Что знают о вас мобильные приложения?

Введение

Только в 2018 году мобильные приложения загружались пользователями более 205 миллиардов раз (рис. 1) [1].

Рисунок 1. Количество загрузок приложений

Данные, представленные Marketing Land, показывают, что 57% общего времени использования цифрового мультимедиа приходится на нативные мобильные приложения для смартфонов и планшетов [2].

Сегодня большинство пользователей хранит на своих смартфонах и других мобильных устройствах как личную, так и корпоративную информацию. По некоторым данным, более 70% хранят конфиденциальную информацию как свою, так и своего работодателя.

При этом стоит учесть, что:

- Уязвимости высокого риска были обнаружены в 38% мобильных приложений для iOS и в 43% приложений Android
- Большинство проблем безопасности находятся на обеих платформах. Небезопасное хранение данных является наиболее распространённой проблемой, встречающейся в 76% мобильных приложений. Пароли, финансовая информация, личные данные и переписка находятся под угрозой
- Хакерам редко требуется физический доступ к смартфону для кражи данных: 89% уязвимостей можно использовать с помощью вредоносных программ
- Большинство случаев вызвано слабостью механизмов безопасности (74% и 57% для приложений iOS и Android соответственно и 42% для серверных компонентов). Поскольку такие уязвимости появляются на этапе проектирования, их исправление требует значительных изменений в коде
- Риски необязательно являются результатом какой-либо одной уязвимости на стороне клиента или сервера. Во многих случаях они являются результатом нескольких, казалось бы, небольших недостатков в различных частях мобильного приложения. Взятые вместе, эти упущения могут привести к серьёзным последствиям, включая финансовые потери для пользователей и репутационный ущерб для разработчика
- Многие кибератаки полагаются на невнимательность пользователя. Повышенные привилегии или загруженное программное обеспечение могут проложить путь к разрушительной атаке

При этом то, что информацию о вас так или иначе собирают практически все мобильные (впрочем, не только мобильные) операционные системы, известно давно. Об этом регулярно говорят. Но знаете ли вы, что с не меньшим успехом информацию о вас собирают и мобильные приложения? И это не только Google Maps, Google Chrome и браузер Safari. Ведь, например, «удалённые» пользователем записи истории браузера Safari на самом деле не исчезают из «облака», а остаются в iCloud в течение длительного времени.

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

Причём Apple оказалась единственной компанией, которая продолжает хранить на своих серверах записи из истории браузера даже после того, как пользователь их удалит (рис. 2).

Но самое интересное – это приложения, которые устанавливают себе пользователи. Особенно остро эта проблема стоит перед пользователями Android, ведь, в отличие от iPhone, установить приложения, минуя Google Play, довольно просто.

Возьмём для примера известное приложение «Фонарик». Приложения-фонарики для Android запрашивают в среднем 25 разрешений для доступа к разным функциям и данным смартфонов [3].

- 408 таких приложений запрашивают до 10 разрешений
- 267 – от 11 до 49 разрешений
- 262 приложения запрашивают от 50 до 77 разрешений
- Более того, например 77 программ запросили доступ к записи звука

Рисунок 2. История посещений

- 180 приложений просили доступ к данным контактов
- 21 приложению-фонарику был необходим доступ к возможности записывать контакты

Представители Avast заявили, что доступ к личным данным пользователя таким образом могут получать не только разработчики приложений, но и рекламодатели, которым эти сведения необходимы для монетизации. Всего компания Avast изучила 937 приложений. Исследователи рассматривали как те программы, которые до сих пор доступны в Google Play Store, так и те, которые когда-либо появлялись в магазине.

Ответа на естественный вопрос «Зачем?» у меня нет! Причём это вопрос к пользователям. Зачем они дают эти разрешения?

На самом деле, все разрешения приложений можно разделить на две группы:

- Обычные
- Опасные

К обычным можно отнести такие, как доступ в Интернет, создание ярлыков, подключение по Bluetooth и так далее. Эти разрешения выдаются приложениям без обязательного согласия пользователя, то есть система вас ни о чём не спрашивает.

Для того чтобы получить одно из «опасных» разрешений, приложение должно получить разрешение от владельца устройства. Чем это опасно? Стоит ли выдавать подобные разрешения?

Опасные разрешения

В категорию «Опасные» входят группы разрешений, которые так или иначе связаны с безопасностью данных пользователя. В свою очередь, каждая из групп содержит несколько разрешений, которые может запрашивать приложение.

Стоит учесть, что если одно из разрешений пользователь уже одобрил, то все остальные разрешения из той же группы приложение получит автоматически, пользователю уже не нужно их одобрять.

Например, если приложение уже успело запросить и получить разрешение на чтение SMS, то впоследствии оно автоматически получит разрешение и на отправку SMS, и на приём MMS, и на все остальные разрешения из данной группы.

Android 8. Настроек в данной операционной системе стало гораздо больше, что одновременно и хорошо, и плохо. С одной стороны, есть больше возможностей для того, чтобы сделать систему безопаснее, с другой – в настройках стало сложнее разобраться: на них приходится тратить больше времени. Да и находятся эти настройки теперь в разных местах, в том числе довольно неочевидных. Но с помощью данного путеводителя мы попробуем облегчить вам задачу.

Разрешения, которые настраиваются в списке «Разрешения приложений» (App permissions)

В этот список входят разрешения, позволяющие приложениям получить доступ к хранящимся в смартфоне личным данным его владельца: контактам, истории звонков, коротким сообщениям, фотографиям и так далее, а также тем встроенным устройствам, которые позволяют личные данные получить и записать: камере, микрофону, телефону и GPS-приёмнику.

Прежде чем приложение получит какое-либо разрешение, оно должно в явном виде попросить его у пользователя. Вы решаете, к чему приложения получают доступ.

Выдача приложению любого из этих разрешений означает, что оно получит возможность заполучить информацию данного типа и загрузить куда-нибудь в облако, не спрашивая больше вашего явного согласия на то, что именно оно собирается делать с вашими данными.

Поэтому рекомендуется как следует подумать перед тем, как выдавать приложению то или иное разрешение. Особенно в том случае, если оно точно не требуется для работы этого приложения. Например, игре в большинстве случаев совершенно незачем иметь доступ к вашим контактам и камере, мессенджер может как-нибудь обойтись без данных о вашем местоположении, а какой-нибудь модный фильтр для камеры определённо переживёт без доступа к истории звонков.

В целом решать вам, но чем меньше разрешений вы выдадите приложениям, тем целее будут ваши данные.

SMS

Что это: Разрешение на отправку и приём SMS, MMS и WAP push-сообщений, а также на просмотр сообщений в памяти смартфона.

Чем опасно: Приложение с этими правами сможет читать всю вашу SMS-переписку, включая сообщения из банков с одноразовыми кодами для входа в интернет-банк и подтверждения транзакций.

Также приложение сможет посылать сообщения, например для того, чтобы доставить спам от вашего имени (и за ваш счёт) всем вашим друзьям. Или подписать вас на какую-нибудь платную «услугу».

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → SMS* (рис. 3).

Календарь (Calendar)

Что это: Разрешение на просмотр событий в календаре, удаление и изменение уже имеющихся, а также добавление новых событий.

Чем опасно: Доступ к электронному ежедневнику может позволить узнать, чем вы занимались в прошлом, чем будете заниматься сегодня и в будущем. Для шпионского приложения это очень полезное разрешение.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Календарь*

Камера (Camera)

Что это: Разрешение на доступ к камере, чтобы приложение могло делать фотографии и записывать видео.

Чем опасно: Однажды получив это разрешение, приложение сможет в любой момент сделать фото или записать видео, не предупреждая вас об этом. Такой компромат на вас злоумышленники могут использовать с самыми разными целями.

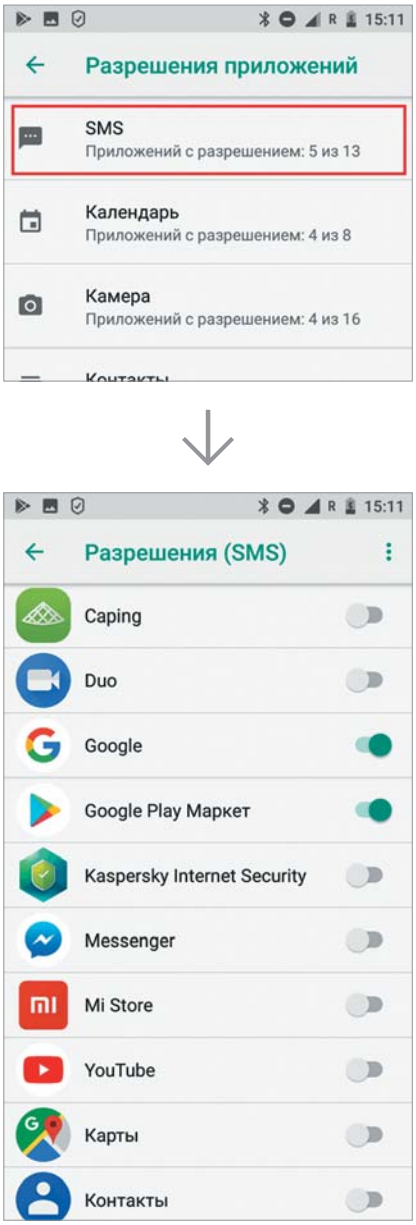

Рисунок 3. Разрешения приложений SMS

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Камера*

Контакты (Contacts)

Что это: Разрешение на доступ к вашей адресной книге: чтение, изменение имеющихся и добавление контактов, а также доступ к списку аккаунтов, которые вы зарегистрировали в данном смартфоне.

Чем опасно: Получив это разрешение, приложение может заполучить всю вашу адресную книгу и отправить эти данные на сервер. Этим злоупотребляют даже легитимные сервисы, что уж говорить о всевоз-

можных мошенниках и спамерах – для них это просто находка.

Также это разрешение даёт доступ к списку тех аккаунтов, с помощью которых вы входите в приложения на данном устройстве, например: Google, «Яндекс», Facebook, «ВКонтакте», Telegram и многих других сервисов.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Контакты*

Местоположение (Location)

Что это: Доступ к вашему местоположению как примерному (на основе данных о базовых станциях мобильной сети и точках доступа Wi-Fi), так и более точному (на основе данных GPS и ГЛОНАСС).

Чем опасно: Позволяет приложению шпионить за всеми вашими перемещениями в пространстве.

Помимо всего прочего, если наблюдать за передвижением смартфона достаточно долго, то очень легко вычислить, где живёт его владелец (длительное пребывание ночью), где он работает (длительное пребывание днём) и так далее.

Ещё один довод в пользу того, чтобы не давать это разрешение кому попало: геолокация очень быстро сажает батарейку. В итоге, чем меньше приложений пользуется определением местоположения, тем дольше будет жить смартфон от зарядки до зарядки.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Местоположение*

Микрофон (Microphone)

Что это: Разрешение на запись звука с встроенных в смартфон микрофонов.

Чем опасно: С этим разрешением приложение сможет записывать всё, что происходит рядом со смартфоном. Все ваши звонки, разговоры не по телефону – вообще всё.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Микрофон*

Нательные датчики (Body sensors)

Что это: 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, скажем, в фитнес-браслете, и вы ими пользуетесь (встроенные в смартфон датчики движения не входят в эту категорию). Эти данные могут использовать различные компании из индустрии здравоохранения, например, чтобы оценивать стоимость вашей страховки.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Нательные датчики*

Память (Storage)

Что это: Чтение и запись файлов в общую память смартфона. В Android у каждого приложения есть свой собственный кусочек памяти, куда имеет доступ только оно, а ко всему остальному объёму имеют доступ все приложения, которые получили данное разрешение.

Чем опасно: Приложение сможет «потрогать» все ваши файлы. Например, просмотреть все фотографии (да-да, и те самые фотографии из отпуска тоже) и загрузить их к себе на сервер. Или зашифровать ваши файлы и потребовать выкуп за расшифровку.

Также это разрешение опасно тем, что многие приложения используют общую область памяти для загрузки и временного хранения своих дополнительных модулей и обновлений, и вредоносное приложение может в этот момент их заразить. Эта атака называется *Man-in-the-Disk*.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Память*

Телефон (Phone)

Что это: Разрешение на чтение и изменение истории звонков; считывание вашего телефонного номера, данных сотовой сети и статуса исходящих звонков; добавление голосовой почты; доступ к IP-телефонии; просмотр номера, на который вы в данный момент звоните с возможностью завершить звонок или переадресовать его на другой номер; ну и, конечно же, исходящие звонки на любые номера.

Чем опасно: По сути, обладая этим разрешением, приложение может делать всё что угодно, если это касается голосовой связи. Узнать, когда и кому вы звонили, либо, скажем, мешать звонить (на какой-то определённый номер или вообще), постоянно отменяя звонок, подслушать ваш разговор или позвонить куда угодно за ваш счёт, в том числе на «очень платные» номера.

Где настроить: *Настройки → Приложения и уведомления → Разрешения приложений → Телефон*

Разрешения, которые настраиваются в списке «Специальный доступ» (Special app access)

Есть ещё один список разрешений – доступ к различным функциям Android. Если эти разрешения попадут в руки вредоносному приложению, то позволят ему сделать много чего нехорошего, поэтому их также следует давать крайне осторожно.

Тем более что эти разрешения спрятаны глубоко в настройках, и далеко не всегда очевидно, как именно они могут быть использованы: для понимания возможных последствий нужно неплохо представлять, как устроен Android и как работают зловреды.

Экономия заряда батареи (Battery optimization)

Что это: Новые версии Android сильно ограничивают приложениям возможность работы в фоновом режиме – делается это в первую очередь ради того, чтобы смартфон дольше работал от батареи. При этом для разработчиков тех приложений, для которых работа в фоне критична (например, музыкальные плееры, фитнес-приложения или те же антивирусы), оставлена возможность полноценно работать в фоне. Но для этого они должны попросить у пользователя разрешение на то, чтобы стать исключением, на которое не распространяется функция «Экономия заряда батареи».

Чем опасно: Например, шпионским вредоносным приложениям также может очень хотеться работать в фоновом режиме, чтобы эффективно следить за перемещением пользователя. Поэтому стоит внимательно относиться к данному разрешению и периодически проверять список приложений, которые могут беспрепятственно работать в фоне.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Оптимизация батареи → Не экономят заряд.*

Приложения администратора устройства (Device admin apps)

Что это: Это разрешение даёт приложению право пользоваться набором функций удалённого администрирования. Изначально этот набор функций был разработан для того, чтобы ИТ-службы в организациях могли правильно настраивать смартфоны сотрудников, не бегая за каждым из них, а делая всё удалённо, со своего рабочего места.

Чем опасно: Во-первых, это разрешение позволяет приложению поменять на смартфоне пароль, принудительно заблокировать экран, отключить камеру или даже удалить все данные. Во-вторых, приложение, обладающее данным разрешением, довольно сложно удалить, и зловреды очень любят это использовать, чтобы прочно закрепиться в системе. Поэтому выдавать разрешение стоит только в том случае, если вы на 100% уверены в благих намерениях приложения.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Приложения администратора устройства* (рис. 4)

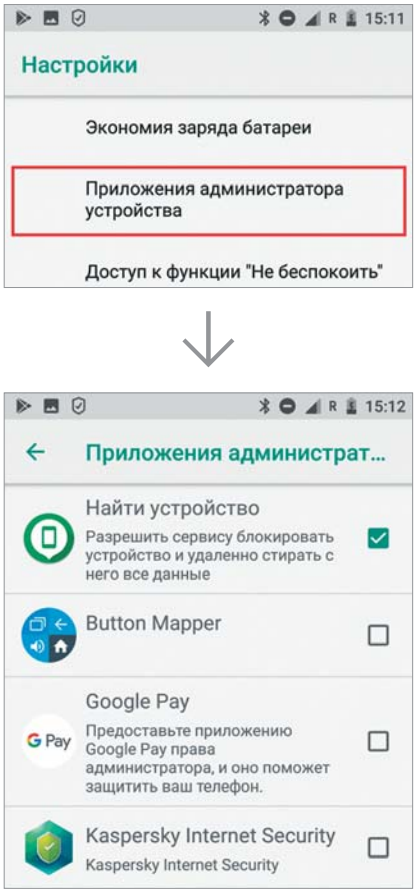

Рисунок 4. Приложения администратора устройства

Доступ к функции «Не беспокоить» (Do Not Disturb access)

Что это: В новейших версиях Android есть функция «Не беспокоить» с массой настроек. Она позволяет полностью отключить звук голосовых звонков и сообщений, скрывать всплывающие уведомления. Также можно настроить расписание, по которому работает этот режим, и добавить исключения для всех контактов или только для помеченных, чтобы на звонки и сообщения от них режим «Не беспокоить» не распространялся. Данное разрешение позволяет приложению изменять настройки этого режима.

Чем опасно: Вредоносное приложение может в нужный момент включить режим «Не беспокоить», чтобы владелец телефона пропустил какие-то важные звонки или сообщения. Например, звонок от службы безопасности вашего банка в момент совершения подозрительной транзакции.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к функции «Не беспокоить»*

Поверх других приложений (Display over other apps)

Что это: Это разрешение позволяет приложению выводить изображение поверх других приложений.

Чем опасно: Вредоносные приложения могут скрывать от пользователя какие-то важные предупреждения, а также подсовывать ему фальшивые формы ввода номера кредитной карты или пароля поверх окон легитимных приложений. Это разрешение – один из двух ключевых механизмов, используемых атакой под названием *Cloak&Dagger*.

Также это разрешение часто используют AdWare, чтобы выводить рекламные баннеры поверх всего остального, и вымогатели-блокировщики полностью перекрывают экран своим окном и требуют выкуп за то, чтобы это окно убрать.

В общем, в подавляющем большинстве случаев лучше это разрешение приложениям не выдавать.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к функции «Не беспокоить»*

Вспомогательные VR-сервисы (VR helper service)

Что это: Это разрешение предоставляет приложению доступ к приложениям и устройствам виртуальной реальности, а также возможность работать в фоновом режиме, пока пользователь использует приложения виртуальной реальности.

Чем опасно: Не считая возможности работы в фоне, которая может быть использована создателями вредоносных приложений, это разрешение выглядит не слишком опасно. Но если приложение не имеет никакого отношения к виртуальной реальности, то на всякий случай лучше ему это разрешение не давать.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Вспомогательные VR-сервисы*

Изменение системных настроек (Modify system settings)

Что это: В Android существует два типа настроек системы: обычные и *«глобальные»*, причём все по-настоящему опасные настройки постепенно переехали во вторую часть, а в первой остались всякие второстепенные, например изменение яркости и громкости. Данное разрешение позволяет приложению менять обычные настройки, но не «глобальные».

Чем опасно: Звучит угрожающе, но на самом деле, это довольно безобидное разрешение: в настройках, которые это разрешение позволяет изменять, не осталось ничего по-настоящему опасного.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Изменение системных настроек*

Доступ к уведомлениям (Notification access)

Что это: Это разрешение на обработку уведомлений. Например, оно нужно приложению Google Wear, чтобы пересылать уведомления на умные часы. Также его использует штатный лончер – «главное приложение» Android, чтобы выводить всплывающие уведомления на рабочем столе рядом с иконками соответствующих приложений.

Чем опасно: В уведомления попадает немало конфиденциальной информации: SMS, сообщения

мессенджеров и так далее. Если у какого-нибудь шпионского приложения или банковского трояна есть возможность туда подглядывать, то они могут узнать много всего такого, о чём вам, вероятно, не хотелось бы им рассказывать. Поэтому разрешать доступ к уведомлениям каких попало приложений не стоит.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к уведомлениям*

Картинка в картинке (Picture-in-picture)

Что это: Android позволяет приложениям выводить видео в режиме «картинка в картинке». Выглядит это как небольшое окошко в правом нижнем углу экрана, которое отображается поверх окон всех других приложений.

Чем опасно: Тем же, чем и разрешение «Поверх других приложений». Например, таким образом вредоносное приложение может скрыть какое-то важное предупреждение. Поэтому разрешение на «картинку в картинке» лучше выдавать только тем приложениям, в добросо**вестности которых вы уверены.**

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Картинка в картинке*

Доступ к платным SMS (Premium SMS access)

Что это: У Google есть *специальный список*, в который попадают номера платных SMS-сервисов в разных странах мира. Если какое-то приложение пытается отправить SMS на номер из этого списка, то система выводит предупреждение: спрашивает пользователя в явном виде, точно ли ему это нужно и следует ли разрешить приложению это делать.

Чем опасно: Существуют целые семейства зловредов, зарабатывающих тем, что тайком подписывают пользователей на платные SMS-сервисы. Не очень понятно, насколько список номеров Google полон, но, вероятно, он защищает хотя бы от самых популярных троянов-подписчиков.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к платным SMS*

Неограниченный мобильный Интернет (Unrestricted data access)

Что это: Для экономии мобильного трафика и заряда батареи Android позволяет настроить, какие приложения могут использовать передачу данных в фоновом режиме (это настраивается для каждого приложения индивидуально: для этой настройки не существует полного списка, где можно было бы быстро расставить галочки).

Кроме того, в Android есть более жёсткий общий режим «Экономия трафика» (его можно включить в *Настройки → Сеть и Интернет → Передача данных → Экономия трафика*). При его включении передача данных в фоне для большинства приложений отключается. Чтобы приложение продолжало иметь доступ к передаче данных при активированной «Экономии трафика», оно должно запросить данное разрешение.

Чем опасно: По большому счёту, фоновая передача данных в режиме строгой экономии трафика может понадобиться только тем приложениям, которые используются для общения: мессенджерам, почтовым клиентам, социальным сетям и так далее, чтобы вовремя доставлять вам сообщения. Глобально интернет в роуминге может быть очень и очень не дёшев. В результате можно попасть на очень серьёзные деньги!

Если данное разрешение запрашивает какое-то приложение, которое не имеет никакого отношения к общению, то это хороший повод задуматься, а не пытается ли оно за вами шпионить.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Неограниченный мобильный Интернет*

Доступ к истории использования (Usage access)

Что это: Это разрешение позволяет приложениям получить доступ к метаданным вашего устройства. Например, к таким: какими приложениями вы пользуетесь и как часто, какой у вас оператор, какой язык выставлен в настройках и так далее.

Чем опасно: Никаких личных данных как таковых с помощью этого разрешения приложение получить не сможет. Однако по косвенным данным об использовании смартфона можно составить в достаточной степени уникальный цифровой портрет пользователя, который может пригодиться для слежки.

Также это разрешение используют банковские зловреды, чтобы отслеживать, какое приложение в данный момент запущено и показывать фишинговое окно, созданное для имитации конкретного приложения (например, банковского).

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к истории использования*

Установка неизвестных приложений (Install unknown apps)

Что это: По сути, это примерно то же самое, что в прежних версиях Android называлось разрешением на установку из неизвестных источников. Но если раньше это была всего одна галочка, то в Android 8 настройки более сложные. Теперь отдельные приложения могут запрашивать право на установку других приложений и каждому из них можно запретить это или разрешить. Например, разрешить делать это только файловому менеджеру (впрочем, не стоит) (рис. 5).

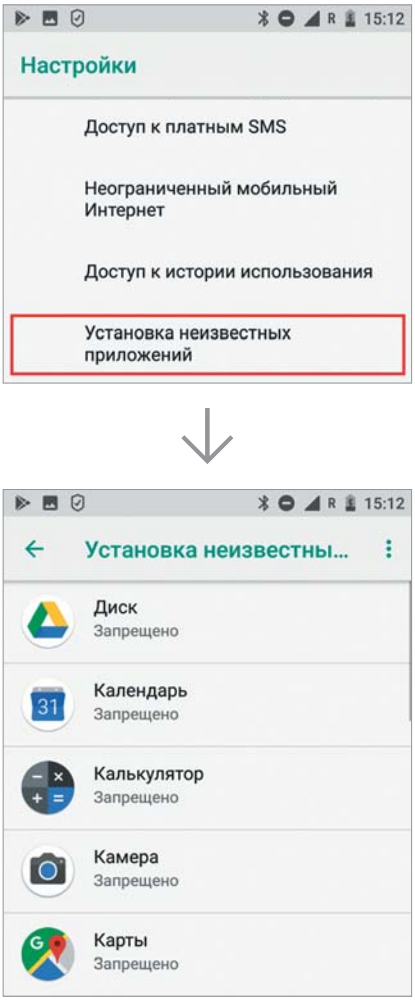

Рисунок 5. Установка неизвестных приложений

Чем опасно: Даже в Google Play периодически *пробираются вредоносные приложения*, что уж говорить о программах, загруженных с сомнительных сайтов. Рекомендуем запретить установку неизвестных приложений всем программам в вашем смартфоне, особенно браузеру – это убережёт от автоматической загрузки и установки зловредов со взломанных сайтов.

Когда вам всё-таки нужно что-то установить не из официального магазина (дважды подумав, стоит ли оно того), не забудьте вернуть запрет сразу после того, как приложение установлено.

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Установка неизвестных приложений*

Разрешения, которые настраиваются отдельно

Помимо тех пунктов настроек, которые собраны в списках «Разрешения приложений» и «Специальный доступ», в Android 8 есть ещё несколько важных разрешений, на которые стоит обратить внимание. Эти разрешения при неправильном использовании могут быть даже более опасными.

Специальные возможности (Accessibility)

Что это: Это очень мощный набор возможностей, который изначально был создан для того, чтобы облегчить жизнь людям с нарушениями зрения. «Специальные возможности», например, позволяют приложению зачитывать вслух всё, что происходит на экране. И наоборот, переводить голосовую команду, отданную пользователем, в то или иное действие с графическим интерфейсом.

Чем опасно: Этот набор возможностей позволяет одному приложению получить доступ к тому, что происходит в других приложениях, тем самым нарушая принцип изоляции, принятый в Android.

Используя «Специальные возможности», вредоносное приложение может подсматривать за тем, что вы делаете. А также делать что угодно с графическим интерфейсом: грубо говоря, нажимать за вас любые кнопки. Например, оно может изменить настройки, подтвердить любые действия, подписаться на что-нибудь платное или даже купить какое-нибудь приложение в Google Play. Этот набор возможностей – один из двух ключевых механизмов, используемых атакой под названием *Cloak&Dagger*.

Где настроить: *Настройки → Спец. возможности* (рис. 6)

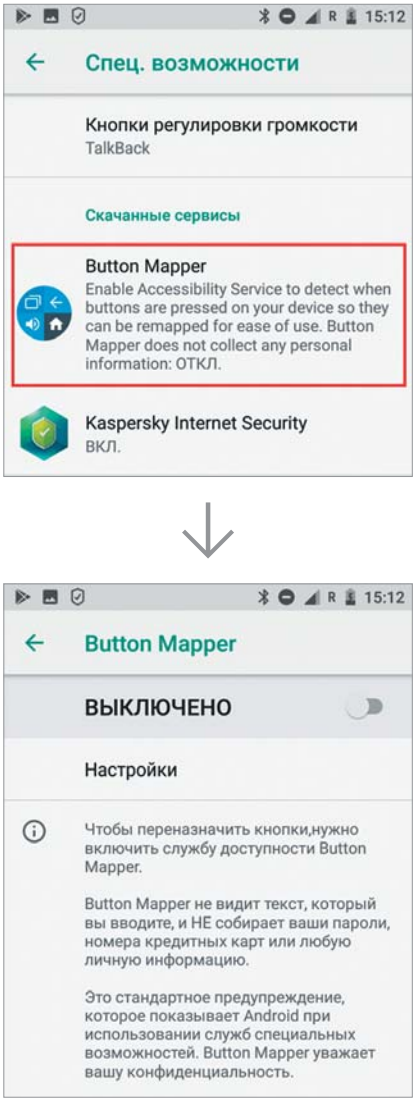

Рисунок 6. Специальные возможности

Запрос на доступ к «Специальным возможностям» – это не всегда прямой признак вредоносной деятельности. Некоторые легитимные приложения используют этот механизм во благо. Например, мобильные антивирусы. Им он нужен для того, чтобы вовремя замечать подозрительное поведение других приложений.

Но в целом, перед тем как разрешать приложению доступ к «Специальным возможностям», лучше хорошо подумать: последствия могут быть очень неприятными.

Приложения по умолчанию (Default apps)

Что это: Ещё один список разрешений, вынесенный в отдельный пункт настроек и заслуживающий повышенного внимания. В Android есть набор приложений, которые используются по умолчанию для ключевых функций смартфона:

- Помощник и голосовой ввод – голосовой помощник по типу Google Assistant
- Браузер – приложение, которое будет по умолчанию использоваться для показа веб-страниц
- Главное приложение – его ещё называют «лончер» – это графическая оболочка, которая отвечает за меню приложений, рабочий стол, виджеты и так далее
- Приложение для звонков – приложение, которое будет использоваться для телефонной связи
- SMS – приложение, которое будет заниматься всем, что связано с короткими текстовыми сообщениями

Для того чтобы стать одним из приложений по умолчанию, программа должна спросить у пользователя разрешение.

Чем опасно: Например, многие банковские трояны очень хотят стать приложением по умолчанию для SMS: таким образом они могут скрывать сообщения о списаниях от банков и воровать одноразовые коды подтверждения операций.

Заметим, что этот трюк уже успешно освоен большинством банковских троянов и используется киберпреступниками на постоянной основе. Неприятных сценариев с использованием приложений по умолчанию гораздо больше. Поэтому стоит обстоятельно подумать, перед тем как разрешить приложению стать «по умолчанию».

Где настроить: *Настройки → Приложения и уведомления → Расширенные настройки → Приложения по умолчанию* (рис. 7)

Права суперпользователя (Root privileges)

Что это: На «рутованном», то есть с полученными правами суперпользователя, смартфоне можно изменять любые настройки, получать доступ к любым файлам, в том числе системным, удалять и устанавливать любые приложения из любых источников, ставить любую прошивку и так далее.

Чем опасно: Ту же самую силу root-привилегий получает не только пользователь, но и установленные на смартфоне приложения. И они могут воспользоваться открывшимися

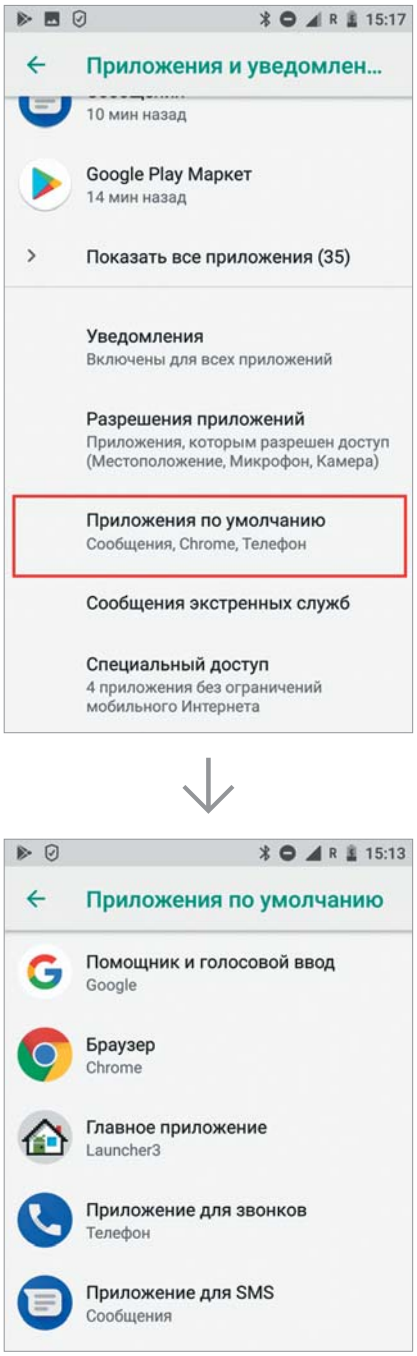

Рисунок 7. Приложения по умолчанию

возможностями для кражи любых имеющихся в смартфоне данных, тотальной слежки и прочей вредоносной деятельности.

Если все перечисленные выше разрешения позволяют получать доступ к данным и функциям, доступ к которым так или иначе предусмотрен операционной системой Android, то root-привилегии дают возможность получить доступ к тем данным и функциям, к которым вообще-то никогда и не планировалось никого пускать. И это, уже не говоря о том, что приложение, имеющее root, само может настроить себе все разрешения.

Потому, если собираетесь «рутовать» смартфон – хорошенько подумайте, стоит ли оно того. Если в систему проберётся зловред, умеющий пользоваться root-привилегиями, то последствия могут быть гораздо более неприятными, чем в случае «нерутованного» Android.

Кроме того, даже если пользователь не «рутовал» свой смартфон сам, кто-то мог сделать это за него. Например, при установке на смартфон жертвы *шпионских приложений* их разработчики рекомендуют или даже требуют предварительно получать root-привилегии. Также некоторые трояны умеют *получать root-привилегии, используя уязвимости в Android*. Стоит иногда проверять, не получен ли root в вашем смартфоне без вашего ведома.

Где настроить: Получение прав суперпользователя не является штатной функцией Android, поэтому настроить это средствами операционной системы никак нельзя. Более того, даже проверить, получен ли на вашем смартфоне root-доступ или нет, также штатными средствами ОС невозможно (рис. 8).

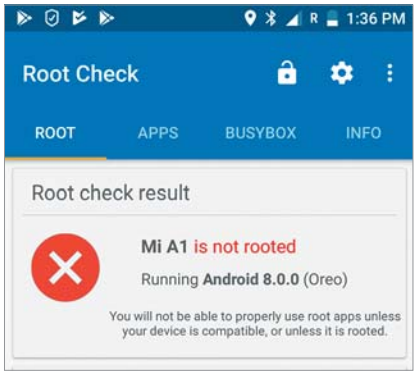

Рисунок 8. Проверка root – красный цвет сообщений означает, что права суперпользователя на этом смартфоне не получены

Если проверка покажет, что ваш смартфон «рутованный», хотя вы ничего такого не делали, – это верный признак, что к вам в смартфон попало что-то неприятное. Быть может, не повезло – вы скачали троян, а может быть, кто-то установил шпионское приложение, чтобы следить за вами. В таком случае рекомендуем сохранить куда-нибудь личные файлы и попытаться как-то избавиться от root, ведь для разных телефонов работают различные способы.

Как настроить разрешения приложений

Есть несколько способов настроить разрешения приложений в Android. Во-первых, приложения запрашивают разрешения в тот момент, когда собираются ими воспользоваться. Можно им это разрешить или запретить. В Android 8 такие запросы выглядят примерно так:

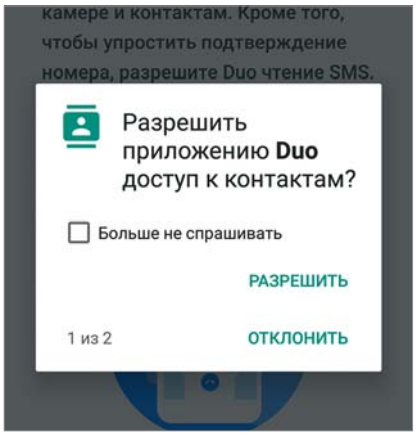

Рисунок 9. Разрешить приложению доступ к контактам

Во-вторых, можно воспользоваться группами разрешений, чтобы посмотреть полные списки тех приложений, которые запросили (или могут запросить в будущем) или уже получили определённое разрешение. Соответственно, если при проверке этого списка вам что-то среди уже выданных разрешений покажется подозрительным, то можно их отозвать (рис. 10).

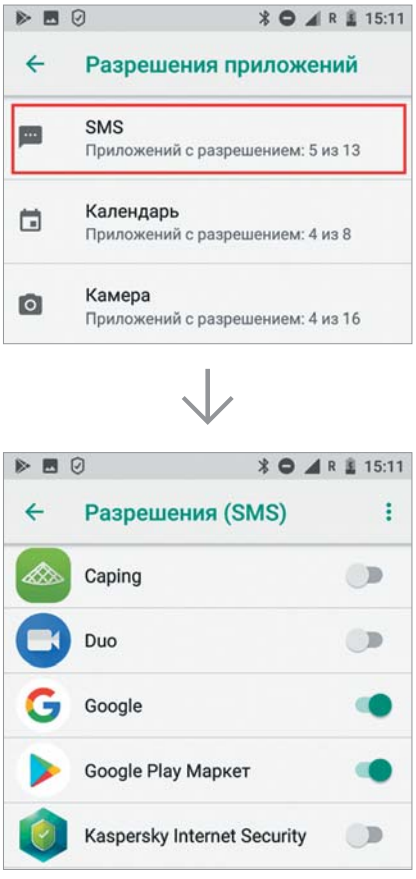

Рисунок 10. Разрешение приложений

В-третьих, есть возможность поступить иначе: для каждого из установленных приложений посмотреть, какие разрешения у него уже есть и какие оно может когда-нибудь запросить. Опять же вы можете отозвать какие-либо разрешения у приложения, если вам что-то не нравится. Однако будьте готовы к тому, что в приложении что-то может перестать работать (рис. 11).

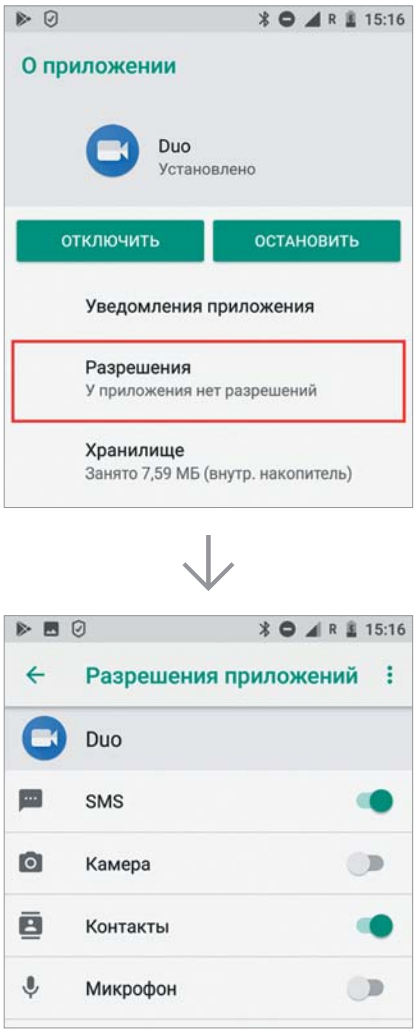

Рисунок 11. Разрешения

Кстати, в настройках Android 8 есть удобнейшая система поиска, по которой можно найти любой пункт меню настроек, если знать, как он называется, включая настройки для каждого из приложений, которые можно найти по названиям этих приложений.

Как видите, Android 8 позволяет гибко и удобно оградить всю вашу ценную информацию и доступ к наиболее опасным функциям операционной системы от слишком жадных до чужих данных или откровенно вредоносных приложений. Не пренебрегайте этой возможностью, всегда думайте о последствиях выдачи тех или иных разрешений и смело отказывайте в доступе, если что-то выглядит подозрительно.

Как увидеть, что разрешено вашим приложениям?

Большинство пользователей много времени проводит, используя приложения: читает новости, проводит время в социальных сетях, слушает музыку, смотрит фильмы, читает электронную почту и т.д. В это время каждый раз стоит проводить аудит этих приложений, чтобы убедиться, что они не перехватывают данные и не выходят за рамки, не собирают данные о вас и не контролируют вас больше, чем хотелось бы.

Выбор разрешений для приложений

Разрешения для приложений – это привилегии, которые имеет приложение, например возможность доступа к камере вашего телефона или списку контактов ноутбука, но решение о том, какие из разрешений включать или выключать, не является строго научным.

Вообще-то, предоставление этих разрешений само по себе ошибкой не является, ведь, как правило, доверенные разработчики не запрашивают ничего лишнего, что им не нужно для функционирования приложения, даже если это не сразу понятно.

Например, Facebook Messenger запрашивает доступ к вашему микрофону не потому, что он подслушивает вас, а потому, что он имеет функцию голосовой почты.

Тем не менее, если вы не планируете использовать эту функцию – можете её запретить.

Если вы действительно хотите углубиться в разрешения, которые просит у вас приложение, проверьте данные и политику конфиденциальности приложения, которые должны объяснить, что он делает с собранными данными (например, это ваше местоположение или список контактов). Эти политики часто формулируются непонятным языком, но они должны помочь решить, что запретить, а что нет.

Даже если вы не вносите никаких изменений, всё равно хорошо бы знать, какие привилегии вы предоставляете своим приложениям. Если есть сомнения, просмотрите список приложений или веб-сайт для получения более подробной информации. Если повезёт (и разработчики выполнили свою работу), вы можете найти список запрошенных разрешений и то, для чего они используются.

Опять же, это может помочь в выборе того, какие из них отключить. Если отключение определённого разрешения заставляет приложение работать с ошибками, вы всегда можете включить его. Рассмотрим, как это сделать на всех основных платформах.

Разрешения приложений в различных операционных системах

Разрешения для Android-приложений

Увы, Android поставляется в различных вариантах, в зависимости от того, какой производитель делает телефон. Ваша версия может не соответствовать в точности, но вы должны найти что-то подобное на своём телефоне.

Откройте «Настройки», меню «Приложения и уведомления». Затем нажмите на приложение, которое хотите посмотреть (если вы не можете его обнаружить, нажмите «Просмотреть все»). Нажмите «Разрешения», чтобы увидеть всё, к чему приложение имеет доступ: приложение обмена сообщениями, например, может иметь доступ к SMS. Чтобы отключить разрешение, нажмите на него. Если разрешение особенно важно для приложения, вам может потребоваться нажать окно подтверждения.

Более полный список разрешений можно найти, нажав «Разрешения на приложение» на экране «Приложения и уведомления». Здесь вы можете просматривать по разрешению от доступа к микрофону до журналов вызовов и отключать всё, что вам не подходит. Как и прежде, вы будете предупреждены, если отключите разрешение, которое является необходимым для приложения.

Если заметили, что приложение ведёт себя странно после того, как вы удалили определённое разрешение, или часть его больше не работает, нужно определить, дать ли это разрешение или жить без этого конкретного приложения.

Разрешения для приложений iOS

Как и в случае с Android, приложения iOS запрашивают разрешения, когда они им понадобятся. Хотя обычно запросы, в том числе и уведомления, появляются тогда, когда вы впервые

устанавливаете что-то новое. Вы можете аннулировать эти разрешения в любое время.

В приложении «Настройки» нажмите «Конфиденциальность», чтобы просмотреть все разрешения, доступные на вашем телефоне: доступ к фотографиям, данные о движении и пригодности, местоположение вашего телефона и т.д. Нажмите любую запись, чтобы увидеть приложения, соответствующие этим разрешениям, и отключить эти разрешения, если это необходимо.

Точный выбор зависит от разрешения. Например, для данных о местоположении вы можете предоставлять доступ к приложению всё время или только при открытии приложения. Тем временем в Apple Health вы можете предоставить доступ к определённым данным, например время сна, но не пройденные шаги.

Прокрутите экран «Настройки» за пределами меню «Конфиденциальность», чтобы найти отдельные записи приложений. Нажмите на любое приложение, чтобы получить доступ к тем же разрешениям, что и раньше, плюс некоторые дополнительные, например доступ к уведомлениям и разрешение использовать сотовые данные, а также Wi-Fi. Опять же, простого нажатия на опцию или переключатель достаточно, чтобы предоставить или отказаться от разрешения.

Разрешения на использование Windows

По мере развития Windows 10 операционная система становится всё более похожей на ОС для смартфона в том, как обрабатываются приложения, и включает в себя способ разрешения приложений. Откройте «Параметры», затем выберите «Конфиденциальность» и перейдите в подраздел «Разрешения приложений», чтобы узнать, что ваши установленные приложения могут выполнять в ОС.

Параметры сортируются по разрешению, а не по приложению, поэтому нажмите любую из записей с левой стороны, чтобы увидеть приложения с такими доступами, как местоположение, камера, фотографии и т.д. Каждый экран выглядит несколько иначе, но если вы прокрутите вниз, то увидите список приложений, связанных с этим разрешением. Вы можете предоставить или отменить их щелчком по соответствующему переключателю.

Со всеми этими разрешениями вы можете полностью отключить соответствующий доступ приложений, например можете решить, что не хотите, чтобы какое-либо из приложений использовало веб-камеру. Обратите внимание, что эти экраны охватывают приложения, установленные только из Windows Store и некоторые приложения, входящие в комплект с Windows, таких как Mail и Cortana.

Для полнофункциональных настольных приложений, имеющих доступ ко всем вашим системным ресурсам, например Photoshop, нет простого способа управления разрешениями, так как эти приложения могут иметь некоторые параметры в соответствующих окнах настроек.

Разрешения для приложений MacOS

Наконец, для macOS, в составе которой достаточно простой экран управления разрешениями, очень похожий на тот, который находится в iOS. Чтобы найти его, откройте меню Apple, затем выберите «Системные настройки». Нажмите «Безопасность и конфиденциальность», затем откройте вкладку «Конфиденциальность».

Здесь вы можете увидеть все категории разрешений: от местоположения до приложения. Нажмите на любую из записей с левой стороны, чтобы узнать, какие приложения запросили и получили разрешение. Эти экраны выглядят несколько иначе, в зависимости от того, с каким разрешением вы имеете дело, но всё достаточно просто.

Чтобы внести изменения в разрешения, щёлкните значок блокировки в левом нижнем углу, затем введите имя пользователя и пароль macOS, чтобы подтвердить, что у вас есть полномочия на изменение этих параметров. Затем можете снять флажок рядом с любым разрешением, которое вам не нравится. Обратите внимание, что изменения не будут применяться для открытия приложений до тех пор, пока соответствующие приложения не будут перезапущены.

Как и в Windows, настольные приложения, конечно, более сложны, чем их мобильные аналоги, поэтому вы можете найти больше разрешений и параметров конфиденциальности, вникая в сами программы, поскольку у большинства будет панель настроек.

Просто помните, что, даже когда вы устанавливаете разрешения на приложение так, как вам нравится, результат всё ещё может быть неопределённым в отношении того, что они будут делать с информацией, которую собирают.

Самый безопасный способ – это не загружать приложения, которым вы не доверяете.

Вместе с тем нужно признать, что проблема разрешения приложений – это далеко не единственная проблема.

Увы, стоит помнить и о том, что критические проблемы безопасности, патчи к которым выпущены много лет назад, до сих пор присутствуют в популярных приложениях Android и официально распространяются через Google Play Store. Почему?

Всё просто. Разработчики не смогли (не захотели) правильно использовать патчи, выпущенные для сторонних компонентов. Почему? Да потому что продукт уже продаётся, значит, нужно его продавать и выпускать новый. Цель разработчика – не безопасность пользователя, а получение прибыли!

Исследователям компании Check Point удалось выявить три критические «дыры», допускающие выполнение произвольного кода. Эти дыры используются сторонними библиотеками, на которые опираются многие приложения. Патчи были выпущены в 2014, 2015 и 2016 годах. Очень часто разработчики программ для смартфонов полагаются на библиотеки, которые заимствуют у проектов с открытым исходным кодом. Если в библиотеке найдена дыра, то, как правило, разработчики выпускают соответствующий патч. Но гарантии, что авторы мобильных приложений будут использовать этот патч, нет никакой.

Результаты проверки Check Point удручают: среди «дырявого» софта есть очень популярные приложения, скачанные из официального магазина сотнями миллионов пользователей. Исследователи перечислили их: Facebook, Facebook Messenger, Lenovo SHAREit, Mobile Legends: Bang Bang, Smule, JOOX Music и WeChat [5].

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам информационной безопасности