КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

19 апреля 2018 г.
г. Минск

#CODEIB

MOBILE & PRIVACY

КОТ ИБ
corporation

КОТ ИБ

ВЛАДИМИР БЕЗМАЛЫЙ,
НЕЗАВИСИМЫЙ ЭКСПЕРТ В ОБЛАСТИ ИБ

EMAIL: CYBERCOP@OUTLOOK.COM

ОБ АВТОРЕ

- Опыт работы в области ИБ с 1990 года;
- Автор более 800 печатных публикаций и двух книг Security Awareness:
  - **«Цифровая гигиена»;**
  - **«Цифровая гигиена Том 2».**

MVP Microsoft Most Valuable Professional

CompTIA Security+ CERTIFIED

KASPERSKY lab CERTIFIED Trainer

KASPERSKY lab CERTIFIED Consultant

Microsoft | Security Trusted Advisor

МОБИЛЬНОЕ УСТРОЙСТВО – ВАШ ПЕРСОНАЛЬНЫЙ ШПИОН

"...знаете ли: лучше быть живым параноиком, чем мертвецом, который ждал от жизни только приятных неожиданностей...“

Макс Фрай

УГРОЗЫ ПРИ ИСПОЛЬЗОВАНИИ СМАРТФОНОВ

- Перехват и прослушивание речи абонентов;
- Фальсификация речи абонентов с целью компрометации;
- Дистанционное включение микрофона и камеры телефона и последующее несанкционированное прослушивание разговоров, фото- и видеосъемка;
- Отправка сообщений SMS и MMS, которые содержат вирусы, осуществляющие кражу информации;
- Неавторизованный доступ к мобильному телефону;
- Вредоносное программное обеспечение, способное выполнять не санкционированные абонентами удаленные команды;

УГРОЗЫ ПРИ ИСПОЛЬЗОВАНИИ СМАРТФОНОВ

- Ложные аутентификация и авторизация ведут к несанкционированному доступу к информации, в том числе путем подделки уникального идентификатора абонента;
- Ложная базовая станция, так называемая ловушка IMSI, которая понижает стандартный уровень шифрования и облегчает перехват и прослушивание данных мобильных телефонов;
- Утрата данных из потерянных или украденных мобильных телефонов;
- Выделение гармоник сигнала микрофона с антенны мобильного телефона, которые могут быть перехвачены до того, как сигнал будет принят ближайшей станцией GSM-связи;
- Вскрытие защиты модулей беспроводной высокочастотной связи малого радиуса действия Near Field Communication (NFC), встроенных в мобильные телефоны.

КОМПРОМАТ

- Сколько пользователей хранят на своих мобильных устройствах конфиденциальную информацию как свою, так и своего работодателя?

  70.7%

- Криминал в России зарабатывает на сборе компромата, включая прослушивание мобильной связи, около

  1 000 000 000 долларов США в год

- Цена системы прослушивания от

  2 000 до 50 000 долларов США

- Цена прослушивания 1 абонента –

  1500 долларов ежемесячно

- При смене SIM-карты ваш голос будет засечен после примерно

  30 секунд разговора

- Подделка голоса и речи человека с использованием цифрового синтезатора стоит

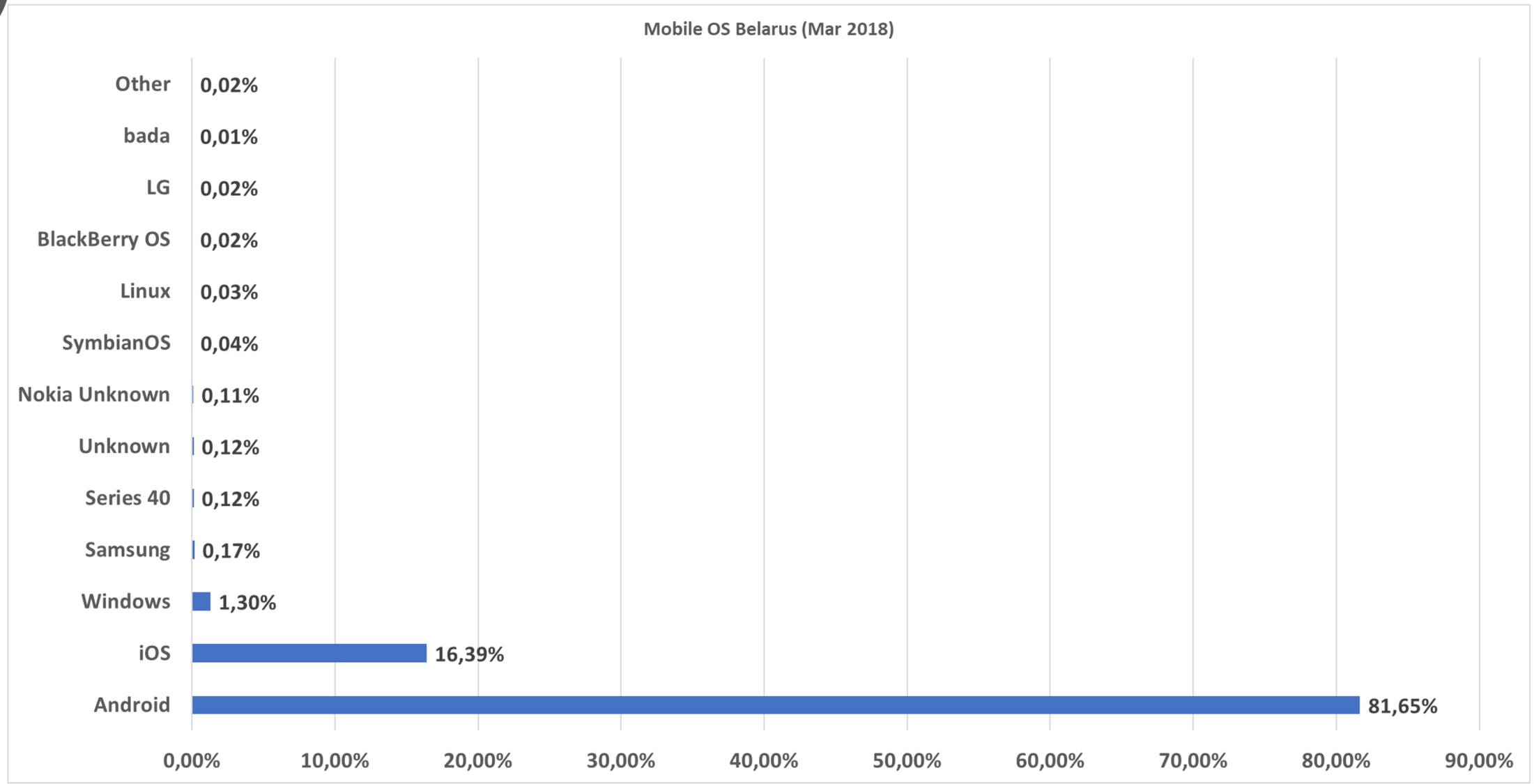
  7000 долларов

ШИФРОВАНИЕ В GSM

- В **64-разрядном ключе 10 разрядов просто заменены нулями**. Кроме того, из-за многочисленных конструктивных дефектов **стойкость шифра находится на уровне 40-разрядного**, который легко может быть вскрыт любым современным компьютером за пару секунд. Таким образом, возможность прослушивания любого абонента в сетях GSM – это не только реальность, но и норма;

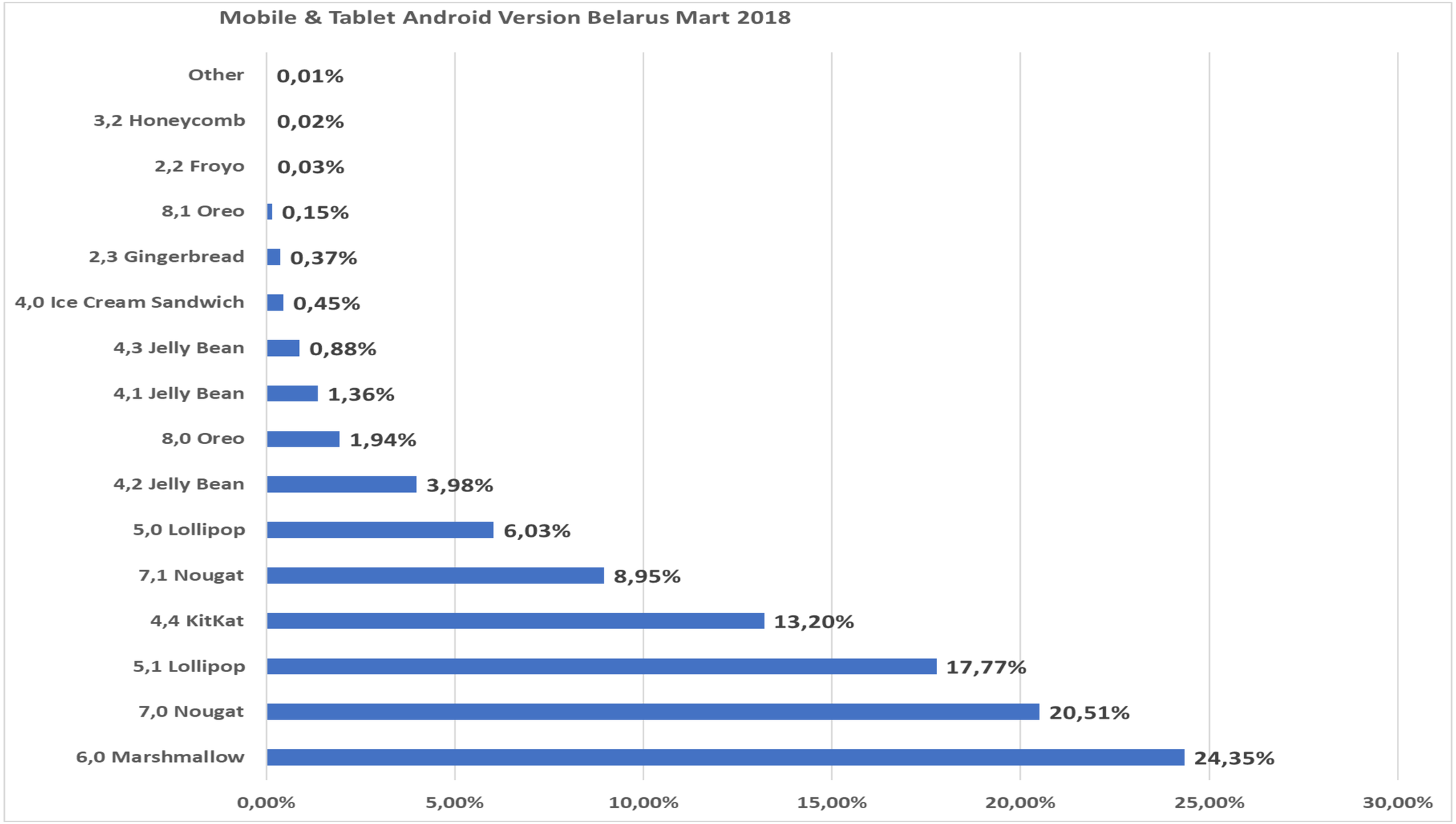
- На сегодня в Интернет выложено множество программ для взлома защиты протоколов связи GSM, использующих различные методы. Однако стоит учесть, что для расшифровки вы вначале должны перехватить соответствующий сигнал. На сегодня в мире существует около 20 видов оборудования для прослушивания трафика в сетях GSM.

СТАТИСТИКА МОБИЛЬНЫХ ОС. МАРТ 2018

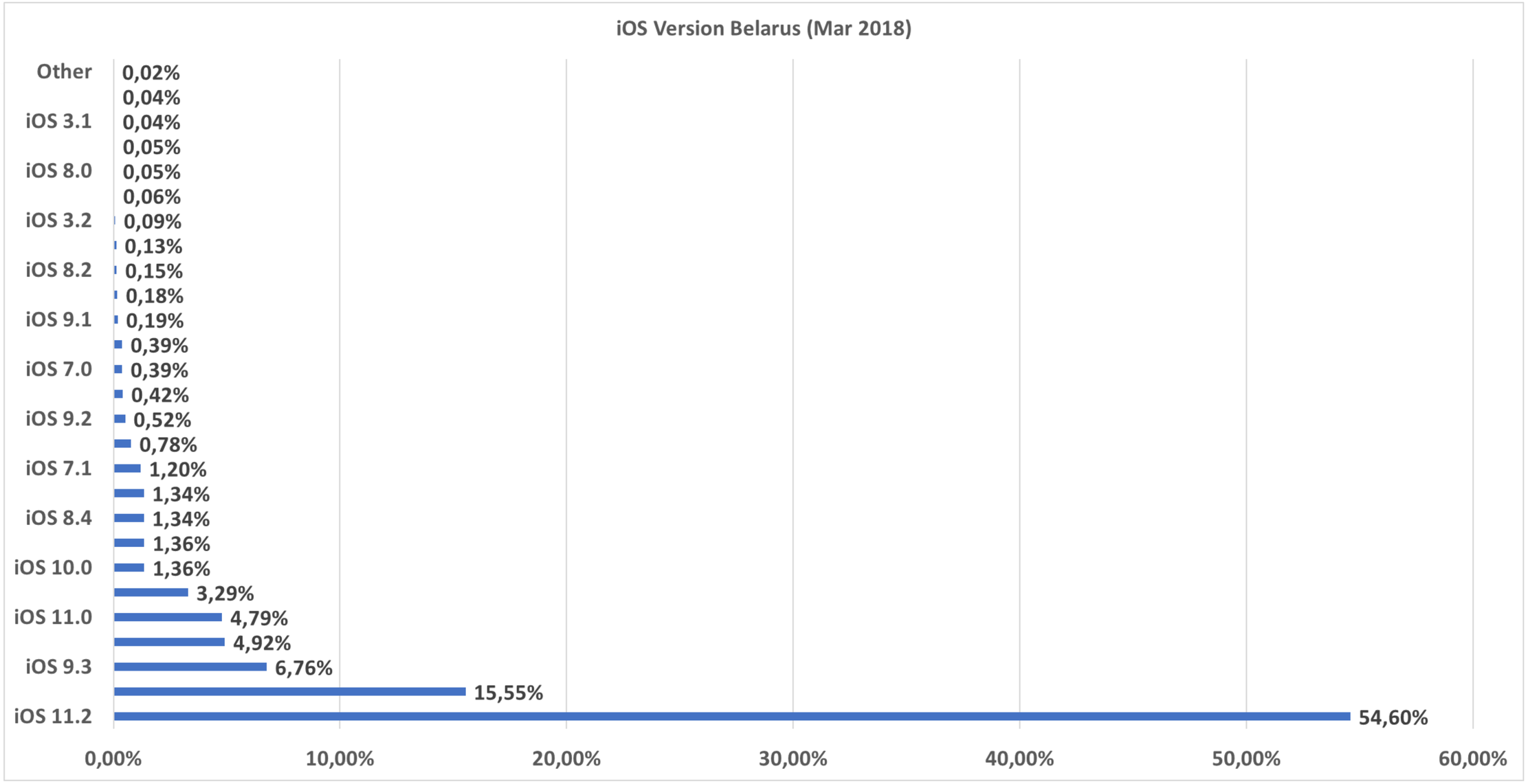


http://gs.statcounter.com/

ВЕРСИИ ANDROID МАРТ 2018 БЕЛАРУСЬ



ВЕРСИИ IOS МАРТ 2018 БЕЛАРУСЬ



APPLE И PRIVACY

APPLE РЕГИСТРИРУЕТ ВАШ IP-АДРЕС (МЕСТОПОЛОЖЕНИЕ)

iMessage при отправке связывается с серверами Apple для определения доступности сервиса на другой стороне, метаданные фактически сохраняются: номер или email абонента , дата/время, IP-адрес, срок хранения данных неизвестен, данных о том, зашифрована ли эта информация на сервере, нет. Apple может передавать эти данные по запросу правоохранительных органов

Источник: ***The Intercept***

APPLE РЕГИСТРИРУЕТ ВАШ IP-АДРЕС (МЕСТОПОЛОЖЕНИЕ)

- Если вы используете резервное копирование iCloud на ваших устройствах Apple, при этом используя шифрование, то учтите, что **ключами шифрования управляет компания Apple, а не вы**.

Даже если вы доверяете компании Apple, то **любой, кто сумеет получить доступ к вашей учетной записи iCloud, фактически получит полную информацию о всем, что вы храните на вашем устройстве.**

APPLE ОТСЛЕЖИВАЕТ С КЕМ ВЫ БОЛТАЕТЕ, ИСПОЛЬЗУЯ IMESSAGE

- Для iMessage не нужен номер телефона вообще – этот протокол работает и на iPad без SIM-карты, и на Mac – привязка абонента идёт к email-адресу;
- На iPhone можно настроить так, чтобы не высвечивать номер телефона, а завязаться исключительно на email.

Рекомендация Настройте ваш iMessage исключительно на email и посоветуйте сделать то же вашим собеседникам.

ВОССТАНОВЛЕНИЕ PIN-КОДА IPHONE

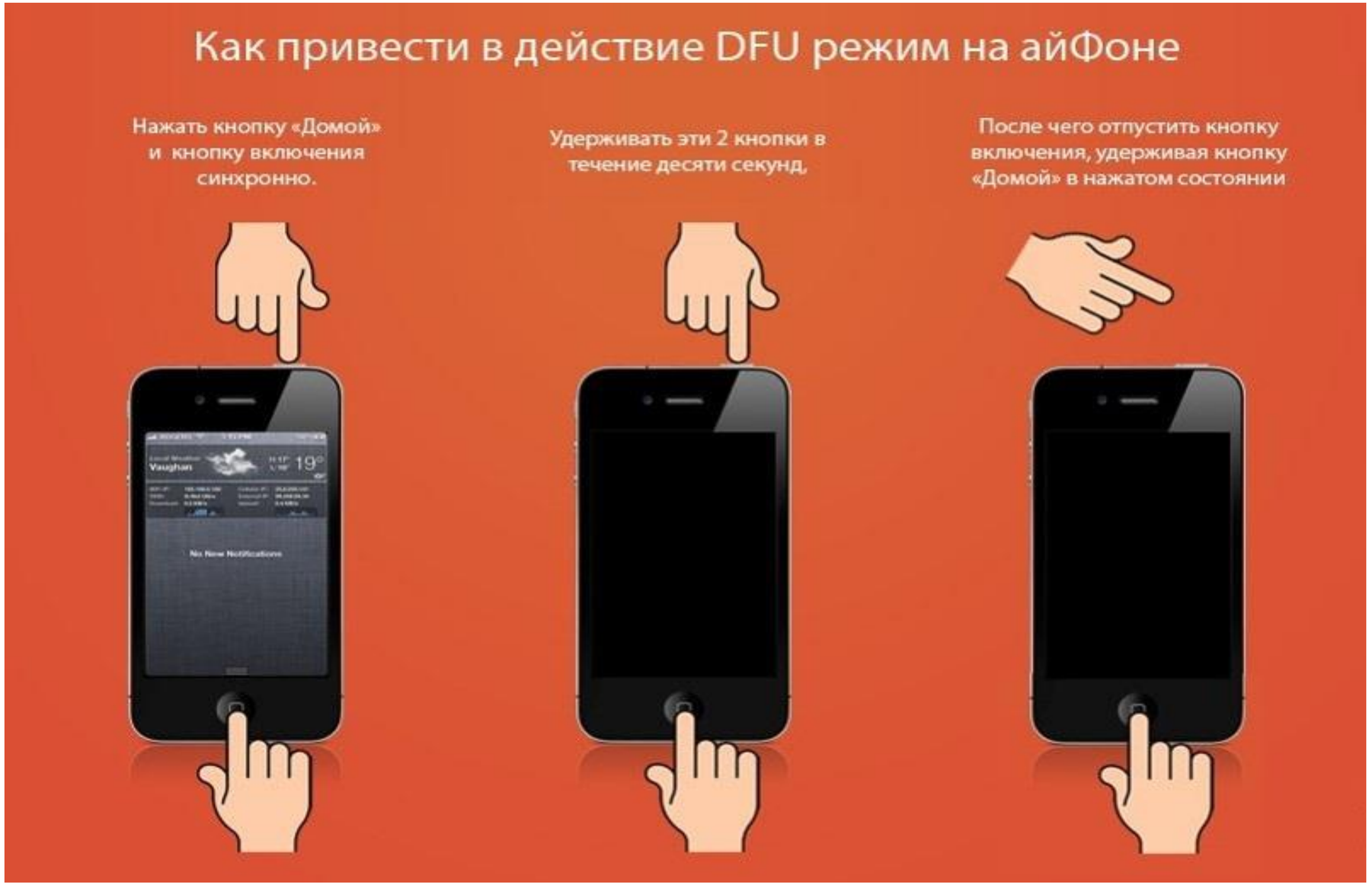
Демо

DEVICE FIRMWARE UPDATE

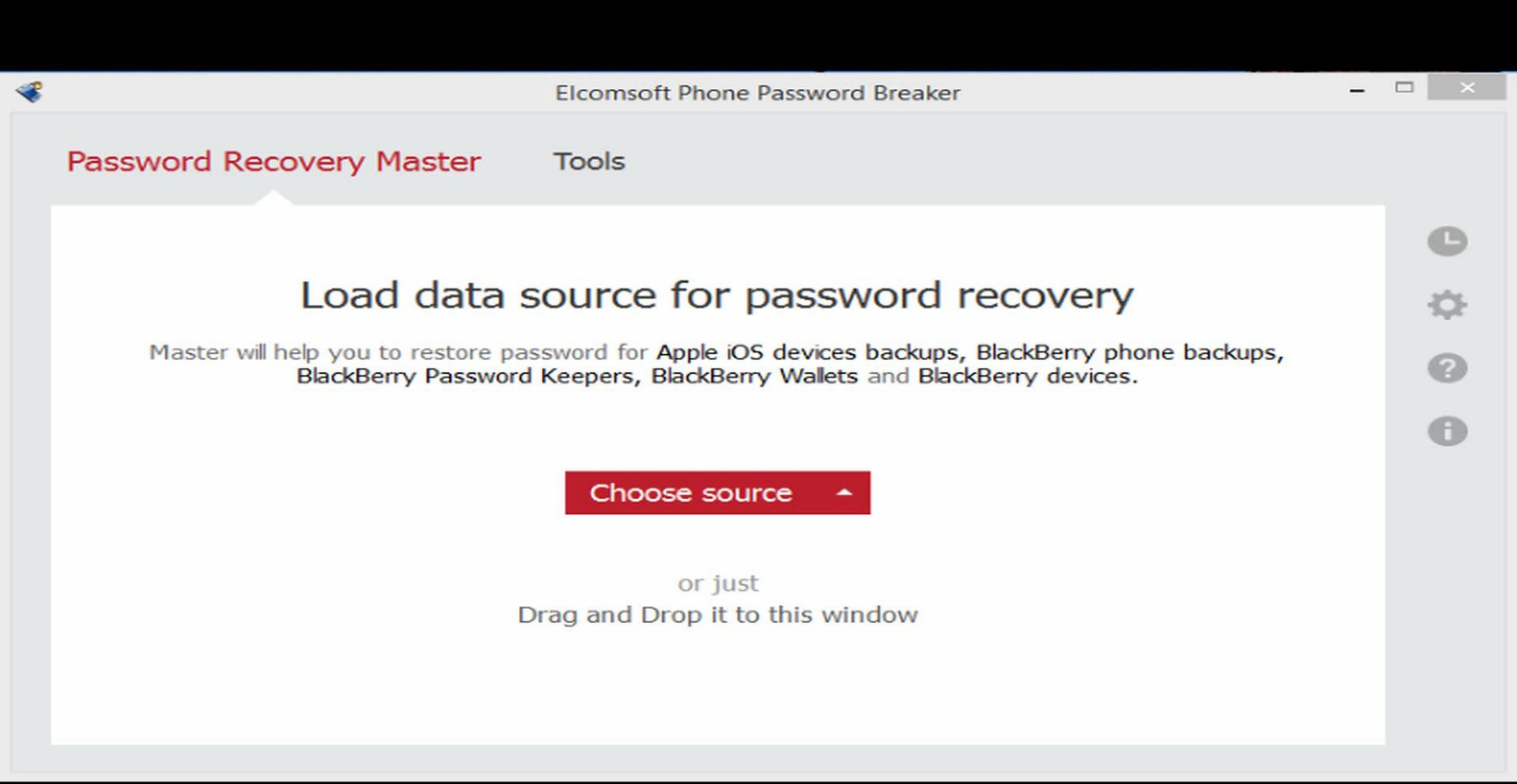
Особенность DFU заключается в том, что iPhone в этом режиме может взаимодействовать с iTunes, но не может загрузить iBoot (бутлоадер)

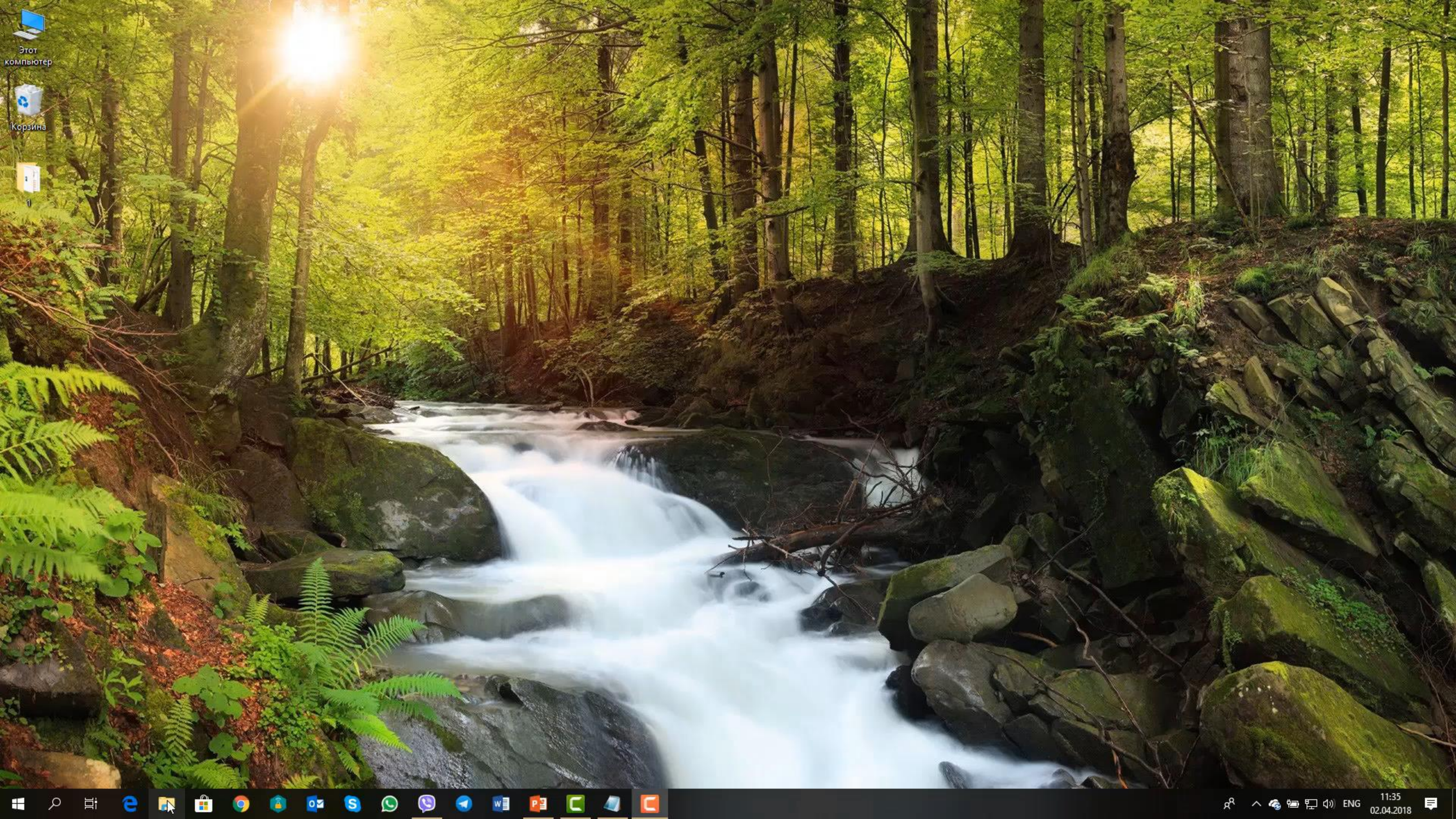
В данном режиме, в котором не запущен бутлоадер и сама ОС, пользователь может выполнять даунгрейд прошивки и устанавливать custom-прошивку.

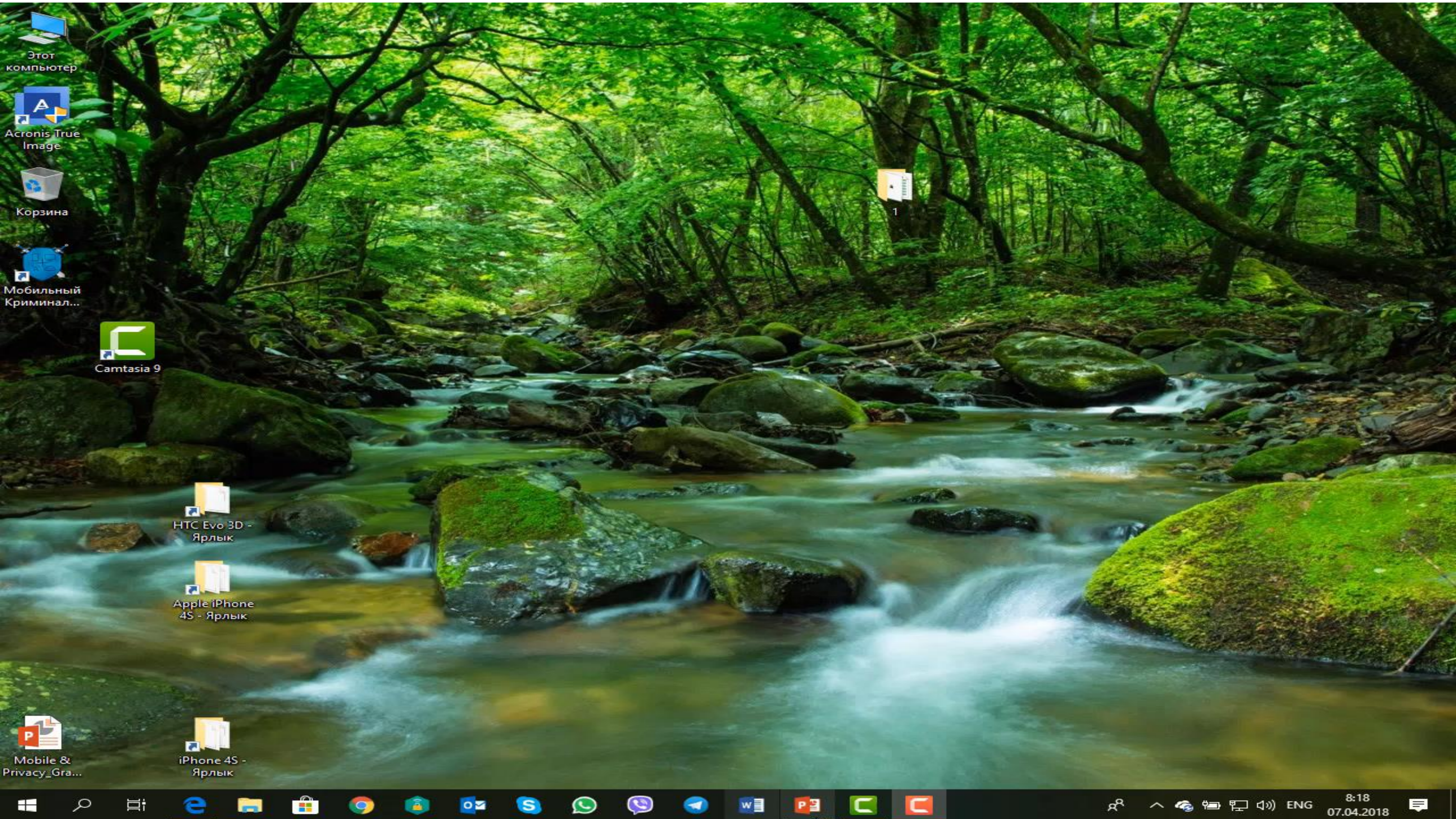
КАК ПРИВЕСТИ В ДЕЙСТВИЕ DFU РЕЖИМ



Восстановление PIN кода iPhone


Elcomsoft Phone Password Breaker
Password Recovery Master
Tools
Load data source for password recovery
Master will help you to restore password for Apple iOS devices backups, BlackBerry phone backups, BlackBerry Password Keepers, BlackBerry Wallets and BlackBerry devices.
Choose source
or just
Drag and Drop it to this window


Этот компьютер
Корзина
1
ENG
11:35
02.04.2018


Этот компьютер
Acronis True Image
Корзина
Мобильный Криминал...
Camtasia 9
1
HTC Evo 3D - Ярлык
Apple iPhone 4S - Ярлык
Mobile & Privacy_Gra...
iPhone 4S - Ярлык
ENG
8:18
07.04.2018

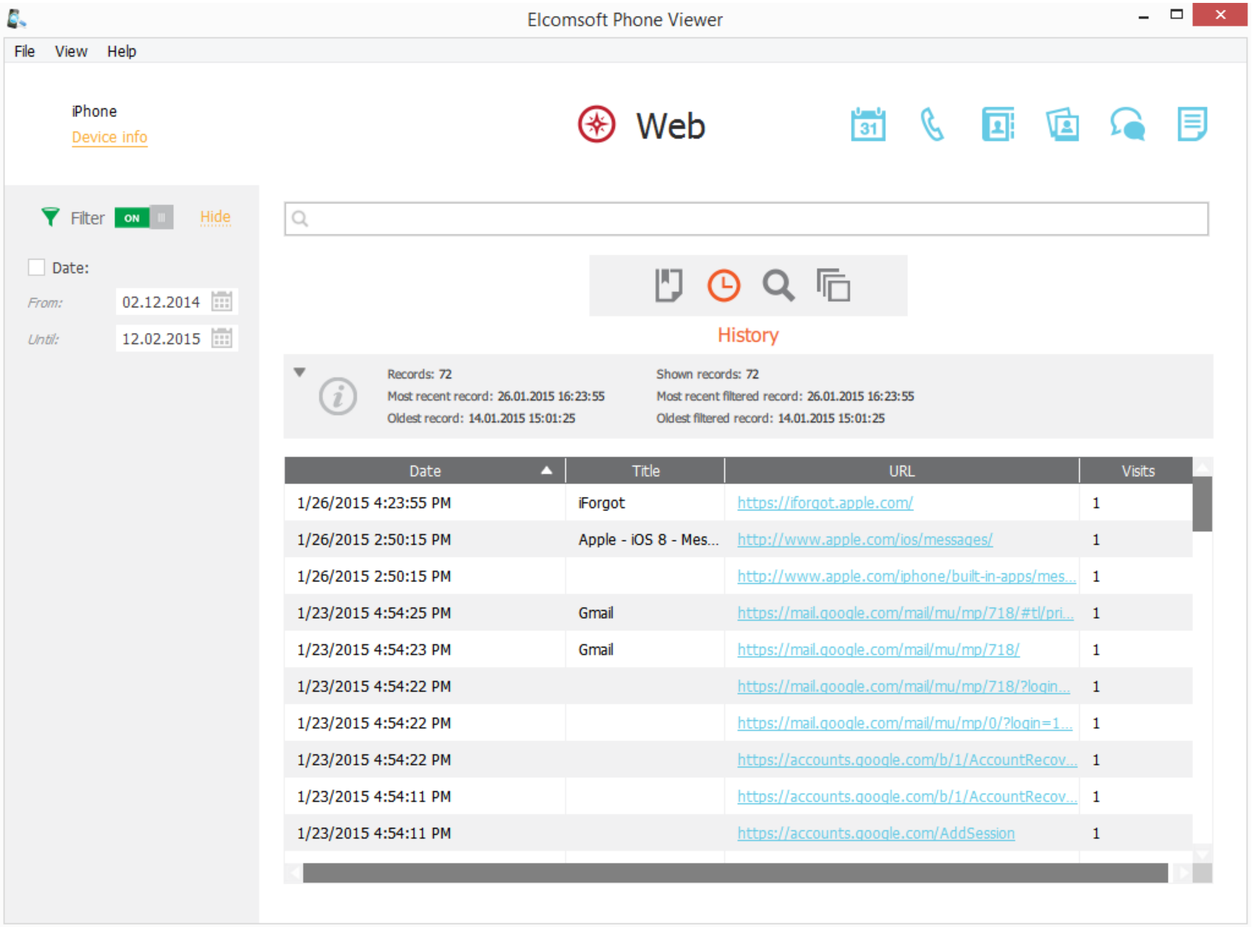
ЖУРНАЛ ЗВОНКОВ

Согласно данным компании ElcomSoft Co. Ltd., Apple автоматически загружает журналы звонков iPhone на удаленные серверы Apple.
Журналы звонков могут храниться на серверах Apple в течение многих месяцев.
Пользователь не в состоянии запретить эту синхронизацию, не отключая iCloud полностью.

Официально не хранится, однако… Данные добываются с помощью Elcomsoft Phone Breaker

ЖУРНАЛ WEB

Данные синхронизируются регулярно и не зависят от настроек резервных копий, что позволяет вести наблюдение за тем, какие сайты посещает пользователь, с минимальной задержкой.



ИСТОРИЯ ПОСЕЩЕНИЙ

Apple оказалась единственной компанией, которая продолжает хранить на своих серверах записи из истории браузера даже после того, как пользователь их удалит.

КАК ОТКЛЮЧИТЬ ДОСТУП APPLE К ВАШИМ ДАННЫМ

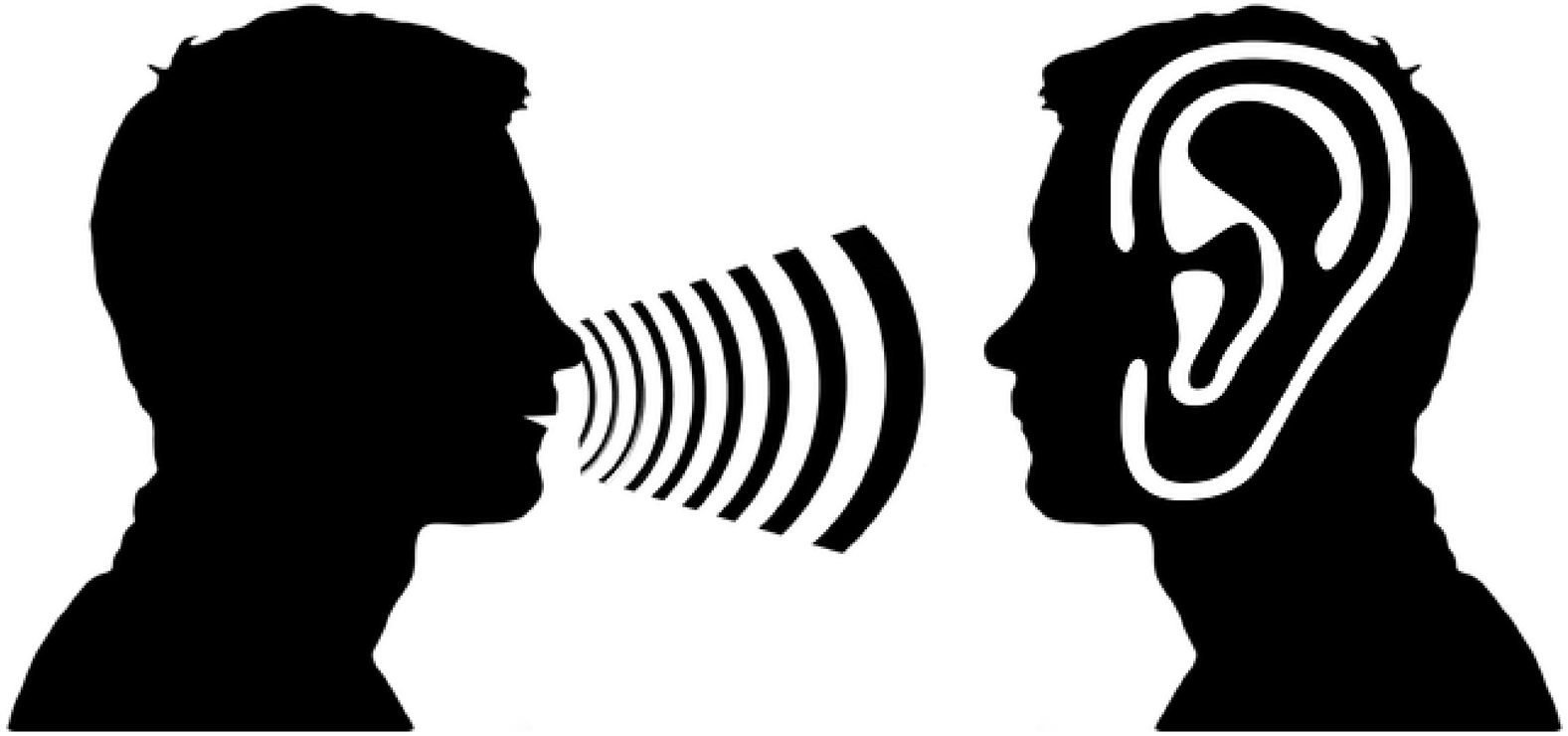
1. Сделайте локальную копию ваших персональных данных через iTunes;
2. Отключите резервное копирование iCloud в **Настройки — iCloud — Хранение** и **Резервное копирование — Резервное копирование iCloud**;
3. Делайте шифрованные локальные резервные копии.

ПОМНИТЕ!

- Если не можете обойтись без облачных бэкапов, как минимум **включите двухфакторную аутентификацию**.
- На доступ к вашим данным со стороны Apple (а соответственно и спецслужб) это не повлияет никак.

- В iOS есть и механизмы синхронизации, и отключить их все абсолютно невозможно - проблему можно решить кардинально, только не пользуясь iCloud вообще.
- Готовы ли вы к этому, или решаетесь на риск - решать только вам. Не забудьте только, что **сервис FindMyPhone, защищающий телефон от потери (и позволяющий удалённо заблокировать или стереть все данные) работает только в связке с iCloud.**

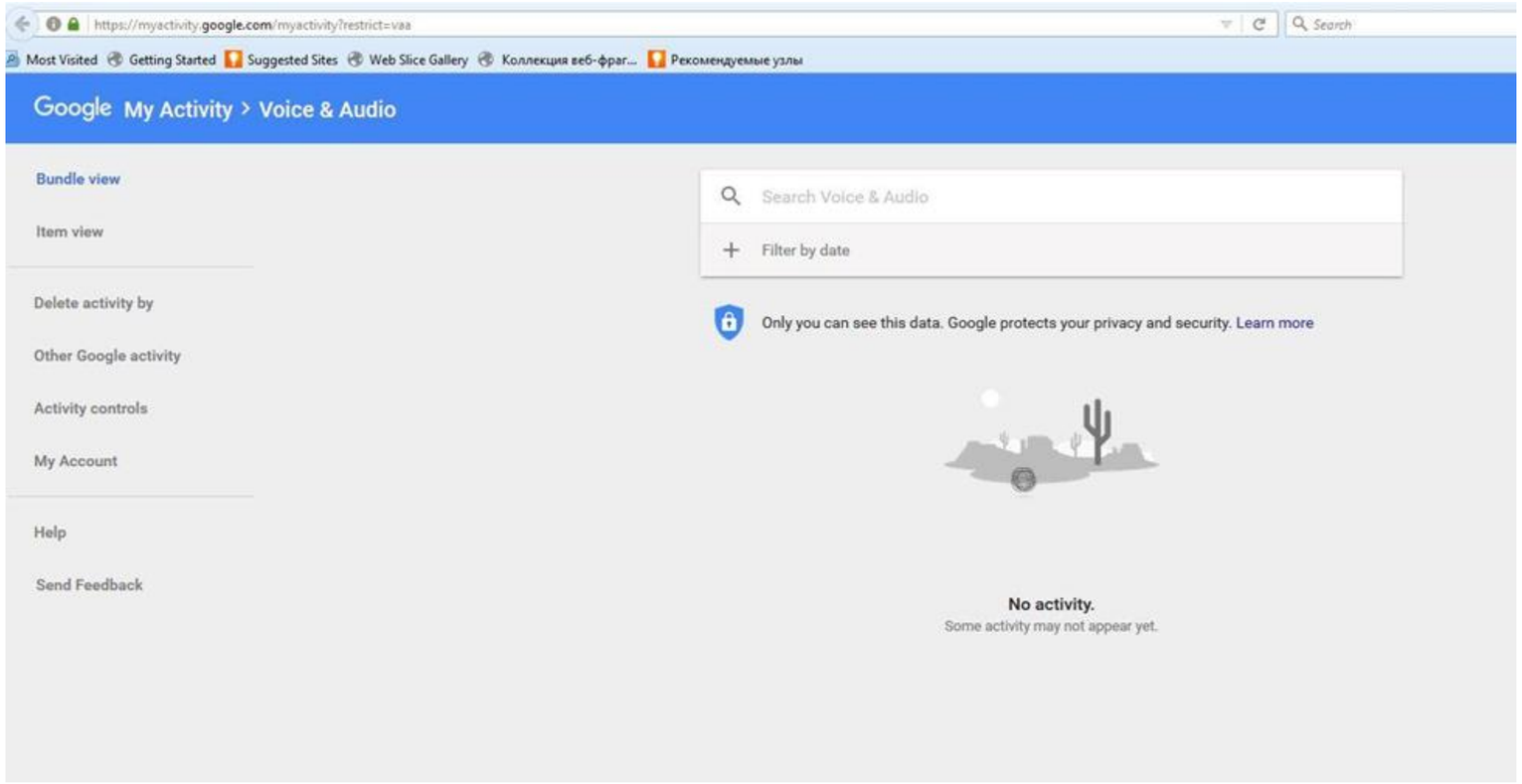
ANDROID



ЧТО ЗНАЕТ О ВАС GOOGLE&

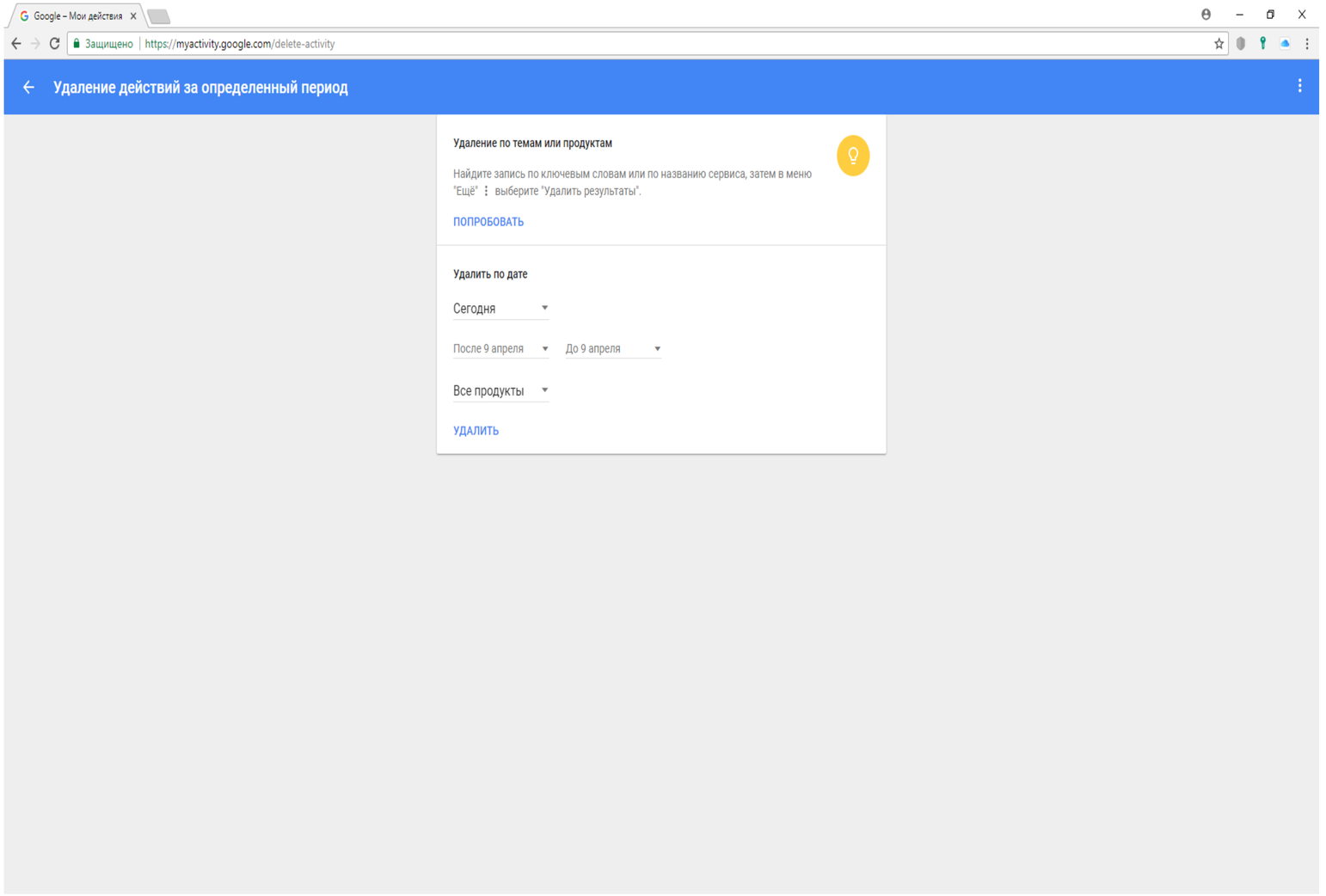
ИСТОРИЯ VOICE & AUDIO

Если вы хотя бы раз произнесли «Ok, Google!», то активировали голосового помощника. Посмотрим, какие ваши голосовые сообщения хранит Google.



https://history.google.com/history/audio

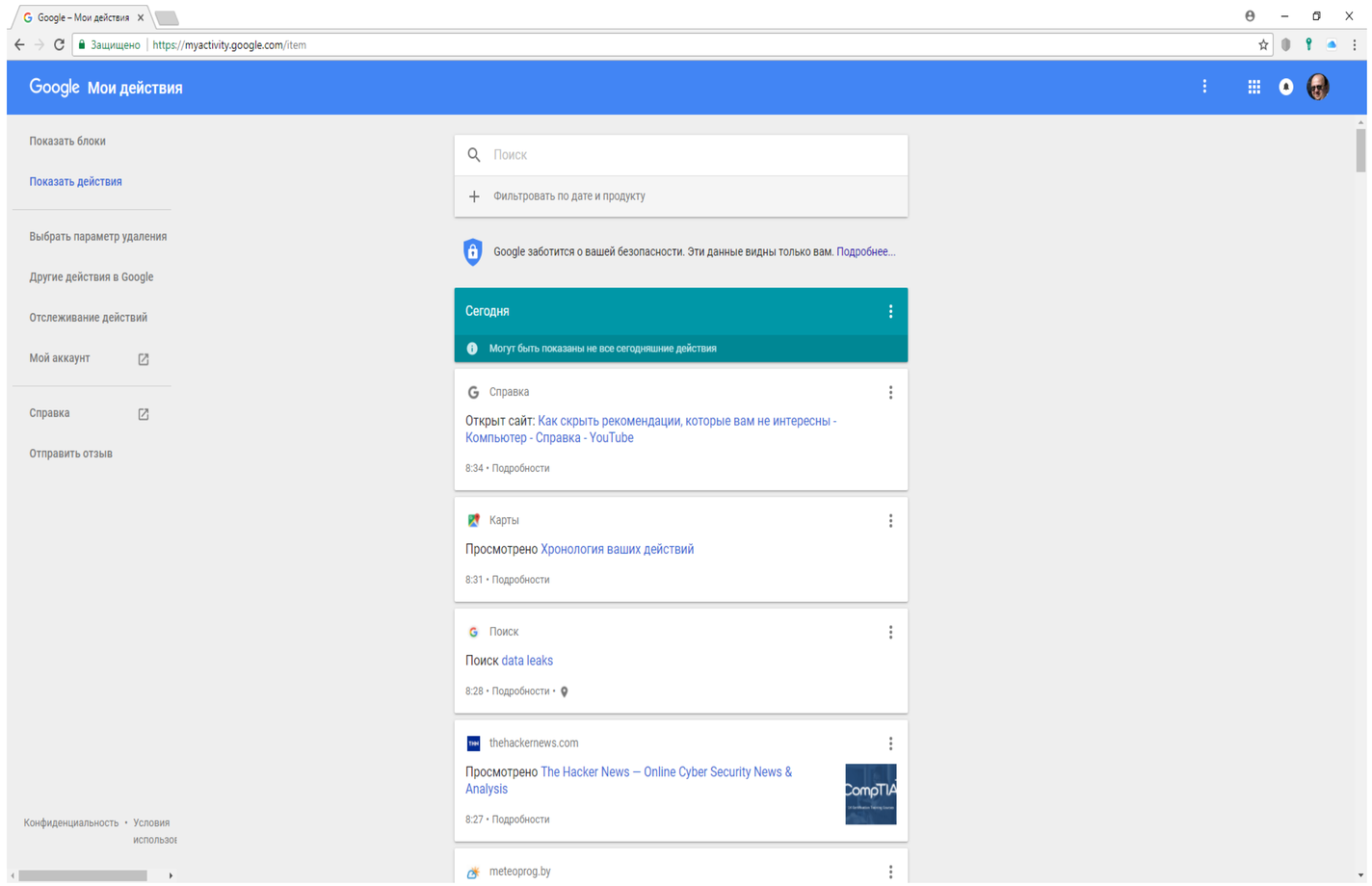
УДАЛИТЬ ЗАПИСИ ЗА ПЕРИОД



Безусловно, вы можете удалить ваши действия, хранящиеся в Google за определенный период. Но задумаемся, делают ли это пользователи?

ПОЛНОЕ ДОСЬЕ GOOGLE

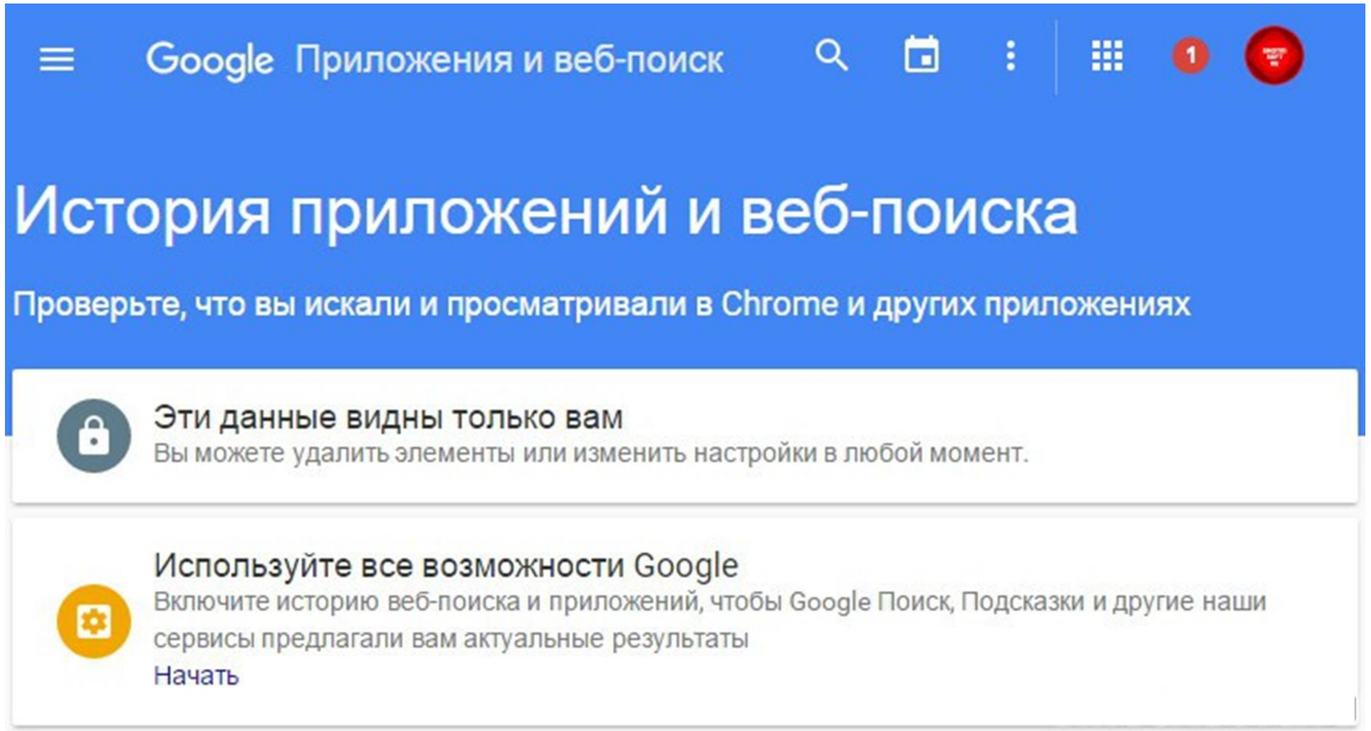
На данной странице вы сможете увидеть и удалить ваши действия, произведенные в Chrome и Android
В частности какие страницы открывались, что просматривалось и т.д.



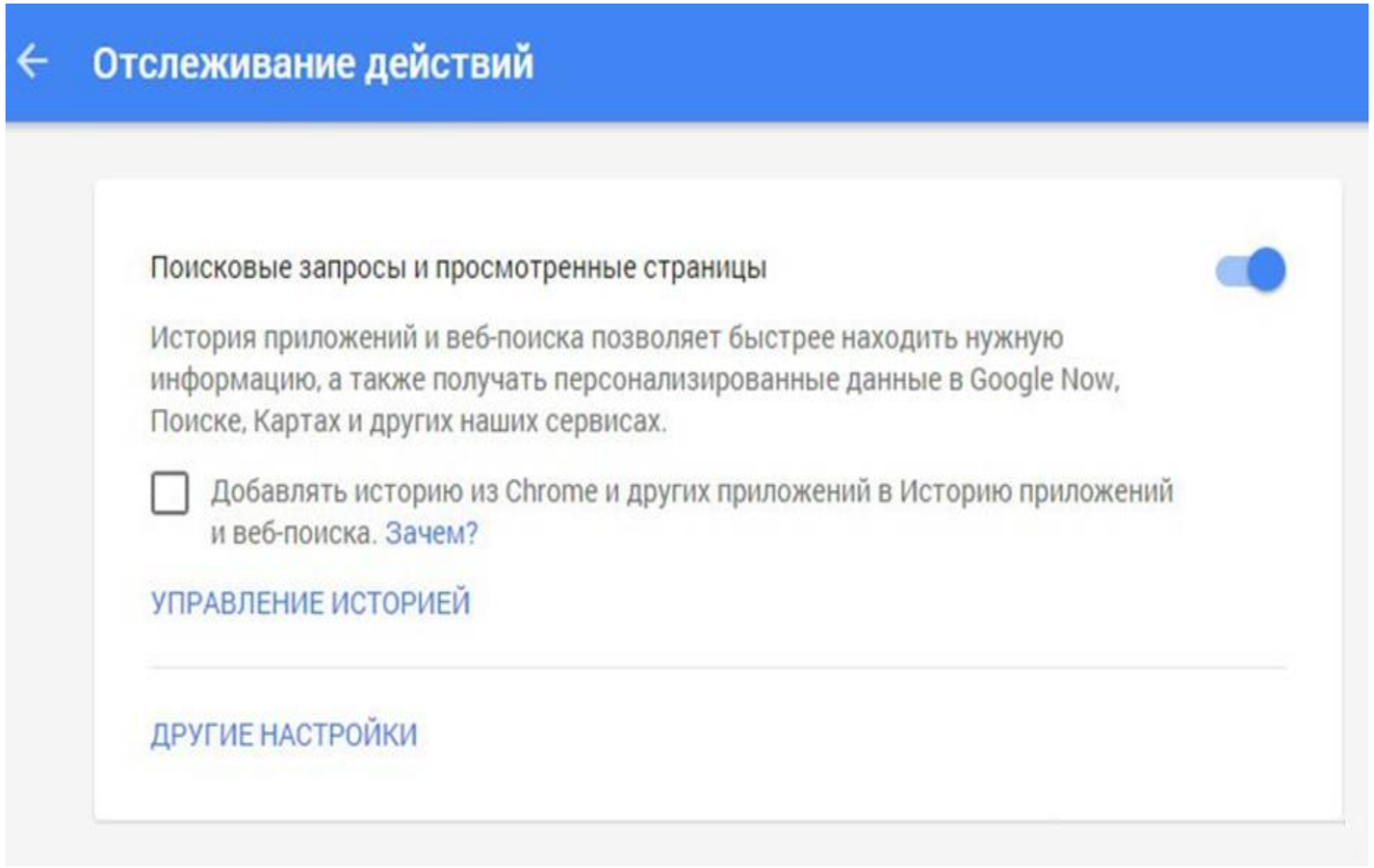
https://history.google.com/history/

ЧТО ХРАНИТСЯ В ИСТОРИИ ПРИЛОЖЕНИЙ И ВЕБ-ПОИСКА

Сохраняются следующие сведения:
поисковые запросы и другие действия в различных сервисах Google, например в Картах;
информация о вашем местоположении, языке, IP-адресе, а также сведения о том, как вы просматривали страницы: через браузер или приложение;
данные о просмотренных объявлениях или покупках на сайте рекламодателя;
недавно использованные приложения или просматриваемые контакты.
Примечание. Эти данные могут сохраняться, даже если вы офлайн.



НАСТРОЙКИ, КОТОРЫЕ ВЛИЯЮТ НА ОТСЛЕЖИВАНИЕ ДЕЙСТВИЙ.



История приложений и веб-поиска
Система сохраняет ваши поисковые запросы из браузеров и приложений (Google Поиске, Google Картах, Google Now и другие сервисы).

История местоположений
Создает персональную карту мест, где вы побывали с устройством, на котором был выполнен вход в аккаунт Google.

Информация с устройств
Включает контакты, календари, приложения и другие данные.

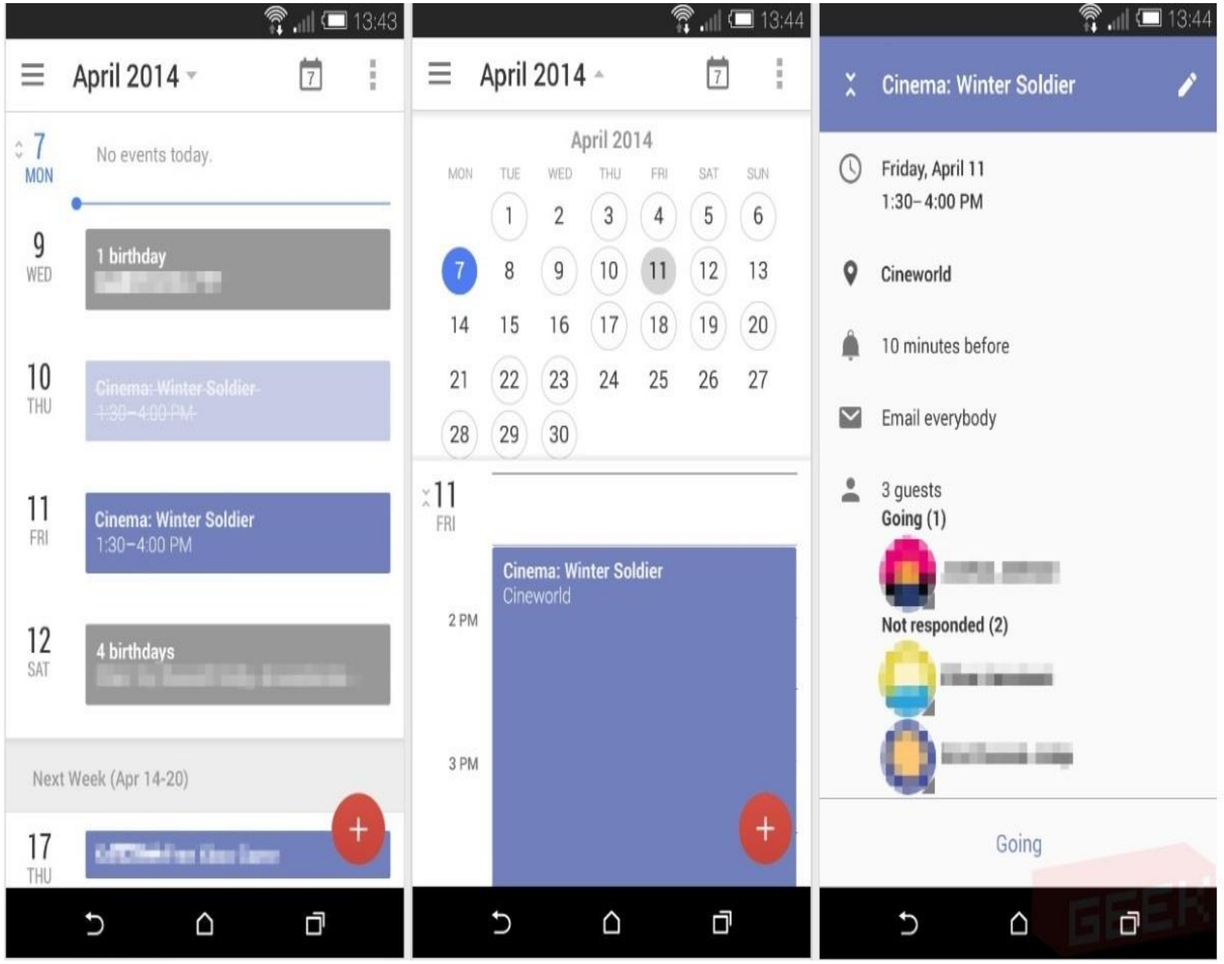
История голосового управления
Сохраняет в аккаунте голосовые запросы (например, следующие за командой "О'кей, Google")

История поиска YouTube
Сохраняет запросы на YouTube

ПРАВА ПРИЛОЖЕНИЙ В ANDROID

В категорию «Опасные» входят девять групп разрешений, которые связаны с безопасностью данных пользователя. Каждая из групп содержит несколько разрешений, которые может запрашивать приложение. Если одно из разрешений в данной группе пользователь уже одобрил, все остальные разрешения из той же группы приложение получит автоматически — без нового запроса пользователю.

КАЛЕНДАРЬ



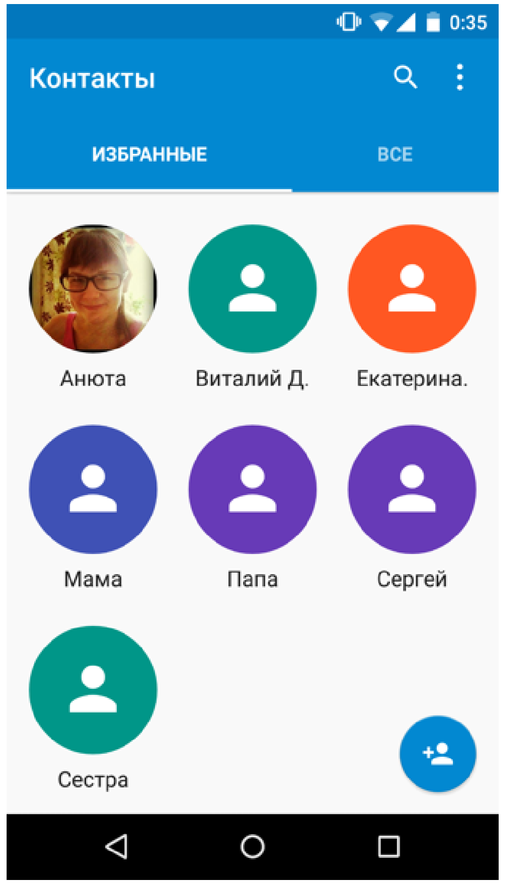
Изменение уже имеющихся в календаре событий и добавление новых.

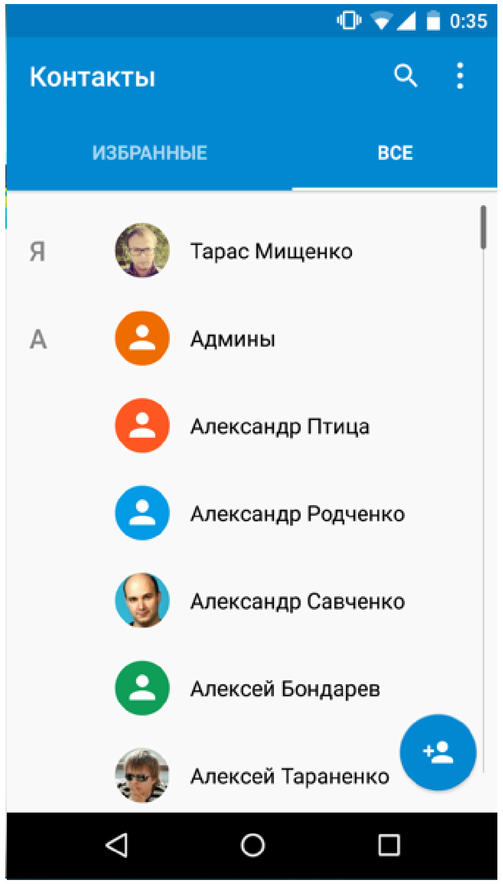
Чем опасно: Если вы активно пользуетесь электронным ежедневником, то доступ к нему позволит узнать все о том, чем вы занимались в прошлом, занимаетесь сегодня и собираетесь заниматься в будущем.

КАМЕРА

Чем опасно: Приложение сможет в любой момент сделать фото или записать видео, не предупреждая вас об этом.

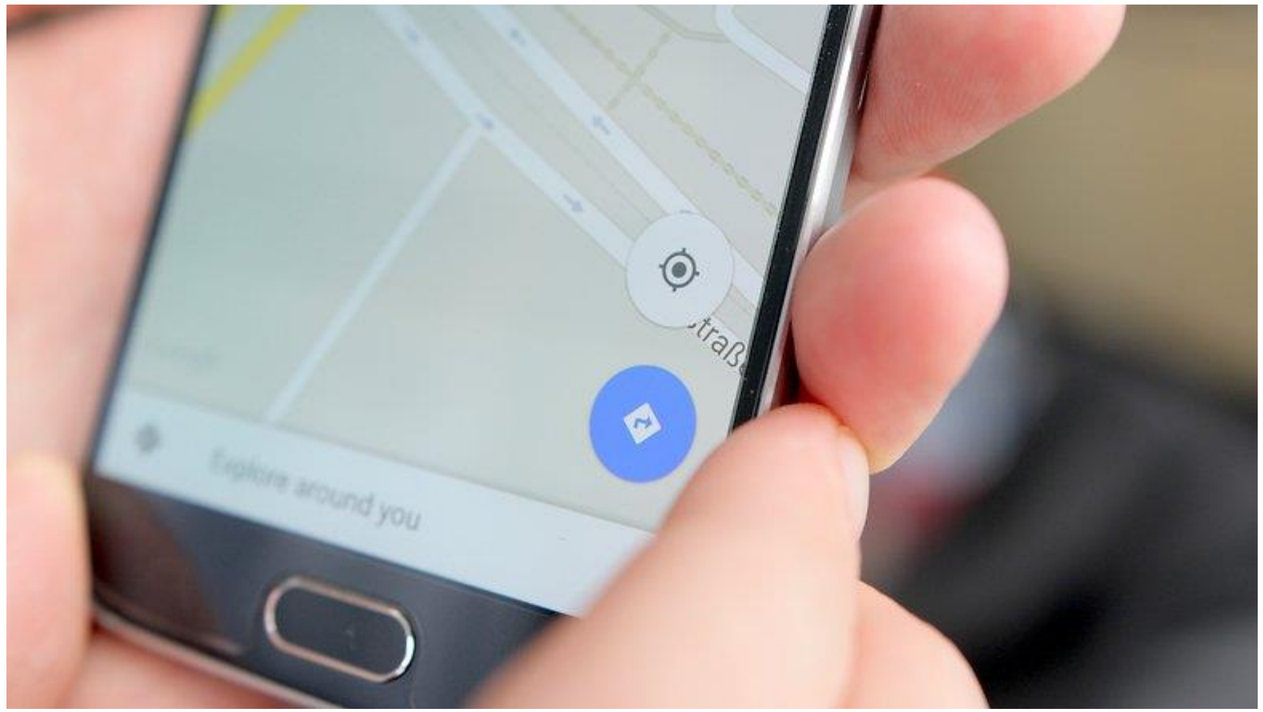
КОНТАКТЫ





Позволяет приложению заполучить всю вашу адресную книгу.
Разрешает доступ к списку всех учетных записей, с помощью которых вы входите в приложения на данном устройстве, — Google, «Яндекс», Facebook, «ВКонтакте» и так далее

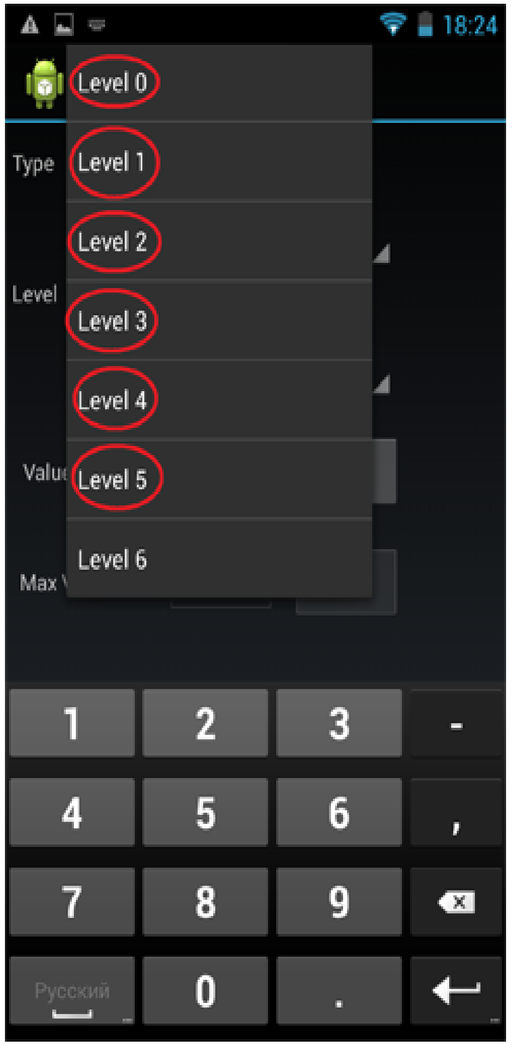
МЕСТОПОЛОЖЕНИЕ



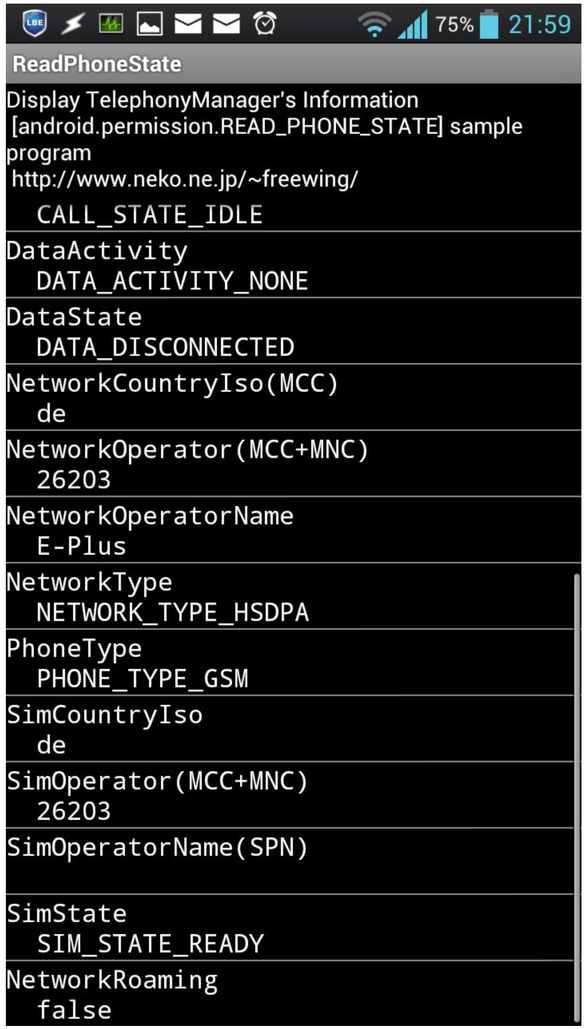
Позволяет приложению следить за всеми вашими перемещениями. Например, жулики могут узнать, что вы уехали в отпуск, и попробовать наведаться к вам домой

МИКРОФОН

Приложение сможет вести аудиозапись всего, что происходит рядом со смартфоном. Всех ваших разговоров.



ТЕЛЕФОН



- Чтение состояния телефона, в том числе вашего телефонного номера, данных сотовой сети, статуса исходящих звонков и так далее.
- Совершение звонков.
- Чтение списка вызовов.
- Изменение списка вызовов.
- Добавление голосовой почты.

ТЕЛЕФОН ИСПОЛЬЗОВАНИЕ IP-ТЕЛЕФОНИИ.

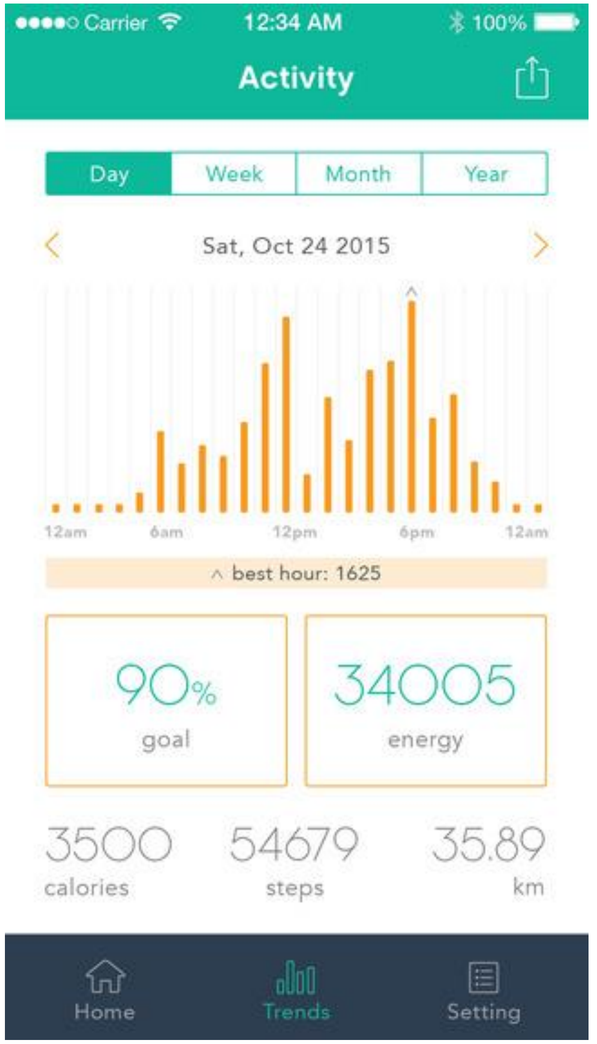
Управление исходящими звонками, в том числе просмотр номера, на который вы в данный момент звоните, возможность завершить звонок или переадресовать его на другой номер.

Чем опасно: Выдавая приложению разрешение данной группы, вы позволяете ему совершать практически любые действия, которые касаются голосовой связи.

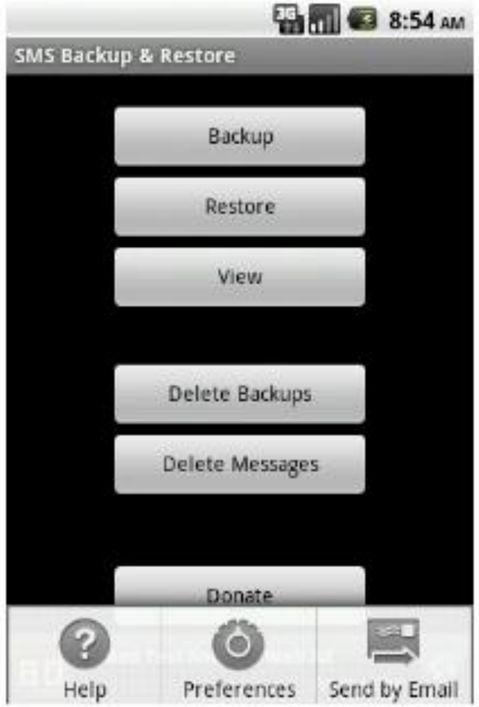
СЕНСОРЫ

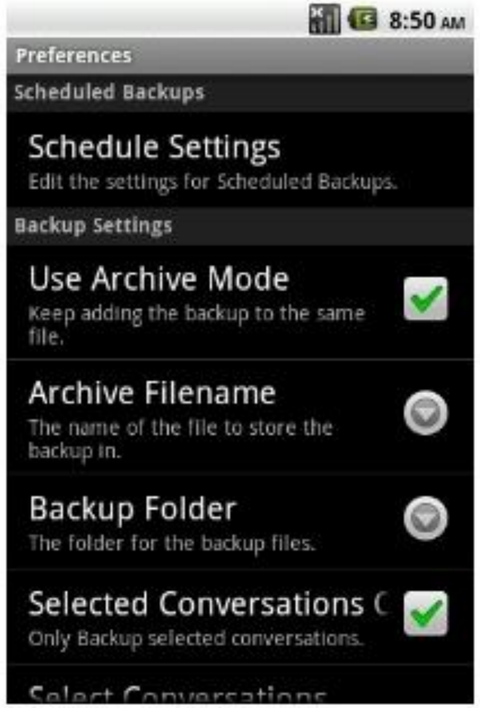
Доступ к данным от датчиков состояния здоровья, таким как пульсомер.

Чем опасно: Разрешает приложению следить за тем, что происходит с вашим телом, используя информацию от датчиков соответствующей категории, если они у вас есть и вы ими пользуетесь (встроенные в смартфон датчики движения не входят в эту категорию).



SMS





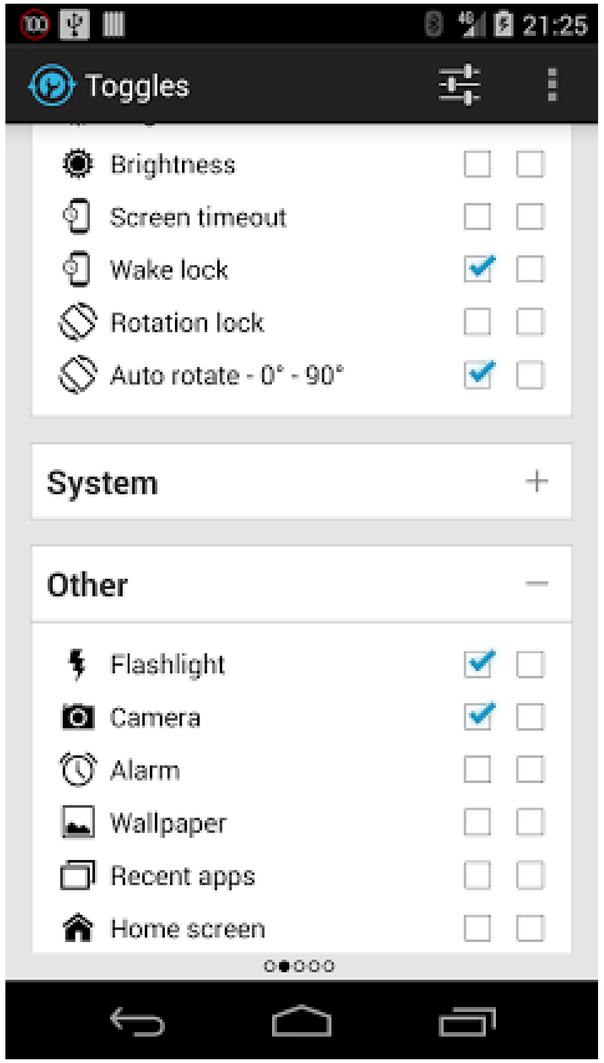
- Отправка SMS.
- Просмотр SMS в памяти смартфона.
- Прием SMS.
- Прием WAP push-сообщений.
- Прием входящих MMS.

Позволяет приложению получать и читать все ваши текстовые сообщения. А также отправлять SMS, например, чтобы подписать вас на какую-нибудь платную «услугу».

ПАМЯТЬ

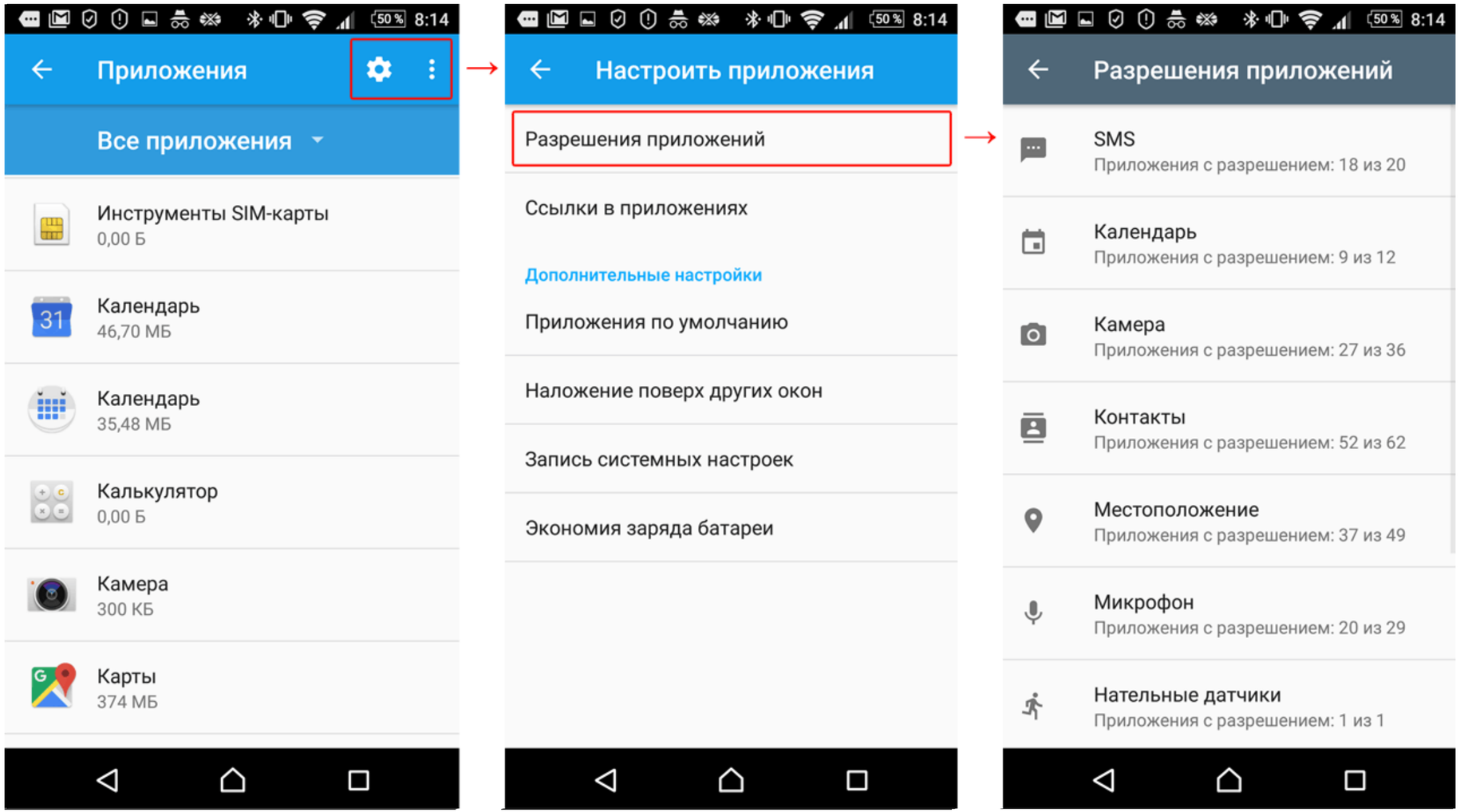
Предоставляет приложению возможность:

- Читать
- Изменять
- Удалять любые ваши файлы, хранящиеся в памяти смартфона.

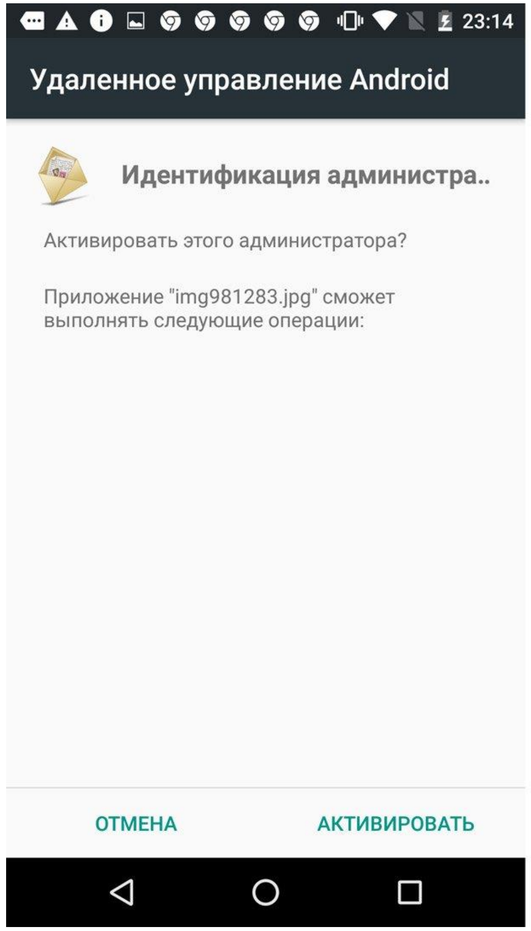


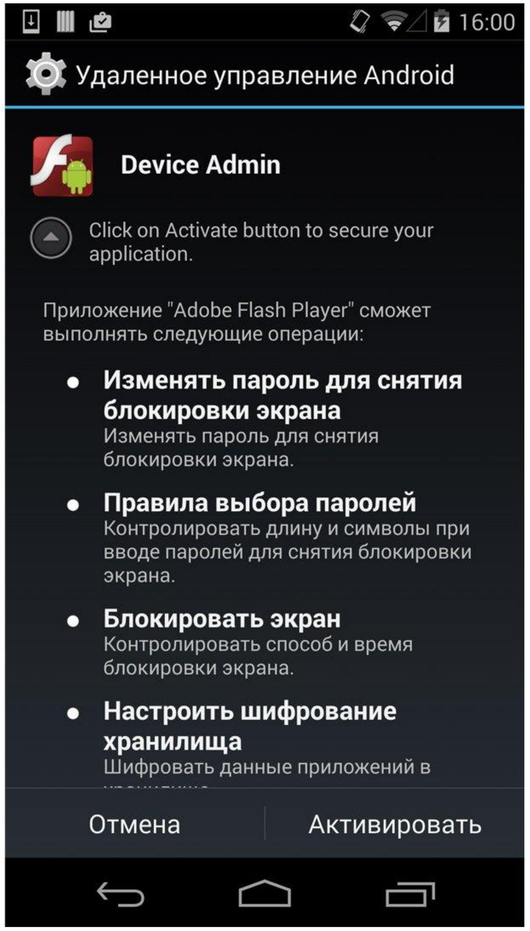
РАЗРЕШЕНИЯ ПРИЛОЖЕНИЙ

Как посмотреть разрешения приложений



ПРАВА АДМИНИСТРАТОРА УСТРОЙСТВА





Обладая этими правами, приложение может среди прочего сменить пароль, заблокировать камеру или даже удалить все данные с устройства.

Мобильный Криминалист Детектив

Файл Вид Инструменты Сервис Справка

Все устройства

Фильтр ...

Подключить устройство | Импорт файла | Открыть дело | Сохранить в архив | Аналитика | Экспорт | Карты | Дроны | Биллинги | Облачные сервисы | Разблокировка экрана

Устройства и Дела

- Все устройства
  - Human trafficking (1)
    - Simon Payge's iPhone 4S (Nojailbreak)
  - Дело не назначено

Устройство	Извлечение	Владелец	Заметки
Simon Payge's iPhone 4S (Nojailbreak) **Модель:** Apple iPhone 4S **IMEI:** 013043005068452 **Дело:** Human trafficking **Номер вещдока:** 65/42	**Эксперт:** <Нет> **Извлечено в версии:** 5.1.2.153 24.04.2013 11:56:32	 Simon Payge	Device found in a stolen car 9904 Fort Hamilton Parkway, Brooklyn NY February 6, 2013

Важные улики

Раздел "Важные улики" показывает данные, отмеченные следователем как "важные" в следующих разделах: Телефонная книга, Сообщения, Журнал событий, Календарь, Заметки и др.

Поиск

Раздел "Поиск" позволяет искать данные во всех разделах одного или нескольких устройств.

Версия: 10.1.0.100 | Заканчивается через 54 дней | Всего дел: 1, Всего устройств: 1

ENG 8:45 07.04.2018

СПАСИБО ЗА ВНИМАНИЕ!

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

19 апреля 2018 г.
г. Минск

#CODEIB

КОТ ИБ
corporation

КОТ ИБ

ВЛАДИМИР БЕЗМАЛЫЙ
НЕЗАВИСИМЫЙ ЭКСПЕРТ В ОБЛАСТИ ИБ

EMAIL: CYBERCOP@OUTLOOK.COM
FACEBOOK:
https://www.facebook.com/vlad.bezmaly
БЛОГ: https://bezmaly.wordpress.com/