Engine.ER Lab

# ЗАЩИТИТЬ-НЕЛЬЗЯ-ИЗОЛИРОВАТЬ(поставьте Запятую):
# или КАК РАСТИ ВО ВРЕМЯ КРИЗИСА

- ЗАЩИТИТЬ НЕЛЬЗЯ, ИЗОЛИРОВАТЬ (banks edition);

- ЗАЩИТИТЬ, НЕЛЬЗЯ ИЗОЛИРОВАТЬ (customers choice).

Дмитрий Кан,
CEO, Engine.ER Lab
kan.dmitriy@gmail.com

Engine.ER Lab

de-facto : Фрод ЕСТЬ.

Тренд сезона: Компрометация и генерация фрода непосредственно с endpoint-терминала клиента (MitE – Man in the Endpoint), с использованием его логина, пароля, PIN-кода, fingerprint, фото и видео.

БЕЗОПАСНОСТЬ
- Главная
- Администратору
- Стратегия безопасности
- Госрегулирование
- Техническая защита
- Пользователю

# Арестован глава крупнейшей компании по выпуску непрослушиваемых смартфонов

Безопасность Госрегулирование **Новости поставщиков** Бизнес Законодательство Кадры Техника
мобильная версия

12.03.2018, ПН, 12:09, Мск , Текст: Валерия Шмырова

**ФБР арестовало главу Phantom Secure — компании, которая создает непрослушиваемые смартфоны на базе BlackBerry и Android. Бюро утверждает, что компания кастомизирует аппараты специально под нужды наркоторговцев и прекрасно знает, что ее клиентами являются преступники.**


## Арест Винсента Рамоса

Федеральное бюро расследований (ФБР) арестовало владельца канадской компании Phantom Secure, которая занимается кастомизацией BlackBerry и Android смартфонов, превращая их в полностью безопасные, непрослушиваемые и неотслеживаемые устройства. Об этом со ссылкой на судебные документы и источники, знакомые с ситуацией, сообщает ресурс Motherboard. На своем рынке Phantom Secure является одной из наиболее успешных и уважаемых компаний, занятых созданием безопасных смартфонов, отмечает издание.

Как следует из искового заявления, поданного против гендиректора Phantom Secure **Винсента Рамоса** (Vincent Ramos) в суд Южного округа штата Калифорния, ответчик обвиняется в соучастии и пособничестве корпоративному рэкету и распространению наркотиков.

# Как два наркобарона создали абсолютно непрослушиваемый смартфон и заработали миллионы на его продажах





25.10.2019, Пт, 13:11, Мск , Текст: Валерия Шмырова

**Компания MPC, которая производила защищенные от прослушки смартфоны на основе Google Nexus 5 и Nexus 5X, принадлежит руководителям шотландской преступной группировки, занимающейся наркобизнесом. Компанию закрыли после того, как правоохранители занялись расследованием убийства блогера, к которому она была причастна.**

## Как появилась MPC

Компания MPC, выпускавшая защищенные от прослушки смартфоны, принадлежит представителям криминального мира — шотландской группировке «Братья», которую возглавляют **Джеймс** (James) и **Барри Гиллеспи** (Barrie Gillespie). Об этом сообщает издание Motherboard.

Основным бизнесом группировки Гиллеспи является транспортировка и продажа наркотиков. Несколько лет назад, чтобы обеспечить безопасность операций, «Братья» закупили у компании Enpetcom защищенные телефоны BlackBerry. Но

NetApp: новое в СХД
Безопасность
Цифровая трансформация
ИТ в госсекторе
ИТ в банках
ИТ в торговле
Телеком
Интернет
ИТ-бизнес
Рейтинги

## Как появилась MPC

Компания MPC, выпускавшая защищенные от прослушки смартфоны, принадлежит представителям криминального мира — шотландской группировке «Братья», которую возглавляют **Джеймс** (James) и **Барри Гиллеспи** (Barrie Gillespie). Об этом сообщает издание Motherboard.

Основным бизнесом группировки Гиллеспи является транспортировка и продажа наркотиков. Несколько лет назад, чтобы обеспечить безопасность операций, «Братья» закупили у компании Ennetcom защищенные телефоны BlackBerry. Но вскоре об этих устройствах узнала полиция Нидерландов, отследившая связь одного из телефонов со случаями убийств, вооруженного грабежа и перевозки наркотиков.

Тогда «Братья» сами наняли разработчиков, чтобы создать кастомизированную ОС, где особое внимание уделялось вопросам приватности. Эту систему они начали загружать на телефоны, которыми пользовалась их группировка и ее партнеры. Наслаждаясь возможностями новой ОС, Гиллеспи пришли к выводу, что такие аппараты могут быть

ПРЕМИЯ ИННОВАЦИЯ ГОДА
CNEWS FORUM 8 НОЯБРЯ скоро
CNEWS AWARDS 8 НОЯБРЯ скоро
EPSON ДЛЯ БИЗНЕСА new
КАРТРИДЖИ CANON new
КОРПОРАТИВНАЯ МОБИЛЬНОСТЬ new
10 СОВЕТОВ О СВЯЗИ new
РОССИЙСКОЕ ПО new
ЭЛЕКТРОННОЕ ПРАВОСУДИЕ new
ЭКСПЕРТИЗА REDSYS
NETAPP: НОВОЕ В СХД
БЕЗОПАСНОСТЬ
ЦИФРОВАЯ ТРАНСФОРМАЦИЯ
ОБЛАЧНЫЕ ТЕХНОЛОГИИ
ИТ В ТОРГОВЛЕ
ИТ В ГОССЕКТОРЕ
ИТ В БАНКАХ

# Выпущен сверхзащищенный смартфон по цене автомобиля

Техника

мобильная версия

01.06.2016, СР, 11:04, Мск , Текст: Сергей Попсулин

**Британский стартап анонсировал Android-смартфон с несколькими дополнительными слоями защиты данных. Компания планирует продавать его состоятельным бизнесменам, чем и обусловлена его высокая цена, сопоставимая с автомобилем С-класса.**



## Смартфон по цене автомобиля

Британская компания Sirin Labs представила защищенный Android-смартфон Solarin по цене 9,5 тыс. фунтов стерлингов (около ₽ 918 тыс.), к продажам которого планирует приступить 30 июня 2016 г.

Аппарат оснащен 5,5-дюймовым дисплеем с разрешением 2560 x 1440 пикселей, процессором Qualcomm Snapdragon 810, оперативной памятью 4 ГБ и встроенным накопителем на 128 ГБ, основной камерой на 24 МП с оптической стабилизацией и фронтальной на 8 МП, аккумулятором емкостью 4040 мАч и поддержкой LTE.

Защищенность устройства заключается в наличии дополнительных слоев защиты данных в дополнение к стандартным возможностям операционной системы.

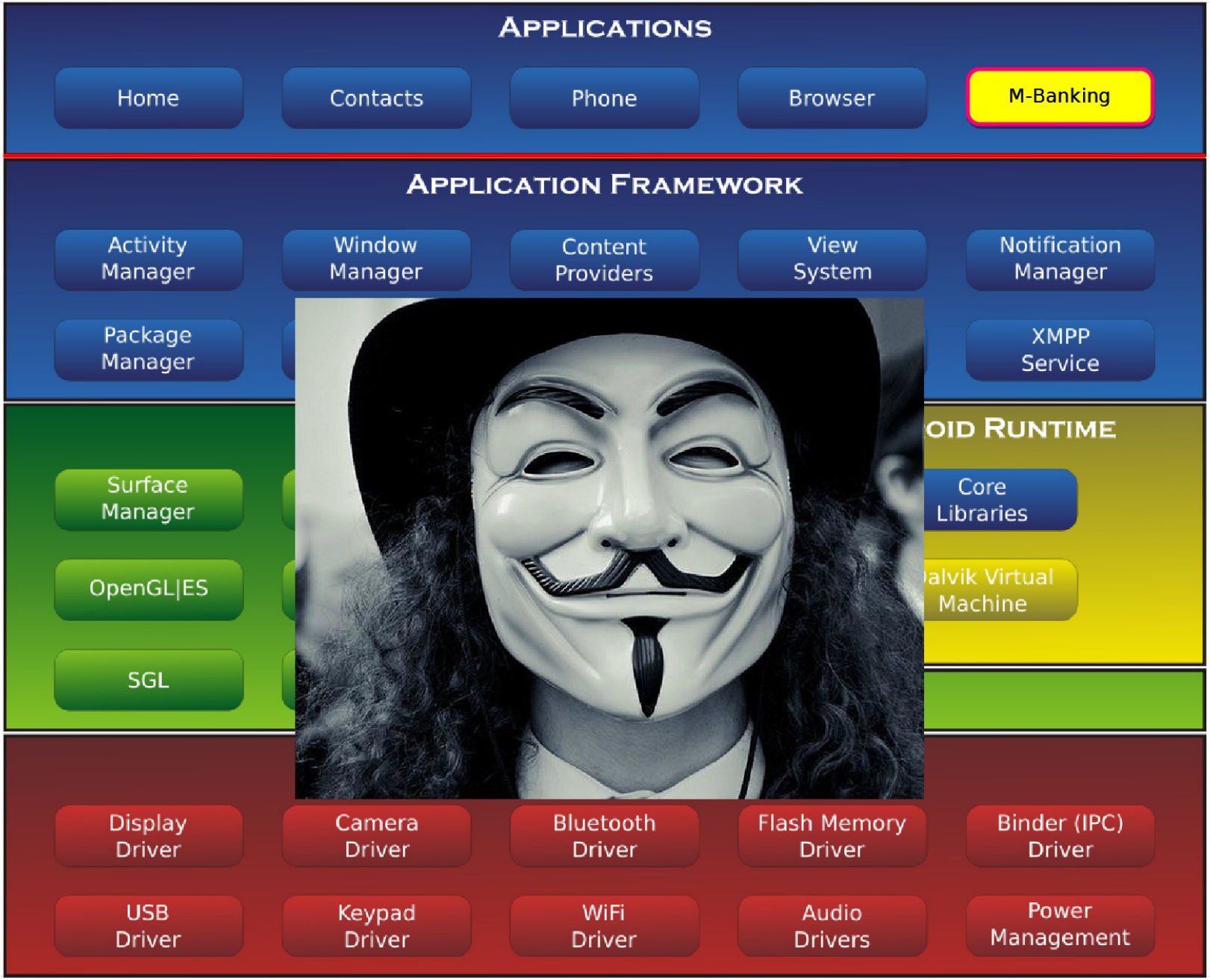
## Аппаратная защита KoolSpan

В дополнение ко всему перечисленному выше смартфон Solarin оснащен чипом шифрования KoolSpan, который отвечает за сквозное шифрование голосовых вызовов и сообщений на основе стандартов AES-256 и FIPS 140-2, отвечающим требованиям военных стандартов.

Защита с помощью KoolSpan активируется отдельным ползунком, который расположен сзади, над объективом основной камеры. Одновременно с включением шифрования и звонков отключаются все прочие каналы передачи данных со смартфона — то есть он превращается в простую «звонилку».

**Ползунок над камерой включает защищенный режим**

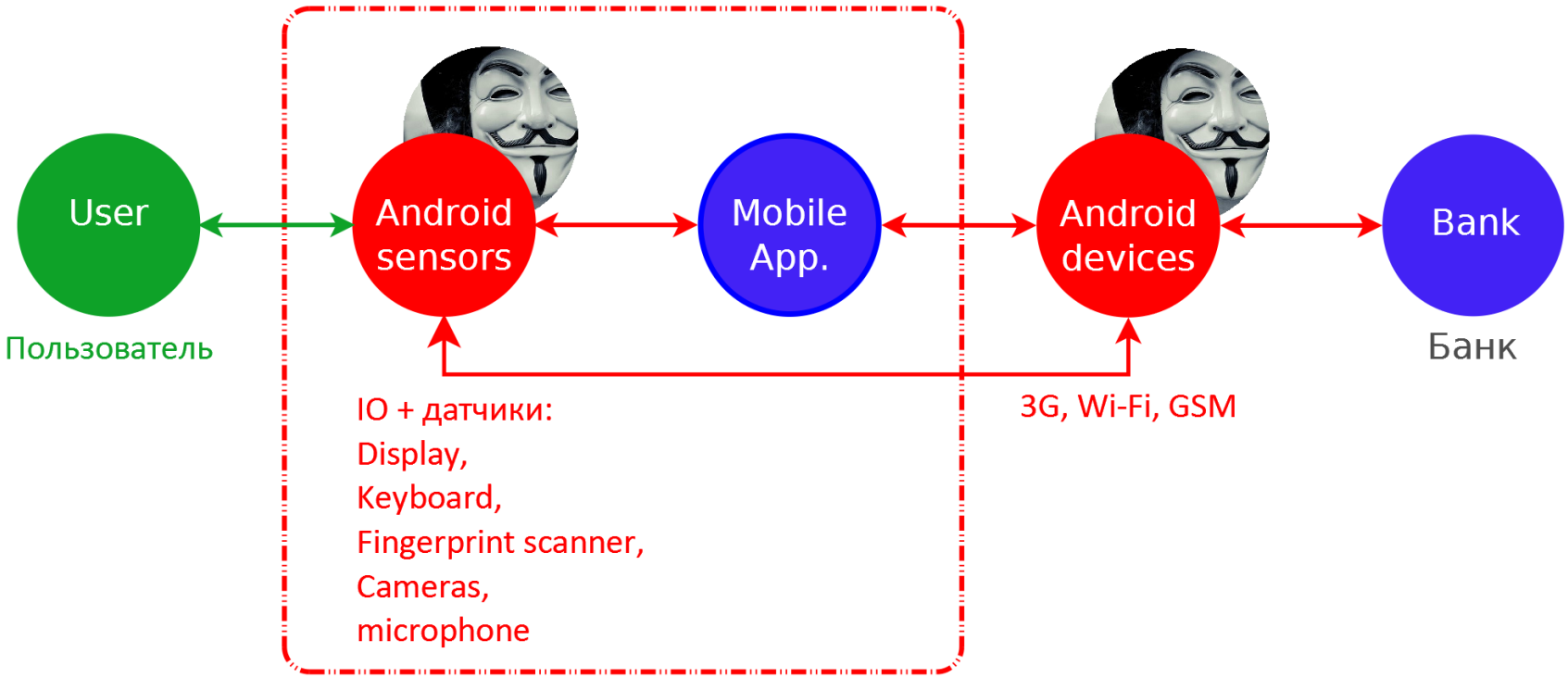

У приложения M-banking **НЕТ** СВОИХ прямых интерфейсов, СВОИХ датчиков и RAM — Display, Fingerprint, Keyboard, Camera, Microphone ++ 3G, WiFi – контролируются **Android**




Компрометация Android позволяет хакерам перехватить контроль над ВСЕМИ устройствами и процессами.

# MitE - Man-in-the-Endpoint

## удалённый параллельный контроль



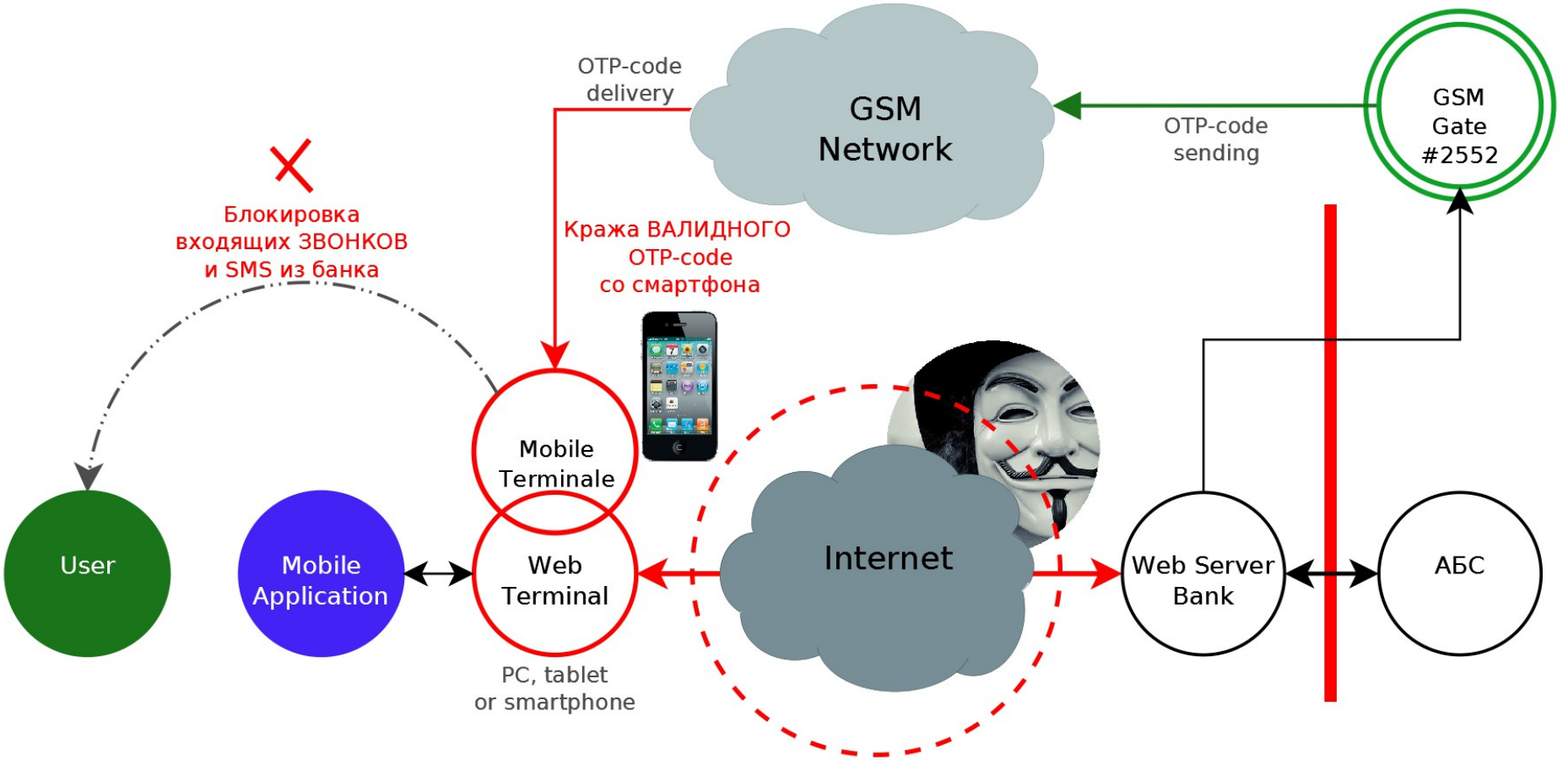

Перехват управления и УДАЛЁННАЯ
эмуляция действий Пользователя
+
блокировка звонков и SMS из банка

Engine.ER Lab



Атака класса MitE позвляет хакерам эмулировать **ЛЮБЫЕ** действия пользователя и генерировать фрод от лица пользователя

# OTP-via-SMS > Смартфон как рог изобилия ...




Компрометация смартфона превращает его для хакеров в рог изобилия ...

# Обнародован список ИТ-компаний - стратегических партнеров АНБ США



14.05.2014, СР, 11:05, Мск , Текст: Сергей Попсулин

**В число стратегических партнеров АНБ США входят крупнейшие американские производители телекоммуникационного оборудования, серверов и программного обеспечения.**



Cisco, Motorola, IBM, Oracle, Microsoft, Verizon, AT&T, Qualcomm, Qwest, Hewlett-Packard, EDS и Intel являются «стратегическими партнерами» Агентства по национальной безопасности (АНБ) США. Об этом говорится в новых документах, полученных от экс-сотрудника Агентства национальной безопасности (АНБ) и ФБР **Эдварда Сноудена** и опубликованных на сайте журналиста **Гленна Гринвальда**. О деталях партнерства в документах не сообщается.

Указано, что эти компании — поставщики телекоммуникационных и сетевых услуг - занимаются строительством сетевых инфраструктур, выпуском аппаратных платформ, ПК и серверов, операционных систем, приложений, аппаратных и программных средств защиты или относятся к системным интеграторам.

# ФБР потребовало от Apple и Google оставлять «дыры» для доступа спецслужб к данным пользователей



17.10.2014, ПТ, 13:10, Мск , Текст: Сергей Попсулин

**Директор ФБР Джеймс Коми хотел бы, чтобы Apple и Google оставляли в мобильных устройствах «бэкдоры» для доступа спецслужб к данным. Внедренное в последних версиях платформ Android и iOS шифрование по умолчанию он считает излишним и мешающим правосудию.**



Директор ФБР **Джеймс Коми** (James Comey) призвал ИТ-компании оставлять «дыры» («бэкдоры», лазейки) в своих потребительских продуктах, чтобы спецслужбы могли, в случае необходимости, получать доступ к данным пользователей.

«Правосудие может быть бессильно, если мобильный телефон или жесткий диск будет защищен», — сказал

БЕЗОПАСНОСТЬ
- Главная
- Администратору
- Стратегия безопасности
- Госрегулирование
- Техническая защита
- Пользователю

# Google ведет слежку за пользователями даже когда в смартфоне нет SIM-карты

Безопасность | Стратегия безопасности | Интернет | Веб-сервисы | Корпоративная мобильность
мобильная версия

22.11.2017, СР, 15:01, Мск , Текст: Валерия Шмырова

**Android-устройства фиксируют адреса ближайших сотовых вышек по идентификаторам Cell ID и отправляет их в компанию Google. Данные собираются и передаются даже тогда, когда на устройстве отключены геолокационные сервисы и не вставлена SIM-карта. Google начала прибегать к этой практике 11 месяцев назад и обещает вскоре ее прекратить.**



## Слежка за пользователями

Устройства под управлением ОС Android собирают сведения о местонахождении пользователей и отправляют их в компанию Google, даже если на них выключены все геолокационные сервисы, не запущено ни одно приложение или отсутствует SIM-карта. Данные отправляются в Google каждый раз, как аппарат подключается к интернету. К такому выводу пришло в ходе собственного расследования издание Quartz.

С начала 2017 г. Android-смартфоны стали запоминать адреса расположенных поблизости сотовых вышек, даже если геолокационные сервисы на устройствах отключены пользователем, и отправлять эти данные в Google, выяснило издание. Таким образом, компания стала получать данные, которые по своему составу выходят за рамки

# Откуда прилетит «весло» ...

# WhatsApp, Viber, Skype, Telegram обошли по популярности звонки по мобильнику. Опрос



18.09.2018, ВТ, 12:39, Мск , Текст: Валерия Шмырова

**Исследование компании Deloitte показало, что мессенджеры в России являются самой востребованной функцией смартфонов — их используют 93% пользователей. Таким образом мессенджеры обогнали по популярности голосовые звонки по сотовой связи.**



## Исследование Deloitte

В 2018 г. общение через мессенджеры стало у россиян более популярным, чем звонки по сотовой связи. К такому выводу пришли специалисты консалтинговой компании Deloitte, обнародовавшей исследование «Медиапотребление в России – 2018», сообщает РИА Новости.

Исследование было проведено в июне 2018 г. и охватило 8 федеральных округов, 46 субъектов и более 250 населенных пунктов.

00:01, 20 июля 2018

# Названы самые опасные приложения для смартфонов

Добавить в «Мою Ленту»


Фото: Fotoarena / ZumaPress / Globallookpress.com

Эксперты в области кибербезопасности составили список самых опасных мобильных приложений, которые могут вызвать угрозу для корпоративных клиентов. Об этом говорится в исследовании компании Appthority за второй квартал 2018 года.

Наиболее рискованными приложениями для iOS-устройств специалисты назвали мессенджеры WhatsApp и Facebook Messenger. Кроме того, в тройку лидеров антирейтинга попала навигационная программа Waze.

Приложения WhatsApp и Facebook также получили высшие баллы по уровню

02:43, 1 ноября 2019

# Чиновников по всему миру атаковали через WhatsApp



Фото: Dado Ruvic / REUTERS

Высокопоставленные чиновники в 20 странах подверглись хакерской атаке. Об этом агентству Reuters рассказали знакомые с ходом расследования источники.

Киберпреступники использовали уязвимости в мессенджере WhatsApp, чтобы получить доступ к смартфонам как минимум 1,4 тысячи пользователей. Значительную часть жертв составляют правительственные и военные чиновники из стран, большинство из которых являются союзниками США. В частности, под удар попали индийские журналисты, ученые, юристы и защитники сообщества далитов в Индии. Основная атака проходила в период с 29 апреля по 10 мая 2019 года.

# WhatsApp начал мстить за своих пользователей: Спецслужбы держали их под колпаком и читали всю переписку



30.10.2019, Ср, 12:54, Мск , Текст: Эльяс Касми

**Мессенджер WhatsApp использовался спецслужбами по всему миру для слежки за нужными им людьми. Используя уязвимости сервиса, они внедряли через него на смартфоны жертв израильское шпионское ПО Pegasus, распространяемое по лицензии и разработанное компанией NSO Group. Facebook, владеющая WhatsApp, готовится засудить NSO за незаконное использование ее мессенджера.**



## Небезопасный мессенджер

Facebook подала на израильскую компанию NSO Group в суд, обвинив ее в содействии слежке за пользователями своего мессенджера WhatsApp (она владеет им с февраля 2014 г.), NSO Group устанавливала шпионское ПО Pegasus собственной разработки через

# Скрытый в WhatsApp троян заразил 25 млн смартфонов на Android



15.07.2019, Пн, 08:26, Мск , Текст: Роман Георгиев

**Используя старую уязвимость, вредоносная программа Agent Smith заменяет рекламу в легитимных приложениях. Более 25 млн устройств в Азии уже заражены.**



## Матрица владеет твоим телефоном

Новый вредонос под ОС Android подменяет код в легитимных приложениях, чтобы выводить в них рекламные объявления. Как правило, эта реклама далека от добросовестной. Вредоносная программа уже проявилась на 25 млн устройств, - по крайней мере, так утверждают эксперты компании Check Point Software.

Исследователи назвали программу Agent Smith - в честь антагониста «Матрицы», способного принимать любое обличье.

20:43, 13 января 2017

# В WhatsApp нашли лазейку для мошенников и спецслужб




Фото: Imago Stock & People / Globallookpress.com

В мессенджере WhatsApp обнаружили уязвимость, которая позволяет злоумышленникам либо сотрудникам спецслужб перехватить зашифрованные сообщения. Об этом в пятницу, 13 января, сообщает The Guardian.

«Дыру» в приложении нашел ученый из Калифорнийского университета Тобиас Болтер (Tobias Boelter). Впервые специалист обратился к Facebook (владеет WhatsApp) в апреле 2016 года и описал суть найденной уязвимости. Руководство соцсети отметило, что в курсе подобной проблемы, но в ближайшее время не планирует устранять ее.

Болтер утверждает, что опасная уязвимость до сих пор не закрыта.

В апреле 2016 года WhatsApp внедрил сквозное шифрование сообщений (end-to-end), которое обеспечивает доступ к содержанию переписки только участникам диалога. Мессенджер не раз подчеркивал, что даже работники компании не в состоянии узнать, о чем пишут пользователи.

# На смартфоны в России и США напал троян, который невозможно удалить





05.11.2019, Вт, 14:30, Мск , Текст: Роман Георгиев

**Компания Symantec отметила резкое распространение троянца, который не удаляется даже после аппаратного сброса. Возможно, на определённых устройствах его заново устанавливает какое-то системное приложение.**

## Реклама, руткиты и регулярные возвращения

Компания Symantec обнаружила резкий рост количества заражений троянцем xHelper под Android. Вредоносная программа, заразившая за последние полгода 45 тыс. устройств преимущественно в России, Индии и США, автоматически переустанавливается на устройстве после удаления вручную и даже после сброса устройства на заводские настройки.

12:38 31 января 2019

# Обнаружен способ взломать смартфон по номеру телефона

Добавить в «Мою Ленту»

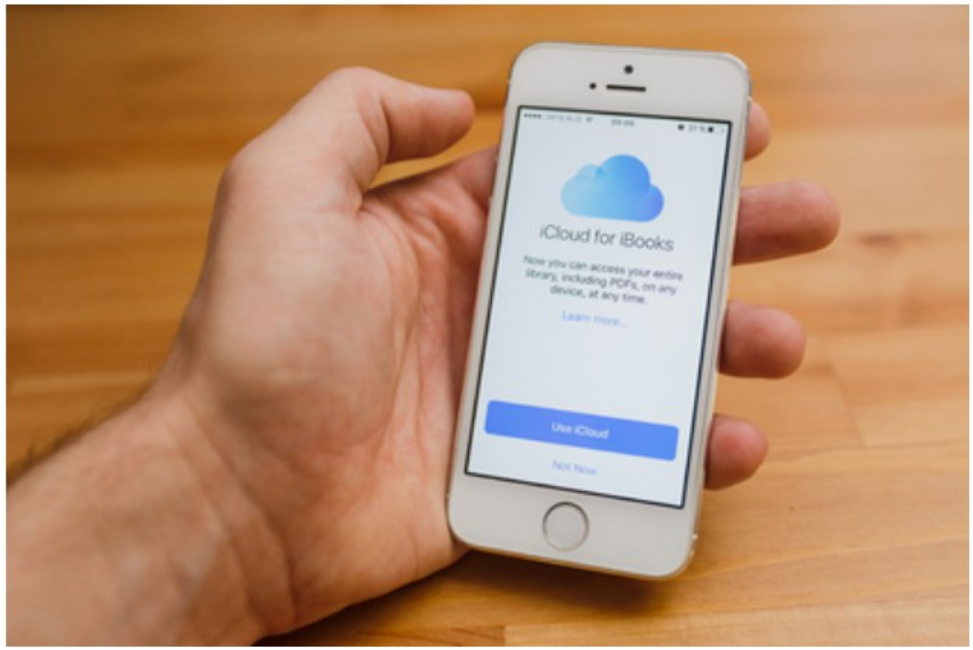



Фото: Shutterstock

Исследователь в области кибербезопасности Мелих Севим (Melih Sevim) обнаружил уязвимость, позволяющую проникнуть в хранилище iCloud на смартфонах бренда Apple. Как сообщает The Hacker News, корпорация пыталась скрыть эту ошибку от пользователей.

Сообщается, что компания связывает номер телефона, привязанный к платежным данным Apple ID, с учетной записью iCloud. Для взлома Севим ввел контактные данные постороннего человека в свой личный аккаунт. Выдав себя за владельца смартфона, он получил доступ к некоторым файлам, в том числе к заметкам.

БЕЗОПАСНОСТЬ
- Главная
- Администратору
- Стратегия безопасности
- Госрегулирование
- Техническая защита
- Пользователю
- Новости поставщиков

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

# Миллионы устройств на Android можно взломать обычной картинкой

Софт | Безопасность | Техника

мобильная версия

08.02.2019, ПТ, 10:42, Мск , Текст: Роман Георгиев

**Google внес ряд исправлений в операционную систему, исправив более 40 уязвимостей, четверть из которых была критической. Как минимум одна из них позволяет запускать произвольный код на устройстве жертвы, просто заставив ее открыть специально подготовленный графический PNG-файл.**



## Без подробностей

Критическая уязвимость в операционной системе Android позволяет злоумышленникам использовать специально подготовленные графические файлы в распространенном формате PNG для взлома мобильных устройств. Исправление этих багов может быть довольно проблематичным.

Google опубликовал бюллетень безопасности Android, в котором отдельно обозначил три критические уязвимости в компоненте Framework: CVE-2019-1986, CVE-2019-1987 и CVE-2019-1988. Все три позволяют запускать произвольный код на конечном устройстве удаленно. Самая серьезная из них (неизвестно, правда, какая именно) позволяет взламывать устройство с помощью специально подготовленного PNG-файла, причем в контексте процесса с высокими привилегиями.

# Трояны научились воровать данные с помощью Telegram



26.03.2018, ПН, 09:12, Мск , Текст: Роман Георгиев

**Эксперты по безопасности компании Palo Alto Networks обнаружили RAT-троянец для мобильных устройств, который с помощью API-сервиса Telegram крадет данные со смартфонов иранских пользователей.**



## «Крыса» в Telegram

Эксперты по безопасности компании Palo Alto Networks выявили новую вредоносную программу для Android, которая использует API для ботов в Telegram для связи с контрольным сервером (C&C) и вывода данных с устройства жертвы.

«Боты» в Telegram это специальные аккаунты, используемые, как правило, для подтягивания контента со сторонних сервисов или для отправки пользователям специализированных уведомлений и новостей.

TeleRAT - не первый вредонос, эксплуатирующий API «ботов» Telegram для проведения атак на пользователей. Ранее экспертам уже попадалась программа IRRAT, которая, правда, использовала эти API только для связи с контрольным сервером. TeleRAT, в свою очередь, производит еще и

скоро
CNEWS FORUM КЕЙСЫ 11 ИЮНЯ

ИННОВАЦИЯ ГОДА 11 ИЮНЯ

new
10 РЕЦЕПТОВ ЦИФРОВИЗАЦИИ

new
РЕШЕНИЯ KYOCERA

new
EPSON ДЛЯ ОФИСА

new
ИННОВАЦИИ ДЛЯ ЦОДА

new
КОРПОРАТИВНАЯ МОБИЛЬНОСТЬ

РОССИЙСКОЕ ПО

NETAPP: НОВОЕ В СХД

БЕЗОПАСНОСТЬ

- Главная
- Администратору
- Стратегия безопасности
- Госрегулирование
- Техническая защита
- Пользователю

# Обнаружен «троян будущего». Как он ворует деньги пользователей?

Безопасность | Пользователю | Техника | Корпоративная мобильность | мобильная версия

15.10.2018, ПН, 09:32, Мск , Текст: Роман Георгиев

**Вредоносная программа GPlayed обладает «универсальной» функциональностью и модульной архитектурой, что делает ее втройне опасной. Эксперты опасаются, что скоро у нее появятся многочисленные подражатели.**



## «Швейцарский нож» мира троянов

Эксперты по информационной безопасности компании Talos выявили новый троян под ОС Andoroid, названный им GPlayed, о котором говорят как о «предвестнике новой и очень опасной эпохи» вредоносного ПО.

GPlayed обладает всеми функциями банковского трояна и инструментов «глубокого» кибершпионажа, но самое важное - это его способность подстраиваться под среду, в которую ему удается проникнуть.

Вредонос GPlayed выдает себя за клиент Google Play и способен подгружать плагины, производить инъекцию скриптов и даже компилировать новый исполняемый .NET-код. Такая архитектура позволяет менять функциональность троянца «на

12:30, 2 апреля 2019

# Опасный мобильный вирус обнаружен в магазине Google Play

Добавить в «Мою Ленту»


Фото: Marcio Jose Sanchez / AP

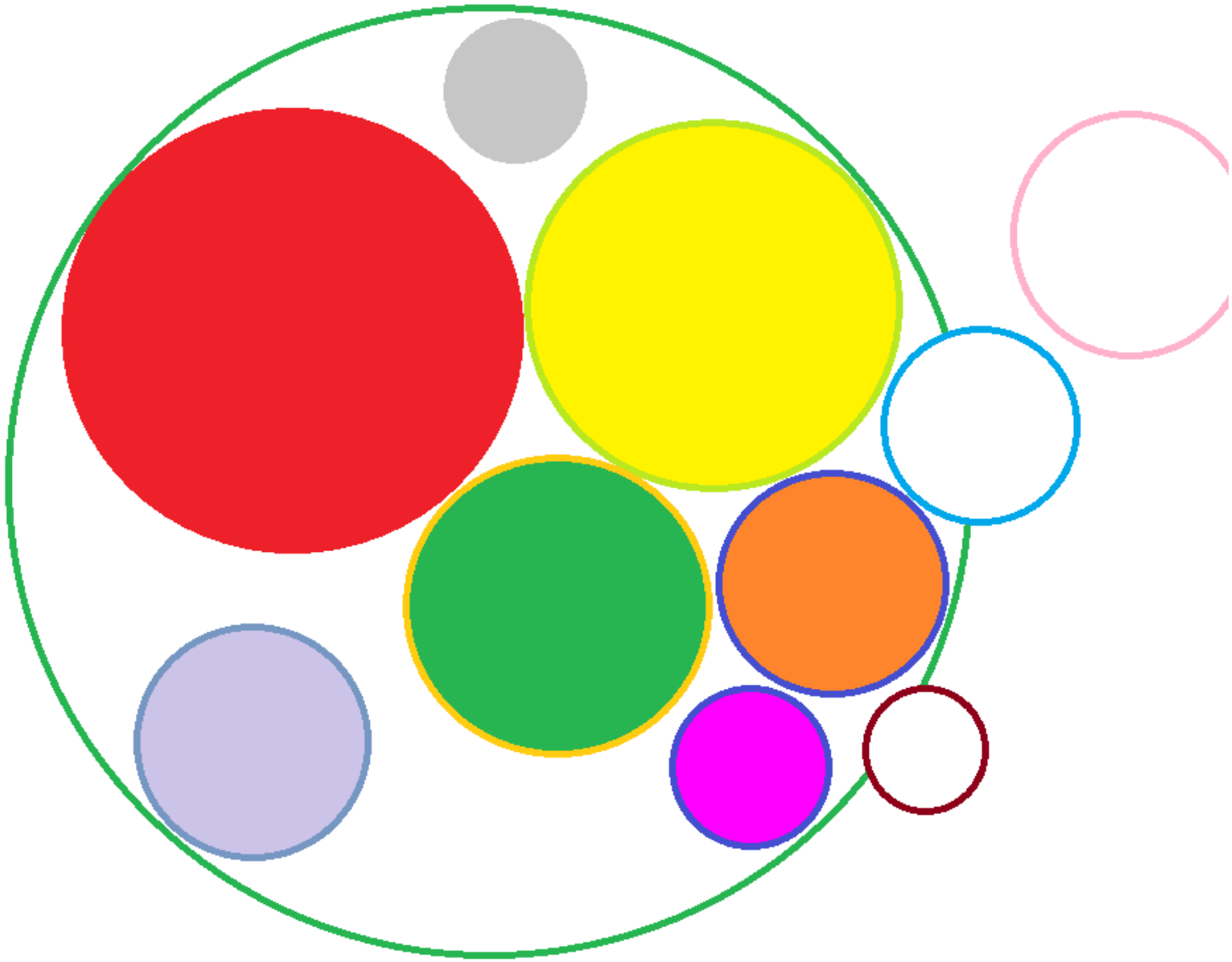
В магазине приложений Google Play обнаружилось 25 версий опасного мобильного вируса. Специалисты объединения Security Without Borders, обнаружившие вредную программу, описали ее в своем блоге.

Шпионское ПО получило название Exodus. Оно скрывалось в приложениях мобильных операторов Италии: пользователи скачивали их, поверив в фальшивые рекламные обещания о дополнительных услугах и бонусах.

Вирус передавал посторонним номер телефона жертвы и идентификатор устройства, затем загружал архив с программами, полностью контролировавшими гаджет: они могли делать снимки экрана, прослушивать разговоры, считывать переписки и отслеживать геолокацию.

Помимо этого, опасная программа могла спрятаться от некоторых установленных программ на Android, следящих за подозрительной активностью.

Engine.ER Lab



Retail & M-Banking market

Engine.ER Lab

Зачем защищать endpoint-терминал клиента?
(где деньги ??!?!)

Engine.ER Lab

Выводы для банков / вендоров:

1. Существующая структура рынка может существенно измениться после первой (*серии*?) массированных MitE-атак;
2. Незащищённый клиент склонен к миграции;
3. Защитить клиентов от MitE-атак сугубо программными методами защиты НЕВОЗМОЖНО — требуются внешние (относительно смартфона) АППАРАТНЫЕ токены или кастомизированные dedicated-смартфоны;
4. Для агрессивного роста необходимы cost-effective токены, минимизирующе затраты банка;
5. Внедрение НОВЫХ стандартов безопасности расширит рынок.

Engine.ER Lab

Что означают

IIHS,
ADAC,
NHTSA,
JNCAP,
EuroNCAP ??!??

Insurance Institute for Highway Safety
Highway Loss Data Institute

Highway safety research & communications

RATINGS NEWS TOPICS VIDEO STATUS REPORT

# UNEQUAL PROTECTION

The Ford Escape was the only poor performer out of 7 small SUVs in the passenger-side small overlap test, despite an acceptable rating on the driver side.

The **Insurance Institute for Highway Safety** (IIHS) is an independent, nonprofit scientific and educational organization dedicated to reducing the losses — deaths, injuries and property damage — from motor vehicle crashes.

The **Highway Loss Data Institute** (HLDI) shares and supports this mission through scientific studies of insurance data representing the human and economic losses resulting from the ownership and operation of different types of vehicles and by publishing insurance loss results by vehicle make and model.

Both organizations are wholly supported by **these auto insurers and insurance associations**.


FOR SAFER CARS
EURO NCAP
www.euroncap.com

Зачем автопроизводители тратят десятки миллионов долларов (USD) на краш-тесты?

# БЕЗОПАСНОСТЬ — это один из ЛУЧШИХ драйверов продаж.

To TRUST ask Toyota, Mercedes, BMW, Volkswagen, Hyundai, Ford, Nissan, Honda, Renault, Peugeot, Chevrolet, Fiat, Audi, Kia, Suzuki, General Motors, Citroen, GMC, Ferrari, Mazda, Subaru, Lexus, Volvo, Mini, Vauxhall, ISUZU ...

The Official Site of The European
New Car Assessment Programme

# LATEST SAFETY RATINGS


2017 ★★★★★

**Hyundai KONA**

Standard safety equipment

HYUNDAI

2017 ★★★★★

**Kia Stinger**

Standard safety equipment

KIA MOTORS

2017 ★★★★★

**BMW 6 Series GT**

Standard safety equipment

Share

Contact | Search | English

EURO NCAP FOR SAFER CARS

About Euro NCAP · Ratings & Rewards · Vehicle Safety · Press & Media · For Engineers

- Latest Safety Ratings
- Best in Class Cars
- Safest Family Cars
- Safest Fleet Cars
- Business & Family Vans
- Quadricycle Ratings
- Hybrid & Electric Vehicles
- Driver Assistance Systems
- Euro NCAP Advanced Rewards

The Offic
New Car

## LATEST S GS


2017 ★★★★★

**Hyundai KONA**

Standard safety equipment

HYUNDAI

2017 ★★★★★

**Kia Stinger**

Standard safety equipment

KIA MOTORS

2017 ★★★★★

**BMW 6 Series GT**

Standard safety equipment

Euro NCAP Advanced Rewards

HOW SAFE IS YOUR CAR ?

Select one or more vehicles among the following possibilities.

Make

Model

OR

Class

OR

ALL RESULTS & REWARDS

Select a make

All

+ MORE FILTER OPTIONS

## 2017 - Rating

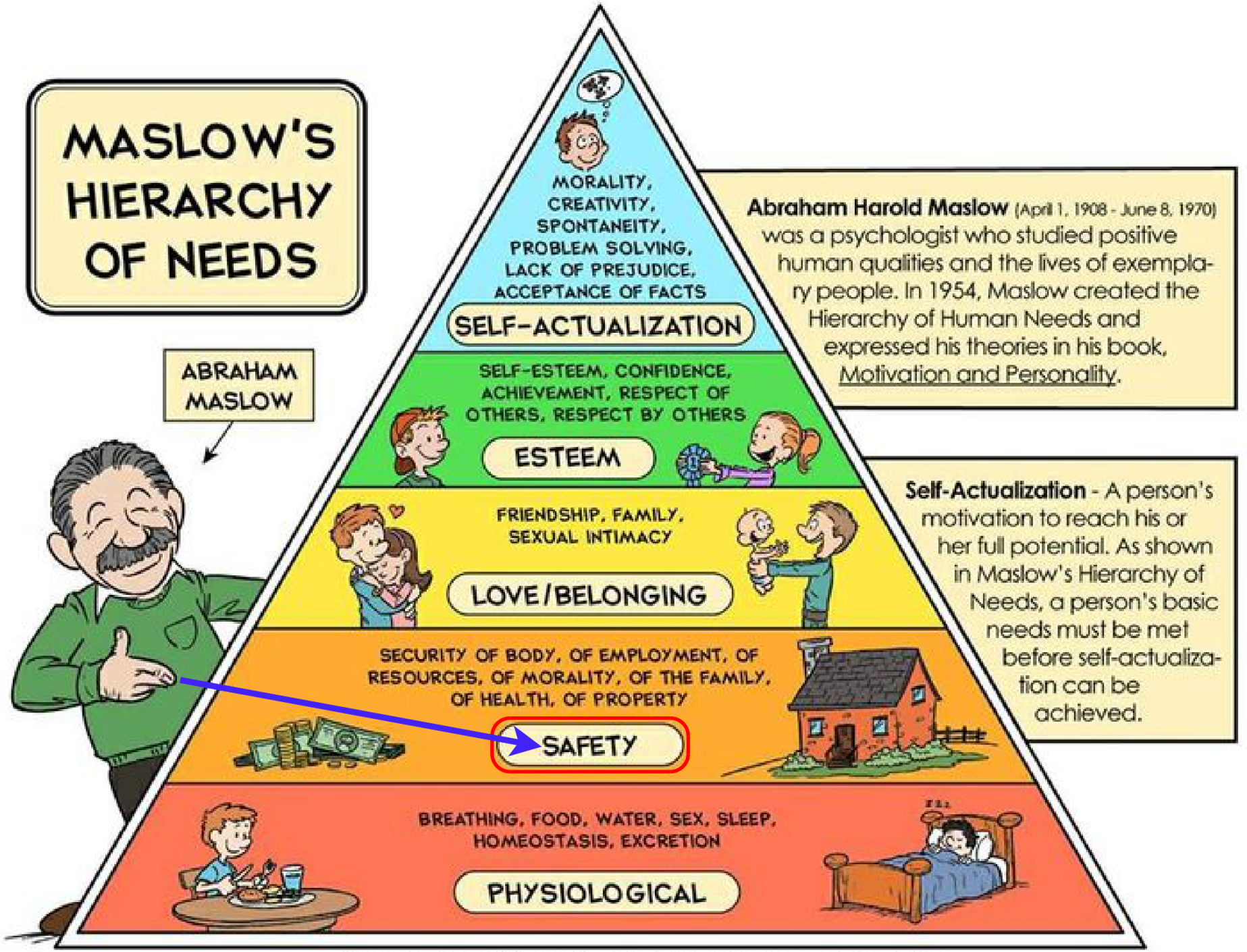
ABOUT 2017 RATING

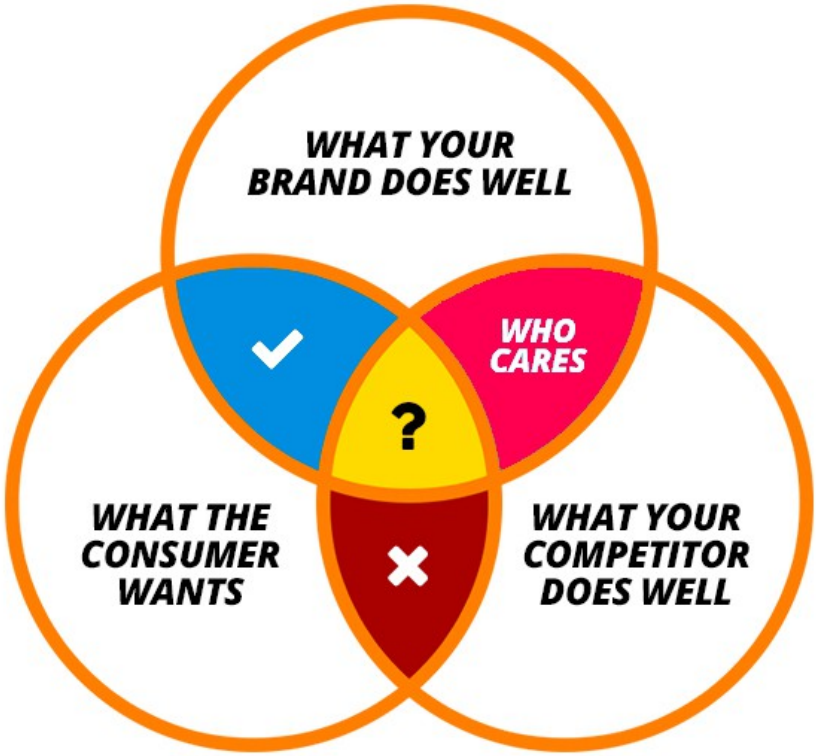
| Make & Model | Safety Equipment | Overall rating | | | | |
|---|---|---|---|---|---|---|
| Volvo XC60 | Standard | ★★★★★ | 98% | 87% | 76% | 95% |
| VW Arteon | Standard | ★★★★★ | 96% | 85% | 85% | 82% |
| Volvo V90 | Standard | ★★★★★ | 95% | 80% | 76% | 93% |
| Volvo S90 | Standard | ★★★★★ | 95% | 80% | 76% | 93% |
| VW T-Roc | Standard | ★★★★★ | 96% | 87% | 79% | 71% |
| Subaru XV | Standard | ★★★★★ | 94% | 89% | 84% | 68% |
| Subaru Impreza | Standard | ★★★★★ | 94% | 89% | 82% | 68% |
| Mercedes-Benz X-Class | Standard | ★★★★★ | 90% | 87% | 80% | 77% |
| Jaguar F-Pace | Standard | ★★★★★ | 93% | 85% | 80% | 72% |


Region61.biz


SUBARU
17
DENSO
17
WALES RALLY GB
STI Performance
MOTUL
BFGoodrich
PIAA
JT07 SRT
STi
BBS


RECARO
RECARO






# Unique Selling Proposition

### ✔ - *Winning Zone*

Clear point of difference that meets the needs.
make it even bigger.

### ✖ - *Losing Zone*

Your copetitor meets the consumer needs better then you do. you'll be crushed.

### ? - *Risky*

Competitive battle ground. use emotion, innovative, superior execution.

### *Who Cares*

Many times, competitors battle in areas the consumer just doesn't care about. Have fun wasting your time.

Engine.ER Lab

## DIY-техника безопасности для пользователей M-Banking:

1. Исходите из того, что Ваш смартфон для мессенжеров и сёрфинга УЖЕ взломан. Правильный вопрос : «СКОЛЬКО программ-шпионов сейчас «живёт» в Вашем смартфоне?»;
2. Используйте выделенный (dedicated) смартфон для M-Banking и удалите с него ВСЕ мессенжеры;
   **98%** вероятности — взлом смартфона будет произведён через мессенжеры (W'App, Telegram, Viber, WeChat и т.д.);
3. Включайте банковский смартфон только для осуществления платежей (Power_OFF <> Battery_Empty);
4. Используйте телефон-фонарик
   (2G GSM Ultra-Thin Mobile Terminal) для приёма OTP-via-SMS и звонков из банка.

Engine.ER Lab

- Когда Ной построил ковчег?
- ДО потопа.