x00000003 — разрешено. Бороться с этим можно тем же методом, что и в предыдущем пункте: загружаемся с флешки и меняем секцию USBSTOR через офлайновый редактор реестра.

5. USB-накопители запрещены через групповую политику

Редактор групповых политик позволяет задать административный шаблон, запрещающий доступ к съемным запоминающим устройствам. Вновь загружаемся с флешки, узнаем пароль локального админа (или сбрасываем, если не удалось узнать), попутно активируем учетку, если она была отключена. После этого запускаем gpedit.msc и отключаем запрет.



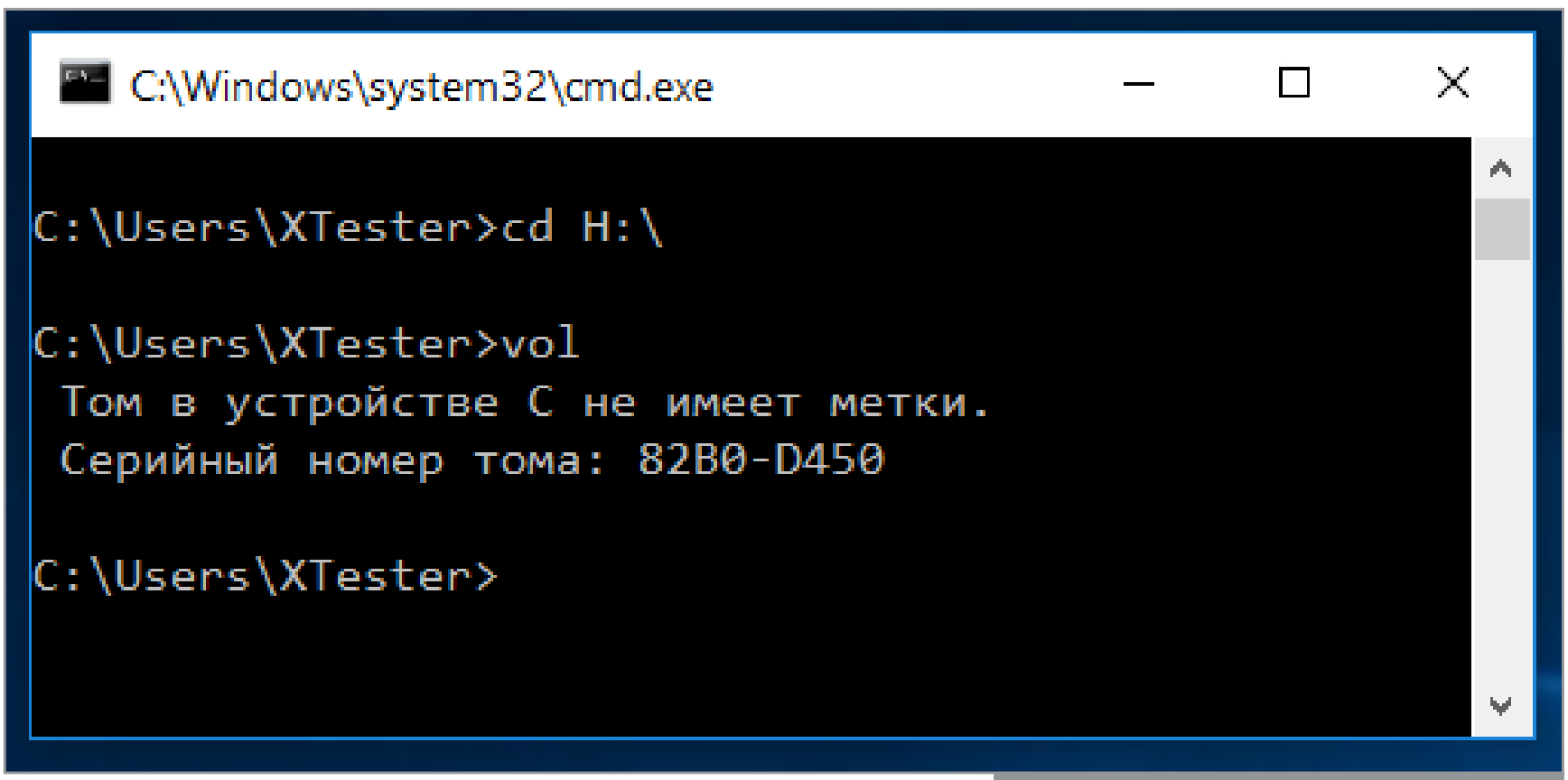
Отключаем запрет на использование USB-накопителей

6. Ограничены права на чтение файлов usbstor.inf и usbstor.pnf в каталоге \Windows\Inf

Очередной трюк с правами NTFS. Если невозможно обратиться к этим файлам в ограниченной учетной записи, то не будут подключаться флешки. Используем права локального админа либо просто перемещаем эти файлы через WinPE на том FAT32. После обратного перемещения в \inf\ права доступа слетят.

7. Подключение устройств по USB контролируется отдельной программой

В помощь админам было написано множество утилит для ограничения использования флешек и внешних дисков. Большинство таких программ просто меняет значение упомянутой выше ветки реестра, но есть и продвинутые варианты. Такие умеют запоминать разрешенные флешки по номеру тома (VSN — Volume Serial Number) и блокировать остальные. Можно просто выгрузить процессы этих программ из памяти или подменить VSN. Это 32-битное значение, которое присваивается тому при его форматировании по значению текущей даты и времени.



Узнаем серийный номер тома

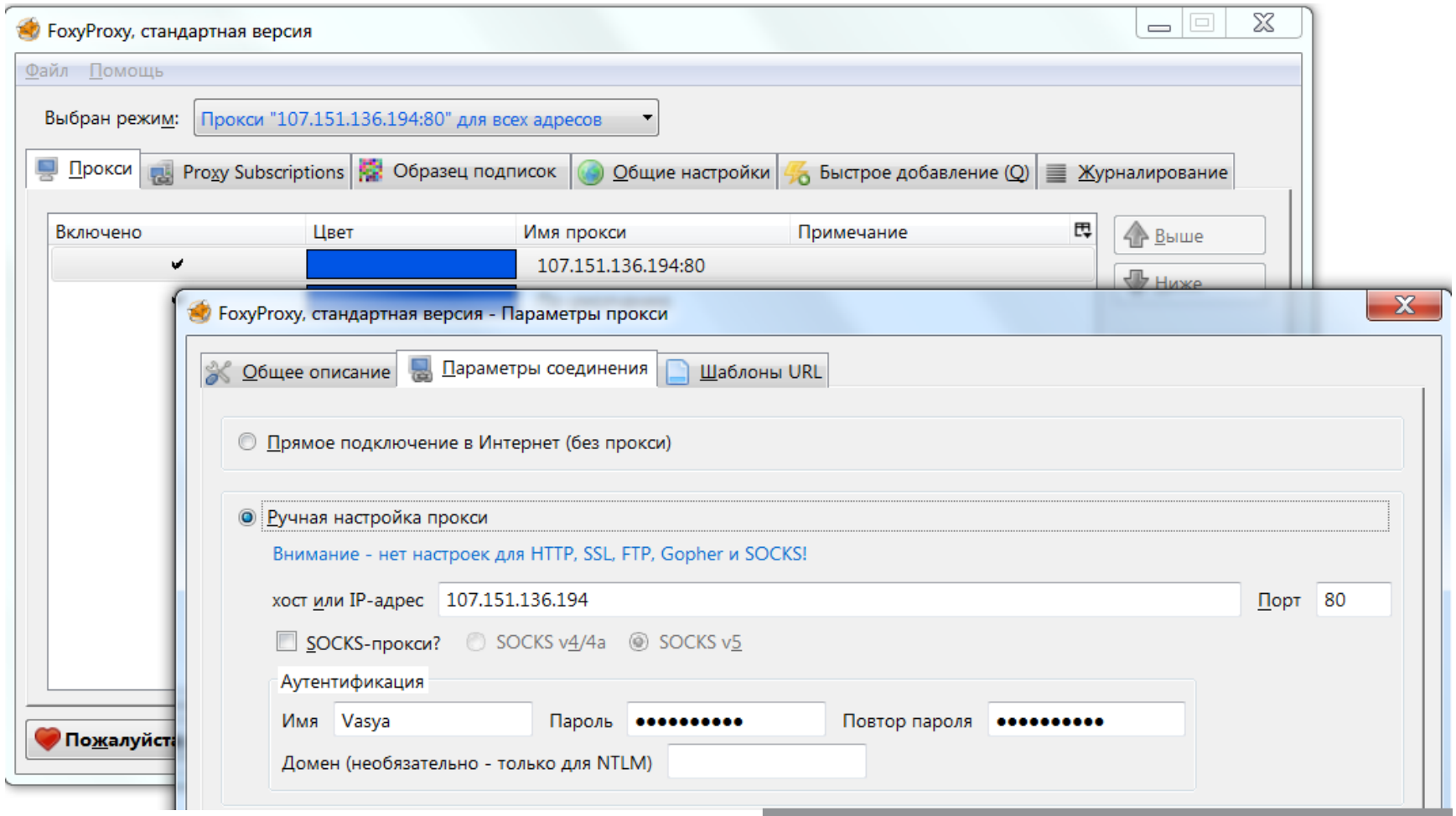
Узнать VSN доверенной флешки можно командой vol или dir. С помощью программы Volume Serial Number Changer присваиваешь такой же номер своей флешке и свободно ей пользуешься. Для надежности замени еще и метку тома (просто через свойства диска).

Другой вариант противодействия — нарушать работу программ контроля, временами загружаясь с флешки и меняя названия ее рабочих файлов (или удаляя из автозагрузки). Если делать все аккуратно, админ сочтет программу глючной и сам удалит ее.

Неожиданное препятствие для использования флешек возникает на компах с посредственным блоком питания (читай — на большинстве дешевых рабочих машин) безо всяких стараний админа. Дело в том, что шина 5 В просаживается настолько, что флешке не хватает питания. В таком случае отключи другое устройство из соседнего (парного) USB-порта или используй активный хаб с собственным блоком питания. Через него можно запитать хоть внешний винчестер.

ПОДКЛЮЧАЕМСЯ К ИНТЕРНЕТУ

Масса ограничений на работе касается использования интернета. В общем случае их можно обойти, перенаправляя весь трафик на неподконтрольный компании сервер. Например, использовать анонимный прокси-сервер через браузерный аддон FoxyProxy или аналогичный. Если менять адрес прокси почаще, то вычислить его использование будет сложнее. Подняв прокси-сервер дома, ты повысишь скорость и защищенность соединения, а заодно и получишь доступ к своей локалке..



Добавляем свой или публичный прокси

Иногда проблема заключается не столько в запрете посещения определенных сайтов, сколько в квоте трафика. Сделать безлимитное подключение сегодня проще всего с помощью смартфона. Подключив выгодный тариф на мобильный интернет, можно раздавать трафик по Wi-Fi или использовать USB-tethering. Подключенный кабелем смартфон не светится в эфире и вызывает меньше подозрений. Ты его заряжаешь от рабочего компьютера, какие проблемы?

Все описанные методы имеют ограниченное применение из-за многообразия вариантов конфигурации. Пошаговые инструкции устаревают быстро, но общие принципы остаются неизменными годами.

WWW

Современный сервис подбора паролей к BIOS по коду ошибки

Программа Кристофа Гренье для дампа CMOS и обнуления пароля (zip)

Скрипт для сброса пароля от разных версий антивируса Касперского (zip)

Утилита для смены VSN