CIS
Современные Информационные Системы
№ 1 (11) / 2020

«ГОРЯЧИЕ» технологи 2020

Стр. 46

Мнения российских ИТ-экспертов

Google & Privacy

Стр. 36

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам ИБ

Кибер-мошенничество

в цифровых сервисах

Стр. 42

Екатерина Данилова
Менеджер по развитию бизнеса
Kaspersky Fraud Prevention

ПРЕДИСЛОВИЕ

ОПЫТ

ИСТОРИЯ

ФОТООТЧЁТ

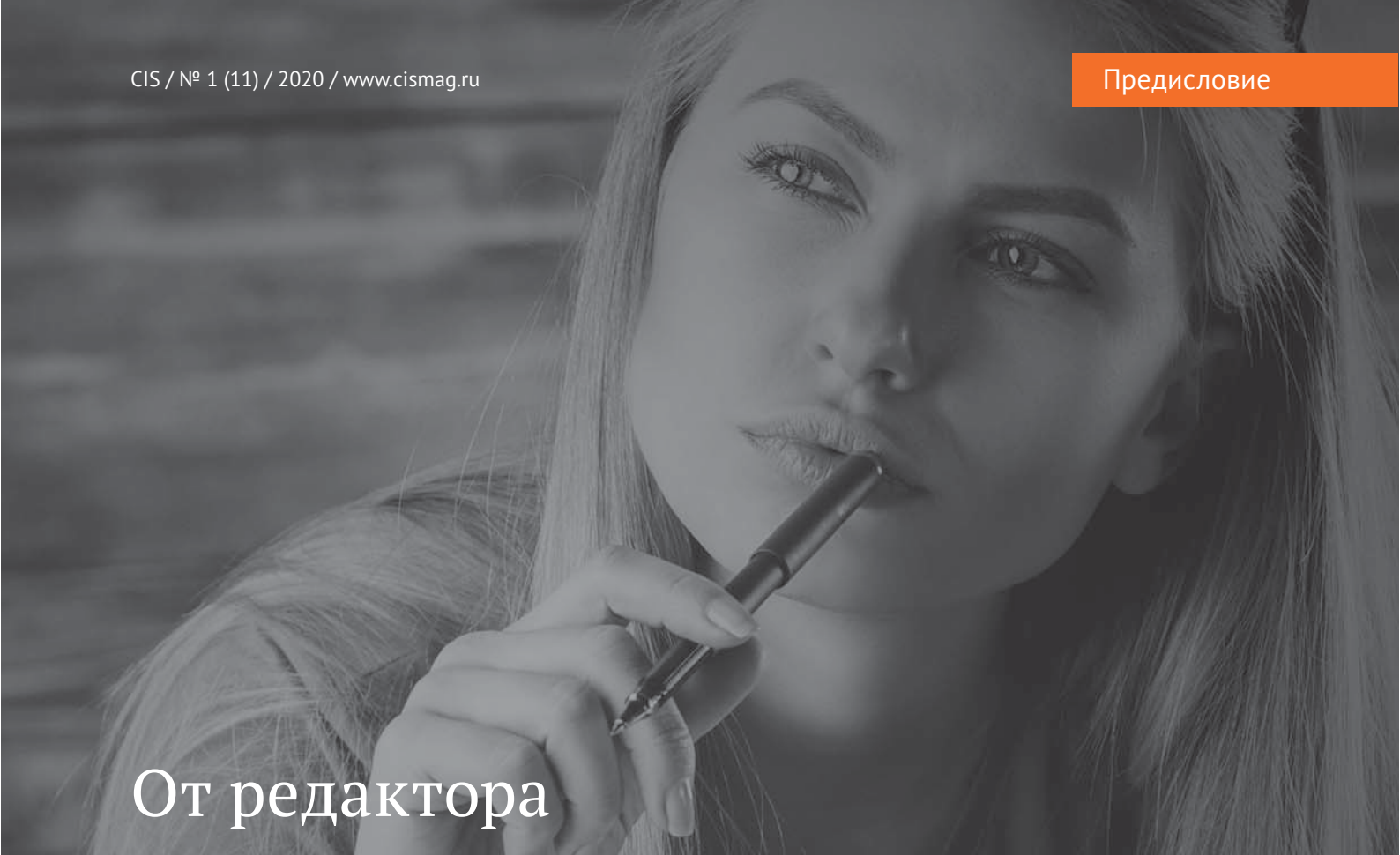
ТЕХНОЛОГИИ

КУЛЬТУРА

РЕШЕНИЯ

КРОССВОРД

КАЛЕНДАРЬ



От редактора

Основой этого выпуска стали авторские статьи ведущих экспертов в сфере информационной безопасности.

Екатерина Данилова, менеджер по развитию бизнеса Kaspersky Fraud Prevention расскажет, каким будет 2020 год для компаний с онлайн-сервисами в разрезе кибермошенничества.

Консультант ООН по вопросам информационной безопасности Владимир Безмалый поведает о сервисах Google и Privacy, проблемах умного телевизора, взломах и многом другом.

В интервью с Алексеем Новиковым, директором экспертного центра безопасности Positive Technologies, узнаем, так ли страшен APT, как это считается.

В обзорной статье о грядущих «горячих» технологиях своими мнениями поделятся российские ИТ-эксперты.

Редакция CIS поведает об исключительном месте – МГТУ имени Н.Э. Баумана, в котором побывала на экскурсии по приглашению доцента кафедры «Информационная Безопасность» Анатолия Лебедева.

Большое количество положительных отзывов о прошедшем конкурсе красоты «Мисс CIS» среди девушек, работающих в ИТ-сфере, уверило нас о необходимости продолжить двигаться в этом интересном направлении. Поэтому мы открываем приём заявок на новый конкурс. Теперь к нам присоединился Клуб IT&Digital-директоров «я-ИТ-ы» – руководители крупнейших предприятий и организаций различных отраслей экономики. Сайт конкурса www.cismiss.ru.

Продолжая добрую традицию, журнал организовывает благотворительную ИТ-конференцию CISummIT Digital Hearts, чтобы собрать средства для помощи детям. Это мероприятие организовано CIS в поддержку Фонда Константина Хабенского. В прошлый раз нам удалось помочь 8 подопечным фонда: 5-ти мальчикам и 3-м отважным девочкам. Будем рады видеть вас на мероприятии, где вы сможете оказать помощь и другим детям, которые в этом нуждаются. Подробности на сайте www.cisevent.ru.

С уважением,
редакция журнала CIS.

Главный редактор: Станислав Понарин.

Фотограф, руководитель интернет-маркетинга: Нина Жиленкова, n.zhilenkova@sovinfosystems.ru.

Корректор: Оксана Макаренко.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Сайт: www.cismag.ru, интернер-блог: www.cismag.news.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77-69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

Адрес редакции: 22-й км Киевского ш., (п. Московский), домовладение 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

Фото на обложке: Екатерина Данилова.

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

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.

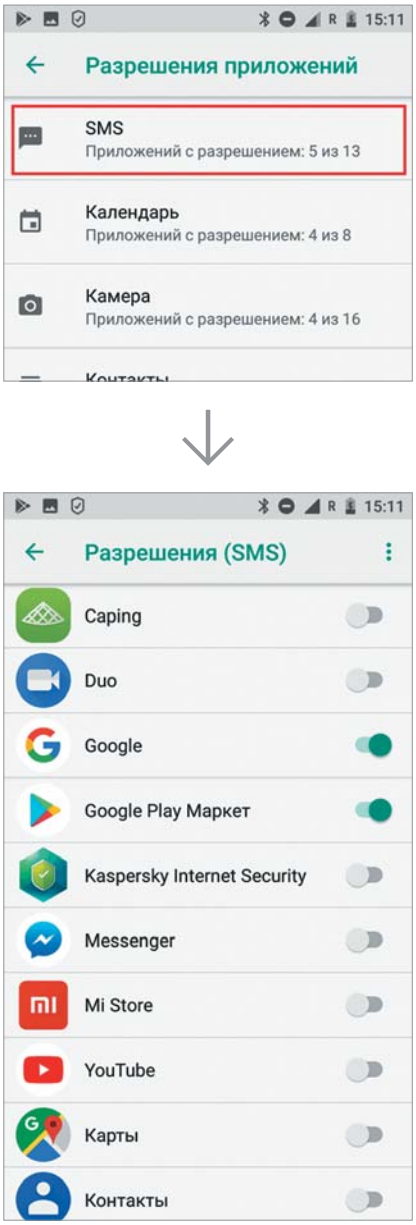


Рисунок 3. Разрешения приложений SMS

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)

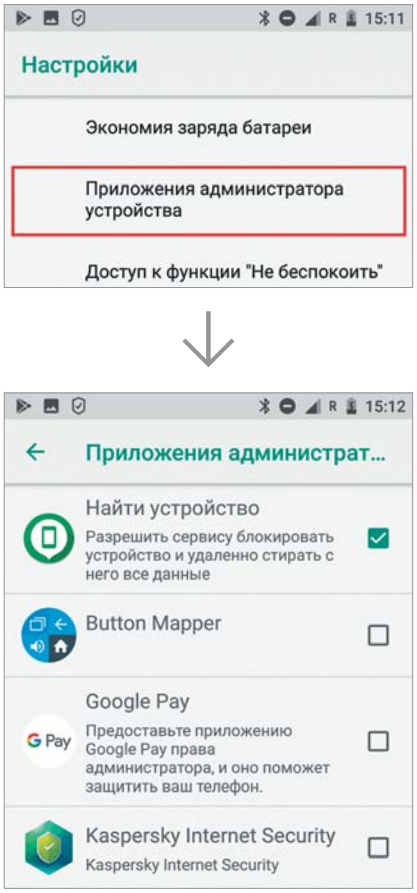


Рисунок 4. Приложения администратора устройства

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).

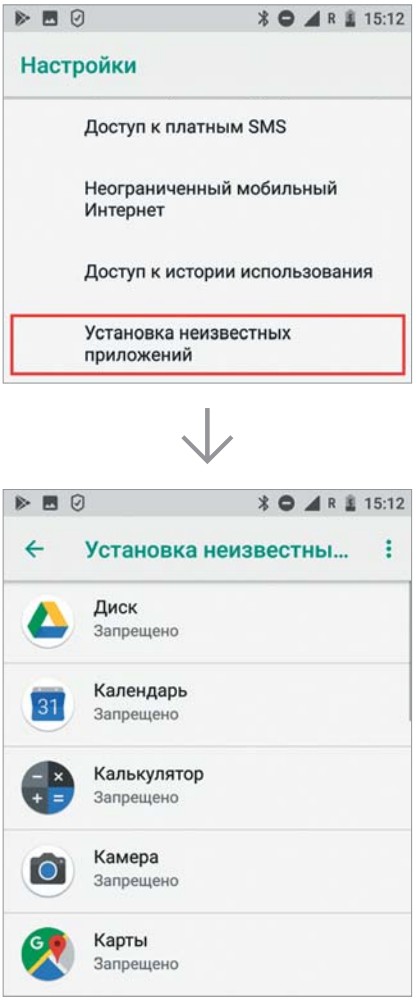


Рисунок 5. Установка неизвестных приложений

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)

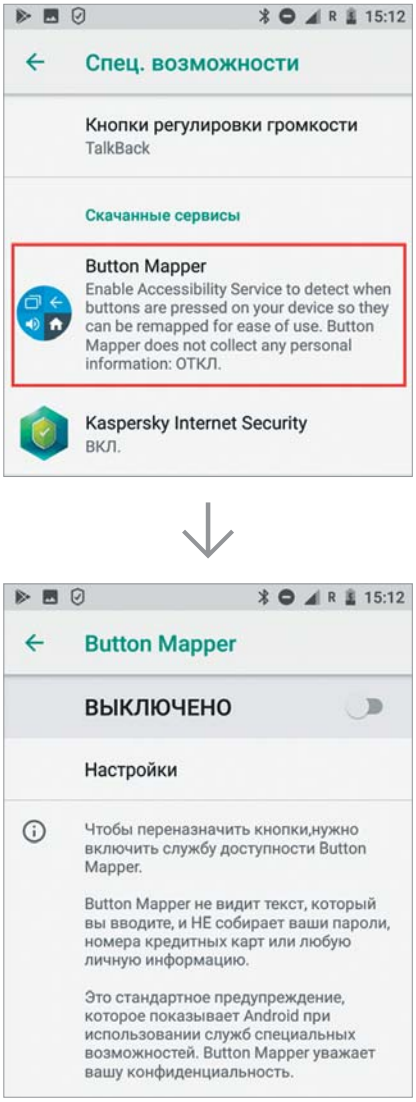


Рисунок 6. Специальные возможности

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.

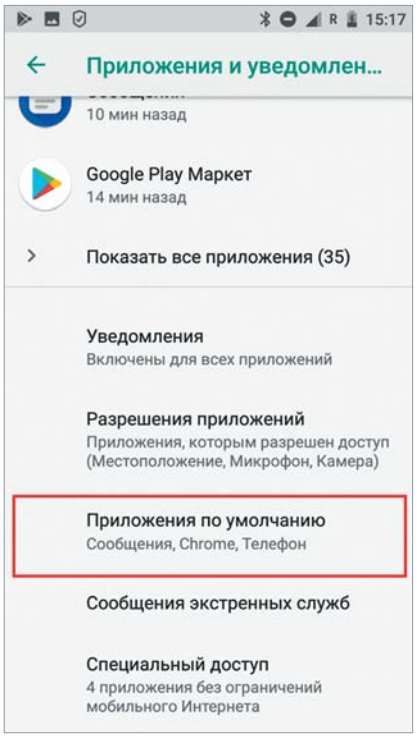
Заметим, что этот трюк уже успешно освоен большинством банковских троянов и используется киберпреступниками на постоянной основе. Неприятных сценариев с использованием приложений по умолчанию гораздо больше. Поэтому стоит обстоятельно подумать, перед тем как разрешить приложению стать «по умолчанию».

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



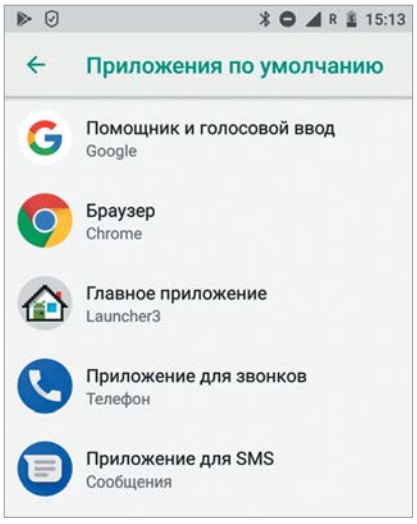


Рисунок 7. Приложения по умолчанию

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).

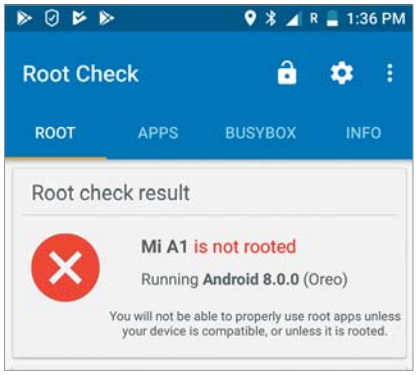


Рисунок 8. Проверка root – красный цвет сообщений означает, что права суперпользователя на этом смартфоне не получены

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:

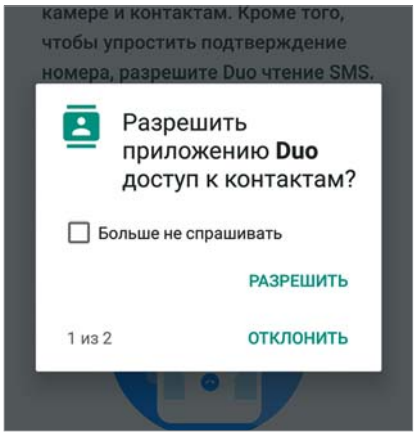


Рисунок 9. Разрешить приложению доступ к контактам

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).

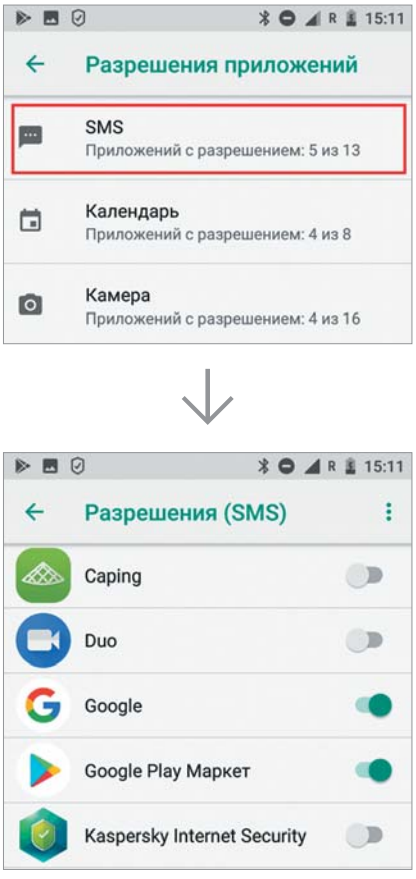


Рисунок 10. Разрешение приложений

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).

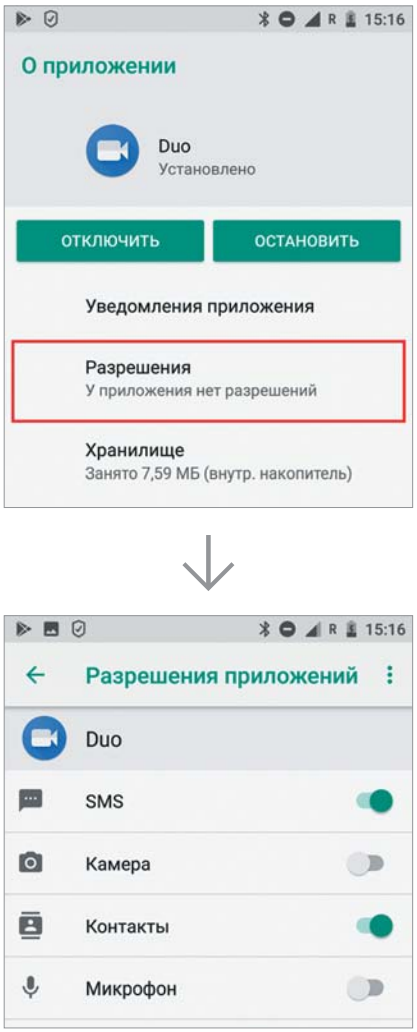


Рисунок 11. Разрешения

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

Вы собрались в дорогу

Как ни странно прозвучит, но очень часто в ходе путешествия (особенно если вам приходится долго ждать ваш вылет, а он всё откладывается) у вас садится телефон. Увы, батареи не резиновые, а в случае, если вам приходится долго ждать и нечем заняться, заряд смартфона расходуется особенно интенсивно.

Книга, фильм, интернет-сёрфинг, звонки домой, да мало ли чем вы будете заниматься. Результат, увы, один – батарея интенсивно расходуется и рано или поздно вам придётся её заряжать. Вам на помощь придут зарядные станции, расположенные в месте ожидания (аэропорт, вокзал, остановка общественного транспорта, трамвай, лавочка в городском парке). Мало ли, вдруг вы забыли PowerBank или не взяли с собой зарядку, а у вас есть только USB-кабель. И вы отправляетесь к ближайшей USB-зарядной станции. Верно?

А задумывались ли вы о том, что такие станции – потенциальная угроза для вашего смартфона. Ведь кто знает, что установлено на той стороне? Поэтому подумайте дважды, прежде чем подключаться в аэропорту (на вокзале) или в поезде (автобусе).

Ведь существует опасность заражения вашего смартфона через USB с помощью атаки Juice Jacking. Данная атака происходит, когда ничего не подозревающие пользователи подключают свои электронные

устройства к USB-портам или используют USB-кабели, которые уже заражены вредоносными программами.

Затем вредоносное ПО заражает устройства, предоставляя хакерам доступ к ним. Они могут читать и экспортировать ваши данные, включая пароли, и даже блокировать гаджеты, что делает их непригодными для использования.

По словам Ливиу Арсена, эксперта по кибербезопасности в BitDefender румынской компании по кибербезопасности и антивирусному программному обеспечению, в подобной атаке используется такой недостаток наших мобильных устройств, как периодический разряд батареи.

Мистер Арсен предостерегает от использования USB-кабелей, которые уже подключены к зарядным станциям или даже выданы в качестве рекламных подарков.

Что можно противопоставить данной атаке? Ношение собственных зарядных проводов, зарядку только напрямую от электрической розетки и использование портативных аккумуляторов, которые были приобретены у известных поставщиков.

Однако стоит учесть, что, помимо кабелей, опасность могут представлять и сами USB-порты, используемые для зарядки.

Хакеры могут легко вырывать USB-порты и заменять их собственным вредоносным оборудованием, – говорит Вьяс Секар, профессор CyLab, специалист по безопасности исследовательского института в Университете Карнеги-Меллона.

«Легко изменить розетку, если у злоумышленника есть физический доступ», – сказал профессор Секар.

Хотя г-н Арсен и профессор Секар выразили неуверенность в том, как часто происходят подобные хакерские атаки, растущая распространённость USB-портов для зарядки в таких местах, как отели, аэропорты и общественный транспорт, привела к увеличению риска стать жертвой кибермошенников.

«Люди хотят удобно заряжать свои телефоны и планшеты, где бы они не находились», – сказал профессор Секар и добавил: «Очевидно, я бы тоже этого хотел, но есть риск».

Профессор Секар, что потребители могут также использовать присоединяемые защитные устройства на кабелях USB, которые называются «USB-презервативы».

«То, что они делают, – очень простой трюк», – отметил он. – Они отключают вывод данных на зарядном устройстве USB».

Это означает, что устройство будет заряжаться, но кабель не сможет отправлять или получать данные.

Насколько реальна атака Juice Jacking?

Технически подобная атака реальна, однако широкого распространения не получила. Вместе с тем окружная прокуратура Лос-Анджелеса в ноябре 2019 года выпустила рекомендацию для путешественников, предупреждая их о потенциальной опасности использования общедоступных портов USB.

Что правда в этом случае?

Увы, подобная атака вполне реальна.

Что ложно?

Хотя для мошенников технически возможно украсть информацию или установить вредоносное ПО через общедоступные USB-порты, эта практика, по-видимому, не получила широкого распространения.

Что делать?

Самая эффективная мера предосторожности – просто **не заряжать телефон с помощью сторонней системы.** Вот несколько советов, которые помогут вам избежать использования общедоступного зарядного устройства для киосков:

- **Держите аккумулятор полностью заряженным.** Возьмите за правило заряжать телефон дома и в офисе, когда вы не пользуетесь им активно или просто сидите за рабочим столом. Когда возникают непредвиденные обстоятельства или вы застряли на улице, в вашем телефоне есть заряд.
- **Носите с собой личное зарядное устройство.** Зарядные устройства стали очень маленькими и портативными: от USB-кабелей до банков питания. Всегда имейте его в своей сумке, чтобы вы могли безопасно заряжать телефон от электрической розетки или в дороге, используя аккумулятор.
- **Если возможно, возьмите с собой резервную батарею.** Если вы не хотите брать с собой запасное зарядное устройство или блок питания, вы можете взять запасную батарею, если в вашем устройстве есть съёмная батарея или батарейный отсек (чехол для телефона, который удваивается как батарея).
- **Заблокируйте свой телефон.** Без правильного PIN-кода, сканирования отпечатков пальцев или идентификации лица ваш телефон не может быть сопряжён с устройством, к которому он подключён.
- **Используйте только USB-кабели питания (USB-презерватив).** В этих кабелях отсутствуют два провода, необходимые для передачи данных, и только два провода для передачи энергии. Они будут заряжать ваше устройство, но передача данных при этом невозможна.
- **Технологические угрозы вокруг нас.** Даже мельчайшие детали, такие как зарядка телефона от зарядного устройства для киосков, могут повлиять на безопасность вашего устройства.
- **Используйте только свой оригинальный зарядный кабель.**

Ведь USB-кабель может подавать питание на устройство, но его также можно использовать для передачи данных. Хотя это может быть очевидно при подключении телефона к другому устройству (например, ноутбуку), данные могут быть не первыми, о чём вы задумываетесь, когда подключаете свой телефон к настенной USB-розетке. Но эксперты по безопасности (и, возможно, преступники) разработали способы превращения этих розеток в порты передачи данных.

Следует также отметить, что как Android, так и iOS имеют встроенные функции, чтобы предотвратить подобную атаку, так как эта угроза безопасности впервые появилась примерно в 2011 году. На большинстве современных телефонов пользователи теперь будут видеть всплывающее предупреждение, если они используют порт USB, который способен передавать данные, а не только питание.

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

CIS / № 1 (11) / 2020 / www.cismag.ru

Проблемы умного телевизора

Весьма возможно, что вы используете умный телевизор. Тем более, что таких сегодня большинство. Однако проблема в том, что умный телевизор записывает ваши привычки: что вы смотрите, когда, а затем компания-разработчик монетизирует эти знания. Увы, проблема в том, что технологии производства сегодняшних телевизоров уже практически не развиваются, а, следовательно, ждать прорыва уже неоткуда.

Снижать бесконечно цены, чтобы победить конкурентов, уже тоже практически невозможно. А ведь прибыль получать хочется всем. И потому на помощь компаниям, выпускающим телевизоры, приходит идея очень тихо зарабатывать на своих покупателях, вернее, на их данных.

ACR: всё связано

Наверное, у нас с вами не было бы такой угрожающей ситуации, если бы не автоматическое распознавание контента (Automatic Content Recognition – ACR). Эта функция Smart TV использует всего несколько пикселей того изображения, которое вы просматриваете в данный момент. Затем эти сведения используются для показа рекламы как внутри вашего телевизора, так и на других ваших интернет-устройствах. Так как ваш смарт-телевизор, вероятно, связан с вашим домашним маршрутизатором, он использует тот же IP-адрес, который идентифицирует ваши конкретные домашние устройства. Этот общий адрес означает, что вы можете использовать рекламу, полученную с помощью вашего телевизионного устройства на все устройства, подключённые к домашней сети. Другими словами, та же реклама, которую вы видели на своём телевизоре Smart TV, может легко появиться на вашем смартфоне.

Возможно, это звучит особенно страшно, потому что телевидение предшествовало Интернету, и люди помнят время, когда просмотр телевизора казался скорее однонаправленным распространением информации. Но времена изменились, и сегодня телевизор уже не только даёт информацию, но и фильтрует её, чтобы вы получали направленную рекламу.

Почему данные ACR могут стать будущим телевизионных измерений

Данные ACR (автоматического распознавания контента) со смарт-телевизоров могут быть одним из самых революционных способов для сетей и рекламодателей измерить привычки просмотра. Это также одна из наименее изученных технологий в телевизионной экосистеме.

Настройка

Весь процесс ACR запускается, когда зритель впервые распаковывает свой телевизор. Когда вы его устанавливаете, появляется экран с вопросом, хотите ли вы поделиться тем, что смотрите. Очень часто этот вопрос формулируется в терминах: «Чтобы получить более точные рекомендации, вы позволите нам отслеживать то, что вы смотрите?» При этом вас не уведомляют о своих намерениях (например, о продаже данных маркетологам и фирмам, которые проводят измерения), но реальность такова, что независимо от того, насколько они искренни, большинство людей просто спешат настроить телевизор и потому на все вопросы просто отвечают «Да», не читая их (безусловно, хорошая новость заключается в том, что вы можете вернуться и изменить свои ответы, если у вас появятся подобные мысли). Но большинство людей, считает абсолютно нормальным, когда маркетологи знают, какие телевизионные шоу они смотрят.

После того как владелец телевизора дал разрешение и подключил

телевизор к Интернету, у него всё впереди: производитель смарт-телевизора может собирать эти данные и использовать их по своему усмотрению.

Сбор данных

На технологическом уровне данные ACR работают, потому что умные телевизоры (с вашего разрешения) захватывают несколько пикселей из того, что зритель в данный момент смотрит, и обмениваются ими с программным обеспечением отслеживания ACR производителя телевизора. Программное обеспечение берёт эти пиксели и сопоставляет их с базой данных, которая отслеживает локальные трансляции в любом регионе, в котором находится зритель. Посмотрев время, продолжительность рекламных пауз и какие рекламные ролики просматриваются, провайдер данных ACR может узнать несколько вещей:

1. Зритель смотрит линейный канал, OTT, DVR или VOD?
2. Какие шоу и рекламные ролики он смотрит каждую секунду.
3. Каков IP-адрес зрителя, что позволит ему узнать свой физический адрес и какие веб-сайты и приложения он посещает (все эти данные анонимны, например: фактические имена не прилагаются). Но прилагается IP-адрес.

Рынок

Зайдите в любой магазин: почти каждый телевизор, который вы увидите, будет умным или подключённым к Интернету. По оценкам, к 2020 году около 75% всех телевизоров, используемых в США, будут умными телевизорами.

Одно существенное изменение с момента запуска умных телевизоров заключается в том, что две компании – Samsung и VIZIO – стали доминировать на рынке. Несмотря на то, что нет конкретной статистики, по большинству оценок Samsung занимает около 40% рынка, а VIZIO – 30%. Такие игроки, как LG, Sony, Panasonic, Magnavox, Philips и тому подобное теперь занимают гораздо меньшую долю рынка, чем пятнадцать или двадцать лет назад. Новые игроки из Китая, такие как Huawei, являются восходящими, но, за исключением Samsung и VIZIO, никто не владеет более чем 10% рынка.

Samsung и VIZIO собирают данные со смарт-телевизоров, но в то время как Samsung использует эти данные только в своих целях (рекомендации и реклама на домашнем экране), VIZIO владеет компанией Inscape, которая продаёт необработанные данные для маркетологов, сетей и измерительных компаний. Другая компания – Samba TV объединяет несколько небольших OEM-производителей и предлагает агентствам возможность переориентировать потребителей.

Значение данных ACR

Данные ACR от умных телевизоров – единственный способ измерить уровень того, что смотрят люди. Это означает, что засчитано будет всё независимо от источника сигнала. Что, учитывая нынешнюю суету вокруг того, как именно измерить зрительскую аудиторию, кажется крайне необходимым для отрасли.

Представьте себе: идёт политическая реклама. Как посчитать хотя бы приблизительно, как будут голосовать? Довольно просто: зная, какую рекламу смотрят, а какую нет, верно?

Рекламодателям нравятся данные ACR, потому что они обеспечивают каждую секунду обратную связь, как работают их объявления. Nielsen предоставляет свои данные в 15-минутных блоках, поэтому, если зрители отключились после первого объявления в пакете, рекламодатель не сможет узнать об этом. А поскольку IP-адреса включены, такие компании, как iSpot.tv и Data + Math, могут использовать эту информацию для создания атрибутивных рейтингов, которые помогают рекламодателям понять, как определённые объявления и места размещения помогли зрителям пройти через воронку продаж от просмотра рекламы, чтобы погуглить продукт, чтобы фактически купить его. Это длительный процесс, который требует большого количества данных и строгости, но это отличный способ доказать маркетологам, что телевизионная реклама действительно работает.

Будущее измерения ACR

Ценность данных ACR будет продолжать расти: к 2021 году она должна превратиться в бизнес стоимостью 5 миллиардов долларов, поскольку сети и рекламодатели используют её, чтобы помочь определить, кто просматривает широкий спектр форматов и вариантов. Данные ACR не вытеснят данные Nielsen, а, скорее, дополнят их вместе с данными телевизионных приставок (от тех, кто всё ещё использует таковые). Взятые вместе, они должны дать нам гораздо лучшее понимание шаблонов просмотра, что, в свою очередь, позволит рекламодателям лучше ориентировать рекламу на определённую аудиторию в зависимости от того, когда, где и на каком устройстве они смотрят. Всё это должно помочь отрасли получить доступ к святому Граалю меньшего количества более целенаправленной рекламы, за которую бренды будут платить больше денег.

На подключённом к Интернету Smart TV этот собранный контент не ограничивается цифровой информацией из передач, которые вы транслируете через интернет-сервисы, такие как Netflix, но также может включать пиксельные подписи с обычного кабельного телевидения и DVD-дисков. И эта информация может передаваться с вашего телевизора компаниям каждые несколько секунд [1].

Опасения по поводу наблюдения

Сегодня даже ФБР озабочено данной проблемой и предостерегает пользователей о необходимости защищать свои умные телевизоры [2]. Однако, как выясняется, текущая бизнес-модель добычи данных, которую используют многие технологические компании, также порадует государственные силовые структуры.

Вместе с тем необходимо учесть, что сегодня, как в ноутбуках и смартфонах, в некоторых смарт-телевизорах есть микрофоны и камеры, хотя, как сообщается, в новых моделях камеры стали меньше [3]. Фактически эти камеры и микрофоны – всё та же проблема «подслушки-подглядки». Это превращает телевизоры в универсальные подслушивающие-подглядывающие устройства. И хотя правоохранительные органы будут предостерегать вас от атак злоумышленников, кто мешает самим правоохранителям вторгаться в вашу личную жизнь? Ведь наблюдение возможно даже тогда, ког-

да вам кажется, что ваш телевизор выключен [4].

Угрозы Smart TV

Вместе со сбором рекламных данных смарт-телевизоры представляют и другие проблемы безопасности, такие как возможность атак злоумышленников для проникновения в домашние настройки Wi-Fi и проникновения на другие устройства в вашей сети. Ведь вполне вероятно, что даже если ваш компьютер хорошо защищён, то незащищённый телевизор может дать возможность проникновения в маршрутизатор или сеть [2].

Несмотря на то, что ФБР напрямую не предупреждает о ботнет, следует отметить, что Internet of Things (IoT), такие как смарт-телевизоры, являются популярными объектами для атак. Тем более, что телевизор служит своему хозяину не год и не два. А обновления к его прошивке практически не выпускаются.

«Многие кибератаки, такие как вредоносное ПО Mirai и атаки Dyn, заражают сеть компьютеров, включая интеллектуальные устройства, такие как бытовые приборы, камеры видеонаблюдения, радионяни, системы кондиционирования / обогрева, телевизоры и т. д., и превращают их все в скомпрометированные серверы, – пишет Алан Грау, вице-президент IoT по встраиваемым решениям в Sectigo [6]. – Эти скомпрометированные серверы затем действуют как узлы в атаке и вместе создают ботнет. Они могут участвовать в различных скоординированных атаках, заражать другие устройства и расширять сеть ботов или участвовать в атаках типа «отказ в обслуживании».

ФБР предупредило о потенциальном риске того, что Smart TV может слушать вас и наблюдать за вами, отметив, что новые телевизоры со встроенными камерами позволяют вести видеочаты. Кроме того, некоторые модели имеют функцию распознавания лиц, «поэтому телевизор знает, кто смотрит, и может предложить соответствующие программы», – говорится в уведомлении, что также может привести к проблемам с конфиденциальностью.

Увы, это не теория. Недавно исследователи обнаружили, что умные телевизоры от Samsung, LG и других компаний отправляют конфиденциальные пользовательские данные в технологические фирмы-партнёры, даже когда устройства не работают [7].

На сегодняшний день уже обнаружены несколько уязвимостей в смарт-телевизорах. А производители Smart TV, как и многих других устройств IoT, не следуют принципам обеспечения безопасности.

По словам ФБР, чтобы защитить себя от всех этих угроз, потребители должны изменить стандартные настройки и пароли безопасности интеллектуальных телевизоров и знать, как отключить микрофоны, камеры и сбор личной информации, если это возможно. Кроме того, необходимо регулярно проверять наличие обновлений программного обеспечения от производителей.

Наши устройства стали умными (возможно, слишком умными), но это не значит, что вы должны быть «тупыми» в том, как их использовать. В следующий раз, когда вы настроите новое интеллектуальное устройство, обязательно подумайте о его возможностях и о том, что можете сделать, чтобы защитить свою конфиденциальность.

Как вы можете защитить свой умный телевизор?

В 2018 году по всему миру было продано 114 миллионов умных телевизоров [5]. В Соединённых Штатах около 45% домов имели хотя бы один умный телевизор. И одна из причин, по которой умные телевизоры стали такими доступными, заключается в том, что возможности отслеживания помогают удерживать цены. Поскольку умные телевизоры и другие интеллектуальные устройства становятся всё более привлекательными для покупки, важно, чтобы рядовой пользователь знал, как ограничить сбор данных на своих машинах.

4. Будьте осторожны при настройке телевизора. Не соглашайтесь автоматически на все условия, чтобы не упустить возможность отказаться от сбора данных. Если вы читаете это до того, как начнёте работать с новым умным телевизором, то подумайте, что вам по вкусу, потому что производители усложняют поиск и отказ от своих функций сбора контента после того, как вы уже согласились с ними. Способ изменения настроек варьируется для каждого телевизора, поэтому вам нужно будет найти спецификации для вашей собственной модели.
5. Вы можете просто выбрать «тупой» вариант и не подключать свой умный телевизор онлайн. Затем вы можете, например, запустить любимый потоковый сервис со своего ноутбука и подключить его к порту HDMI телевизора. Конечно, вы всё равно будете подвергаться врождённому отслеживанию, которое происходит в потоковом сервисе, который используете, но несколько ограничите его распространение.

Если хотите, чтобы телевизор работал в режиме реального времени, вам может помочь VPN. Защита вашего домашнего маршрутизатора с помощью VPN – это отличный способ зашифровать соединение, которое защитит вас от хакеров и повысит анонимность в сети. Вместе с тем нужно помнить, что от «подслушки-подглядки» это не защитит! Безусловно, это усложнит анализ, но не сильно. Да и практически все крупные компании с сервисами ведут у себя логи. Кроме того, стоит помнить, что в ряде стран есть только «доверенные» VPN, которые сдали ключи соответствующим ведомствам.

Поскольку телевизоры относятся к устройствам IoT, они обновляются редко или вообще не получают обновлений. А значит, на сетевом уровне их нужно выделять в отдельную подсеть и отделять от компьютеров. В условиях организации – обязательно, в домашних условиях – желательно. Между подсетями должен быть разрешён только одобренный трафик. Либо подключать телевизор и компьютеры к разным роутерам. Это вполне реально, например: у меня дома есть подключения к двум интернет-провайдерам и установлены два роутера. Далее на телевизорах под управлением Ос Android можно рекомендовать установку специализированных антивирусов, например Eset Smart TV Security.

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

Вас взломали? Проверьте!

В наше время одной из наиболее распространённых проблем является компрометация паролей пользователей. Причин этого очень много. К наиболее распространённым, на мой взгляд, относятся:

- Использование простых паролей
- Использование одного и того же пароля на различных интернет-ресурсах
- Использование бесплатных Wi-Fi

На самом деле, причин намного больше, но результат один и тот же. Как быть? Что можно этому противопоставить?

На мой взгляд, помочь в решении этой проблемы может следующее:

- Использование менеджеров паролей (при этом вам не нужно помнить все пароли, достаточно не забывать мастер-пароль, который, естественно, должен быть сложным)
- Использование различных сервисов для проверки утечки паролей, связанных с вашей учётной записью, с целью своевременной смены пароля
- Использование многофакторной аутентификации

Мало того, стоит учесть, что основной источник утёкших паролей – это взлом форумов через различные уязвимости. Увы, форумы взламывают, извлекают оттуда хеши паролей и затем ломают их с помощью hashcat.

Hashcat

Hashcat – это, по словам создателей, самый быстрый в мире инструмент для восстановления паролей.

Стоит учесть, что это кроссплатформенное программное обеспечение, которое работает как под Windows так и под Linux. Для работы нжны драйвера. Вместе с тем она полностью бесплатна и имеет открытый исходный код.

Официальный сайт: hashcat.net/hashcat

Одновременно использует как ресурсы видеокарты, так и центрального процессора, поддерживает огромное количество алгоритмов, в том числе умеет восстанавливать пароли Wi-Fi. Взлом осуществляется как по словарю и маске, так и с помощью brute force.

Поддерживает работу с такими алгоритмами хэширования: md5, md5crypt, sha1, sha2, sha256, md4, mysql, sha512, wpa, wpa2, grub2, android, sha256crypt, drupal7, scrypt, django и другими.

Драйверы для hashcat

Необходимы следующие драйвера для видеокарт:

- Видеокарты AMD на Windows требуют «AMD Radeon Software Crimson Edition» (15.12 или более поздняя версия)
- Intel CPUs требует «OpenCL Runtime for Intel Core and Intel Xeon Processors» (16.1.1 или более поздняя версия)
- Intel GPUs на Windows требует «OpenCL Driver for Intel Iris and Intel HD Graphics»
- Видеокарты NVIDIA требуют «NVIDIA Driver» (367. x или более поздняя версия)

На данный момент hashcat доступен для macOS, Windows и Linux с GPU, CPU и общей поддержкой OpenCL, что позволяет использовать FPGA и другие ускорительные карты.

Принцип работы

Принцип работы всех программ, позволяющих взламывать пароли, практически одинаковый. Утилиты различаются разве что скоростью перебора паролей, в них могут быть реализованы и разные алгоритмы атак. Основная идея состоит в том, чтобы по заранее заданному подмножеству букв/слов (так называемый словарь) осуществлять быстрый перебор комбинаций. От каждой комбинации вычисляется хеш и сравнивается с оригинальным. В случае совпадения пароль считается взломанным. В случае с Hashcat подбор рекомендуется производить на GPU, так как графический процессор способен перебирать комбинации значительно быстрее.

Типы атак

Hashcat предполагает использование различных типов атак для достижения эффективного покрытия всевозможных хешей:

- Атака «грубой силой» (Brute-force attack)
- Атака по маске (Mask attack)
  - Считается самой эффективной на данный момент. Идея состоит в том, чтобы с помощью частотного словаря (наиболее употребляемые пароли) построить маску и тем самым сократить количество комбинаций
  - Например, достаточно стандартной являются комбинации с заглавной первой буквой и цифрами на конце (Julia1983). В случае обычного перебора это заняло бы чуть более чем 4 года на обычной для современного GPU скорости (100 Мега-хешей в секунду)
  - Используя стандартную для многих людей маску (заглавная буква в начале и год в конце), подобный пароль можно было бы подобрать. Это заняло бы около 40 минут на той же скорости GPU
- Атака перебором всех комбинаций в словаре (Combinator attack)
- Простой перебор по словарю (Dictionary attack)
- Атака по следу (Fingerprint attack)
- Гибридная атака (Hybrid attack)
- Атака перемешиванием (Permutation attack)
- Атака на основе правила (Rule-based attack)
- Атака поиском по таблице (Table-lookup attack), только на CPU
- Атака перебором по заглавным и прописным буквам (Toggle-Case attack)

Традиционная атака «Грубой силой» считается устаревшей, поэтому команда Hashcat рекомендует использовать атаку по маске в качестве полной замены.

Стоит признать, что пароли, увы, могут быть какими угодно стойкими. Но потом они утекают не от пользователей.

Именно об этом я и хотел бы поговорить в этой статье.

Сервисы проверки утечек

Рассмотрим несколько возможностей проверки, не числится ли ваш пароль в списке утечек.

Сервис haveibeenpwned.com

Данный сервис предназначен для того, чтобы пользователи могли проверить свой адрес e-mail на утечку паролей.

Он содержит данные 124684519 учётных записей. Следует учесть, что вы можете заказать уведомление, если ваш e-mail появится в базах данного сервиса.

На вкладке haveibeenpwned.com/Passwords вы можете проверить свой пароль на утечку. База данных Pwned Passwords – это 555278657 реальных паролей, ранее обнаруженных при взломе данных. Они доступны для поиска в Интернете, а также

могут быть загружены для использования в других онлайн-системах.

Сервис Pwned Passwords был создан в августе 2017 года после того, как NIST выпустил руководство, в котором, в частности, рекомендуется проверять предоставленные пользователем пароли на наличие существующих нарушений данных. Обоснование этого совета и предложений о том, как приложения могут использовать эти данные, подробно описано в блоге под названием Introducing 306 Million Freely Downloadable Pwned Passwords.

В феврале 2018 года была выпущена вторая версия сервиса, содержащая более чем полмиллиарда паролей, при этом каждый из которых также подсчитывал, сколько раз они употреблялись. Выпуск третьей версии в июле 2018 года представил ещё 16 миллионов паролей, четвёртая версия вышла в январе 2019 года. Наряду с утечкой данных «Сбор №1» общее количество паролей превысило 551 млн. Наконец, пятая версия вышла в июле 2019 года с ещё 30 миллионами паролей. Итого общее количество записей составило почти 555 миллионов.

Сервис от Google

Сегодня вы можете проверить, не оказались ли пароли, которые сохранены в вашем аккаунте Google, в руках злоумышленников. Для этого достаточно зайти в диспетчер паролей – он сопоставит ваши данные с базой всех крупных утечек.

Информацию об утечках Google собирает сама. В основном данные поступают из открытых источников, но иногда компания находит украденные пароли на просторах «тёмного интернета».

Если Google обнаружит, что какие-то ваши пароли ранее попали в открытый доступ, то предложит их сменить. Также сервис сообщит, если вы используете один и тот же пароль на большом количестве сайтов. Диспетчер предупредит и о слишком слабых паролях, которые легко угадать.

Удобно? Безусловно! Безопасно? Не думаю.

Как это работает?

Конечно, вы знаете, что у Google довольно давно есть менеджер паролей, который синхронизируется между Chrome и Android. В этот менеджер компания добавляет функцию «проверки пароля», которая проанализирует ваши логины, чтобы убедиться, что они не были частью серьёзного нарушения безопасности, ведь на сегодня подобных утечек очень и очень много.

Ранее проверка пароля уже была доступна в качестве расширения, но сейчас Google встраивает её прямо в элементы управления учётной записью Google. Проверить ваши пароли вы можете на сайте passwords.google.com, который является ярлыком URL для менеджера паролей Google.

Ваши учётные данные сравниваются с миллионами миллионов скомпрометированных учётных записей, которые были частью серьёзных нарушений. Google говорит, что он также в некоторой степени контролирует «тёмную сеть» для сбора паролей, но большая часть базы данных, с которой сравнивается проверка паролей, происходит от сканирования открытой сети.

Стоит понимать, что у Google это ни в коем случае не единственный сервис, который делает подобные проверки. В эпоху постоянных утечек и нарушений безопасности в крупных компаниях, затронувших десятки, а может, и сотни миллионов клиентов, таким полезным ресурсом оказался haveibeenpwned.com.

Если ваш пароль скомпрометирован или оказался слишком простым, Google предложит изменить соответствующий пароль. То же самое касается, если Google видит, что вы повторно используете пароли, что является неверной практикой, ведь все сервисы должны иметь уникальный логин-пароль. И, конечно же, Google также будет уведомлять вас об учётных записях с использованием слабых паролей, которые легко угадываются. При этом нужно учесть, что пароли хешировались и шифровались перед отправкой в Google.

Поскольку проверка пароля основывается на отправке вашей конфиденциальной информации в Google, компания стремится подчеркнуть, что данные зашифрованы и даже она не может просмотреть их. Пароли в базе данных хранятся в хешированном и зашифрованном виде, и любое предупреждение о ваших данных полностью локально для конкретного компьютера.

Марк Ришер, директор Google по безопасности учётных записей, обратил внимание на то, что потребителей всё чаще просят хранить свои пароли в нескольких местах одновременно. У Apple есть iCloud Keychain, у Google – менеджер паролей. А кроме того, есть другие сторонние менеджеры паролей. Что делать? Выбрать менеджер и придерживаться его в дальнейшем? Или попытаться синхронизировать несколько менеджеров паролей? Вероятность несоответствия или наличия старого неправильного пароля в одном из этих мест довольно высока. На самом деле, нет достойного ответа на этот вопрос.

Согласно опросу Harris Poll, посвящённому проверке привычек пользователей в использовании паролей в США, результаты весьма тревожны. Слишком многие всё ещё включают в пароли предметы, которые незнакомец может легко узнать, например: день рождения, имя питомца и т.д. И мало кто говорит о преимуществах дополнительных мер безопасности, таких как двухфакторная аутентификация (её используют только 37% респондентов) и менеджеров паролей (15%).

66% опрошенных заявили, что используют один и тот же пароль для нескольких учётных записей в Интернете.

Повторное использование пароля – это главная привычка, которую Google пытается сломать, потому что использование одного и того же пароля для нескольких служб может поставить вас в опасное положение, если хотя бы один из сервисов будет скомпрометирован. Если вы не поклонник цифровых менеджеров паролей, то просто запишите их в записную книжку где-нибудь дома. Даже это более удачный вариант, поскольку не будете повторять один и тот же пароль.

Почему я не буду использовать этот сервис

Прежде всего, потому что это привязывает к браузеру от Google, а меня это не устраивает. Увы, но использовать Google Chrome в корпоративной среде, с моей точки зрения, дурная затея. Почему?

Как я думаю, данный сервис в первую очередь предназначен для персональных пользователей. И тут есть ряд вопросов.

Вместе с тем стоит отметить, что для использования Google Chrome в корпоративной среде существует особая версия – cloud.google.com/chrome-enterprise/browser/download/. Она содержит и групповые политики, и средства централизованного обновления.

Вы доверяете компании Google? Я с большим трудом. Вспомним: «Пароли хранятся в шифрованном виде». А теперь вопрос: где хранится мастер-пароль? У вас? Не думаю. Скорее всего, он хранится у специалистов Google. В любом случае достоверной информации об этом нет.

А как быть, если вы используете не только браузер Google Chrome? Например, вы используете дома Chrome, а планшет – от Apple, впрочем, как и iPhone. Тогда вам придётся устанавливать браузер от Google на все устройства.

Что посоветую я? Использовать сторонние менеджеры паролей. Благо их много. Но я бы все равно рекомендовал использовать платные версии.

Впрочем, естественно, выбирать вам.

Чуть не забыл: если вы станете запоминать пароли в Google, то потребуется уделить внимание следующему:

- Защите ПК (смартфона). Ведь любой, получивший доступ к нему, автоматически получает доступ ко всем вашим паролям
- Кроме того, стоит внедрить многофакторную аутентификацию для вашего аккаунта Google
- Помнить, что несмотря на двухфакторную аутентификацию, любой, получивший доступ к вашему ПК (смартфону), даже если вы вышли из учётной записи Google, будет нуждаться только в вашем пароле, второй фактор ему не потребуется

Firefox Monitor

Данный сервис monitor.firefox.com позволяет узнать, были ли вы частью утечки данных в Интернете. На этой же странице вы можете подписаться на мониторинг утечек с помощью аккаунта Firefox. Вы сможете отслеживать несколько адресов электронной почты.

Выводы

Проблемой в случае использования любых интернет-сервисов проверки электронных адресов на утечку в том, что вы сами пересылаете свой реальный электронный адрес. А в случае компрометации любого из этих сервисов, вы рискуете стать целью атаки направленного фишинга. Поэтому рассмотрим использование подобного сервиса в менеджере паролей на примере Kaspersky Password Manager.

Get Hacked?

Вы можете уточнить, не взломан ли ваш пароль с помощью сервиса Get Hacked? от компании Lancelot Software. Загрузить данное ПО вы можете бесплатно из Microsoft Store.

Описание

Данное приложение обнаружит, если какой-либо из ваших адресов электронной почты будет обнаружен в базах взломанных учётных записей, и немедленно сообщит вам об этом. Вооружившись этой информацией, вы можете немедленно изменить свой пароль.

Функции:

- **Простота в использовании:** всё, что нужно сделать, это ввести имя пользователя или адрес электронной почты, который вы хотите отслеживать
- **Hands-off:** фоновый мониторинг всех ваших предметов. Вы получите уведомление, если обнаружится что-то новое
- **Безопасно:** в приложении используется обширная база данных о нарушениях, созданная доверенной компанией Troy Hunt
- **Постоянно обновляется:** база данных hasibeenpwned часто обнаруживает обновления, у вас всегда будут свежие данные для сравнения
- **Конфиденциальность:** это приложение никогда не сообщит ваш адрес электронной почты или имя пользователя, оно использует его только для проверки haveibeenpwned API (который сам использует безопасный протокол HTTPS)

Kaspersky Password Manager

Проверка паролей

Ваши учётные записи подвергаются большому риску, если у них одинаковые или слабые пароли (например, qwerty или 12345), а также, если эти пароли основаны на информации, которую легко угадать или получить (например, имена родственников или даты рождения).

С Kaspersky Password Manager можно быстро проверить, насколько сложные пароли вы используете и повторяется ли один пароль в нескольких учётных записях.

Когда вы вводите пароль в онлайн-форму для регистрации или его изменения, расширение Kaspersky Password Manager отображает рекомендации, как создать сложный пароль, на основании информации о сложности вводимого вами пароля.

Проверка на скомпрометированность

Для дополнительной безопасности Kaspersky Password Manager может проверить, были ли ваши пароли взломаны или подверглись утечке с онлайн ресурсов.

Программа использует алгоритм криптографического хеширования (SHA-256) для безопасной проверки паролей на скомпрометированность. Программа высчитывает по SHA-256 контрольную сумму для каждого пароля в вашем хранилище и сравнивает их с контрольными суммами по SHA-256 в базе скомпрометированных паролей. Если контрольные суммы совпадают, программа предупреждает, что пароль является скомпрометированным и его лучше сменить.

По умолчанию проверка паролей на скомпрометированность включена.

Следует учесть, что Kaspersky Password Manager проверяет на скомпрометированность только активные записи с паролями.

Проверка на утечку с помощью канала Telegram

В данном случае мы сможем не только узнать, встречается ли наш адрес электронной почты в списке утечек, но и проверить телефон. Для этого потребуется телеграм-канал t.me/LeakCheck

Далее всё просто. Вы вводите искомый адрес электронной почты или требуемый номер телефона и получаете результат: в базах утечек он или нет. И если в базе, то сколько раз он встречается.

Однако куда большей проблемой являются корпоративные пароли. В следующем разделе мы рассмотрим обеспечение парольной защиты Azure AD для Windows Server Active Directory.

Защита паролем Azure AD для Windows Server Active Directory

Защита паролем Azure AD – это функция, которая улучшает политику паролей в организации. Локальное развёртывание защиты паролем использует как глобальные, так и пользовательские списки запрещённых паролей, которые хранятся в Azure AD. При этом выполняются те же

проверки локально, что и Azure AD для облачных изменений. Эти проверки выполняются во время смены пароля и сценариев сброса пароля.

Защита паролем Azure AD разработана с учётом следующих принципов:

- Контроллеры домена никогда не должны общаться напрямую с Интернетом
- Новые сетевые порты на контроллерах домена не открываются
- Изменения схемы Active Directory не требуются. Программное обеспечение использует существующий **контейнер** Active Directory и объекты схемы **serviceConnectionPoint**
- Отсутствуют требования по минимальным функциональным уровням леса и домена
- Программное обеспечение не создаёт и не требует учётных записей в доменах Active Directory, которые оно защищает
- Пользовательские текстовые пароли никогда не покидают контроллер домена: ни во время операций проверки пароля, ни в любое другое время
- Программное обеспечение не зависит от других функций Azure AD; например, синхронизация хэша пароля Azure AD не связана и не требуется для работы защиты паролем Azure AD

Инкрементное развёртывание

Защита паролем Azure AD поддерживает поэтапное развёртывание на контроллерах домена в домене Active Directory, но важно понимать, что это на самом деле означает.

Программное обеспечение агента DC для защиты паролем Azure AD может проверять пароли только в том случае, если оно установлено на контроллере домена, и только для изменений паролей, отправляемых на него. Невозможно контролировать, какие контроллеры домена выбираются клиентскими компьютерами Windows для обработки изменений пароля пользователя. Для обеспечения согласованного поведения и обеспечения безопасности универсальной защиты паролем программное обеспечение агента DC должно быть установлено на всех контроллерах домена в домене.

Многие организации захотят провести тщательное тестирование защиты паролем Azure AD на подмножестве своих контроллеров домена перед полным развёртыванием. Защита паролем Azure AD поддерживает частичное развёртывание, то есть программное обеспечение агента DC на данном контроллере домена будет активно проверять пароли, даже если на других контроллерах домена нет установленного программного обеспечения агента DC. Частичное развёртывание этого типа НЕ является безопасным и НЕ рекомендуется, кроме как для целей тестирования.

Архитектурная схема

Прежде чем развёртывать защиту паролем Azure AD в локальной среде Active Directory, важно понять основные концепции дизайна и функций. Следующая диаграмма показывает, как компоненты защиты паролем работают вместе (рис. 1):

- Служба прокси защиты паролем Azure AD работает на любом присоединённом к домену компьютере в текущем лесу Active Directory. Его основная цель – пересылать запросы на загрузку политики паролей с контроллеров домена в Azure AD. Затем он возвращает ответы из Azure AD на контроллер домена.
- DLL-библиотека фильтра паролей агента DC получает запросы на подтверждение пароля пользователя от операционной системы. Он перенаправляет их в службу агента DC, которая работает локально на контроллере домена.
- Служба DC Agent для защиты паролем получает запросы на проверку пароля от DLL фильтра паролей агента DC. Он обрабатывает их, используя текущую (локально доступную) политику паролей, и возвращает результат: *успешно* или *неудачно*.

Как работает защита паролем

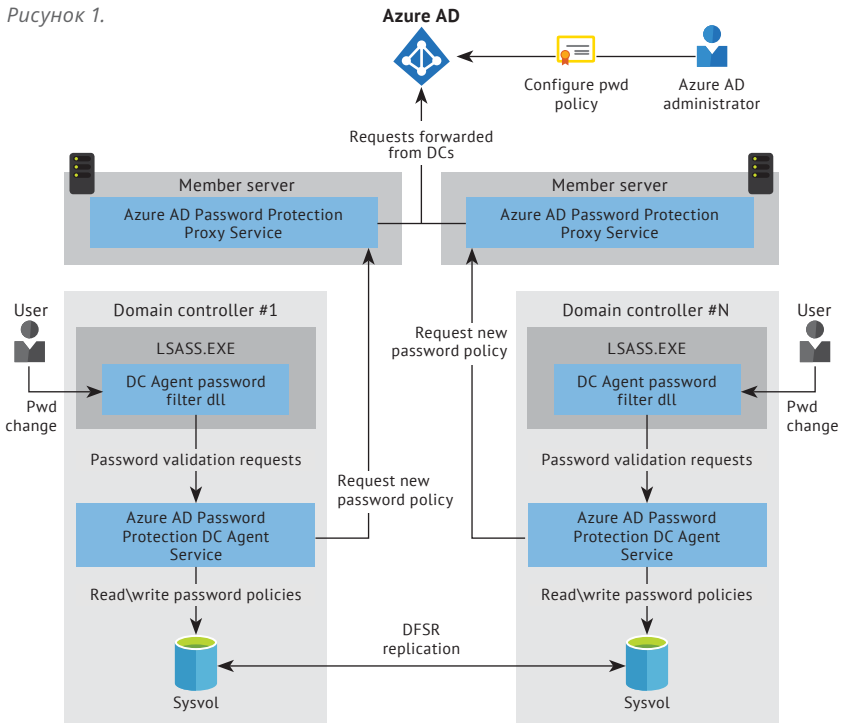
Каждый экземпляр службы прокси-сервера защиты паролей Azure AD объявляет себя на контроллерах домена в лесу, создавая объект **ServiceConnectionPoint** в Active Directory.

Каждая служба агента DC для защиты паролем также создаёт объект **ServiceConnectionPoint** в Active Directory. Этот объект используется в основном для отчётов и диагностики.

Служба агента DC отвечает за инициирование загрузки новой политики паролей из Azure AD. Первым шагом является поиск прокси-службы Azure AD Password Protection, запрашивая у леса объекты proxy **ServiceConnectionPoint**. При обнаружении доступной прокси-службы агент DC отправляет запрос на загрузку политики паролей в прокси-службу. Прокси-служба в свою очередь отправляет запрос в Azure AD. Затем прокси-служба возвращает ответ службе DC Agent.

После того как служба агента DC получает новую политику паролей от Azure AD, она сохраняет её в отдельной папке в корне *общей* папки *sysvol* своего домена. Служба агента DC также отслеживает эту папку в случае репликации новых политик из других служб агента DC в домене.

Рисунок 1.



Служба агента DC всегда запрашивает новую политику при запуске службы. После запуска службы агента DC он ежечасно проверяет возраст текущей локальной политики. Если политика старше одного часа, агент DC запрашивает новую политику у Azure AD через службу прокси, как описано ранее. Если текущая политика не старше одного часа, агент DC продолжает использовать эту политику.

Всякий раз, когда загружается политика паролей защиты паролем Azure AD, она специфична для клиента. Другими словами, политики паролей всегда являются комбинацией глобального списка запрещённых паролей Microsoft и пользовательского списка запрещённых паролей.

Агент DC связывается со службой прокси через RPC по TCP. Прокси-служба прослушивает эти вызовы на динамическом или статическом порте RPC в зависимости от конфигурации.

Агент DC никогда не прослушивает доступный по сети порт.

Прокси-сервис никогда не вызывает сервис DC Agent.

Служба прокси не имеет состояния. Он никогда не кэширует политики или любое другое состояние, загруженное из Azure.

Служба DC Agent всегда использует самую последнюю локально доступную политику паролей для оценки пароля пользователя. Если на локальном DC нет политики паролей, он принимается автоматически. Когда это происходит, регистрируется сообщение о событии, чтобы предупредить администратора.

Защита паролем Azure AD не является механизмом приложения политики в реальном времени. Может быть задержка между тем, когда изменение конфигурации политики паролей производится в Azure AD, и когда это изменение достигает и применяется на всех контроллерах домена.

Защита паролем Azure AD действует как дополнение к существующим политикам паролей Active Directory, а не как замена. Это включает в себя любые другие сторонние библиотеки фильтров паролей, которые могут быть установлены. Active Directory всегда требует, чтобы все компоненты проверки пароля были согласованы, прежде чем принимать пароль.

Два необходимых установщика агента для защиты паролем Azure AD доступны в Центре загрузки Microsoft.

Устраните «плохие» пароли в вашей организации

Лидеры отрасли советуют вам не использовать один и тот же пароль в нескольких местах, чтобы сделать его стойким и не делать простым, например «Password123». Как организации могут гарантировать, что их пользователи следуют рекомендациям передового опыта? Как они могут убедиться, что пользователи не используют слабые пароли?

Первым шагом к созданию более надёжных паролей является предоставление рекомендаций вашим пользователям.

Важно иметь хорошее руководство, но даже при этом мы знаем, что многие пользователи всё равно будут выбирать слабые пароли. Azure AD Password Protection защищает вашу организацию, обнаруживая и блокируя известные слабые пароли и их варианты.

Глобальный список запрещённых паролей

Группа Azure AD Identity Protection постоянно анализирует данные телеметрии безопасности Azure AD, выискивая часто используемые слабые или скомпрометированные пароли. Содержимое глобального списка запрещённых паролей не основано на каком-либо внешнем источнике данных. Этот глобальный список полностью образован на текущих результатах телеметрии и анализа безопасности Azure AD.

Всякий раз, когда новый пароль изменяется или сбрасывается для любого пользователя в любом клиенте Azure AD, текущая версия глобального списка запрещённых паролей используется в качестве ключевого ввода при проверке надёжности пароля. Следует учесть, что киберпреступники также используют подобные стратегии в своих атаках. Поэтому Microsoft не публикует содержимое этого списка.

Пользовательский список забаненных паролей

Некоторые организации могут захотеть ещё больше повысить безопасность, добавив свои собственные настройки поверх глобального списка запрещённых паролей в том, что Microsoft называет настраиваемым списком запрещённых паролей. Microsoft рекомендует, чтобы термины, добавленные в этот список, были в основном сфокусированы на специфических для организации условиях, таких как:

- Торговые марки
- Названия продуктов
- Местоположение (например, штаб-квартира компании)
- Специфичные для компании внутренние условия
- Сокращения, имеющие конкретное фирменное значение

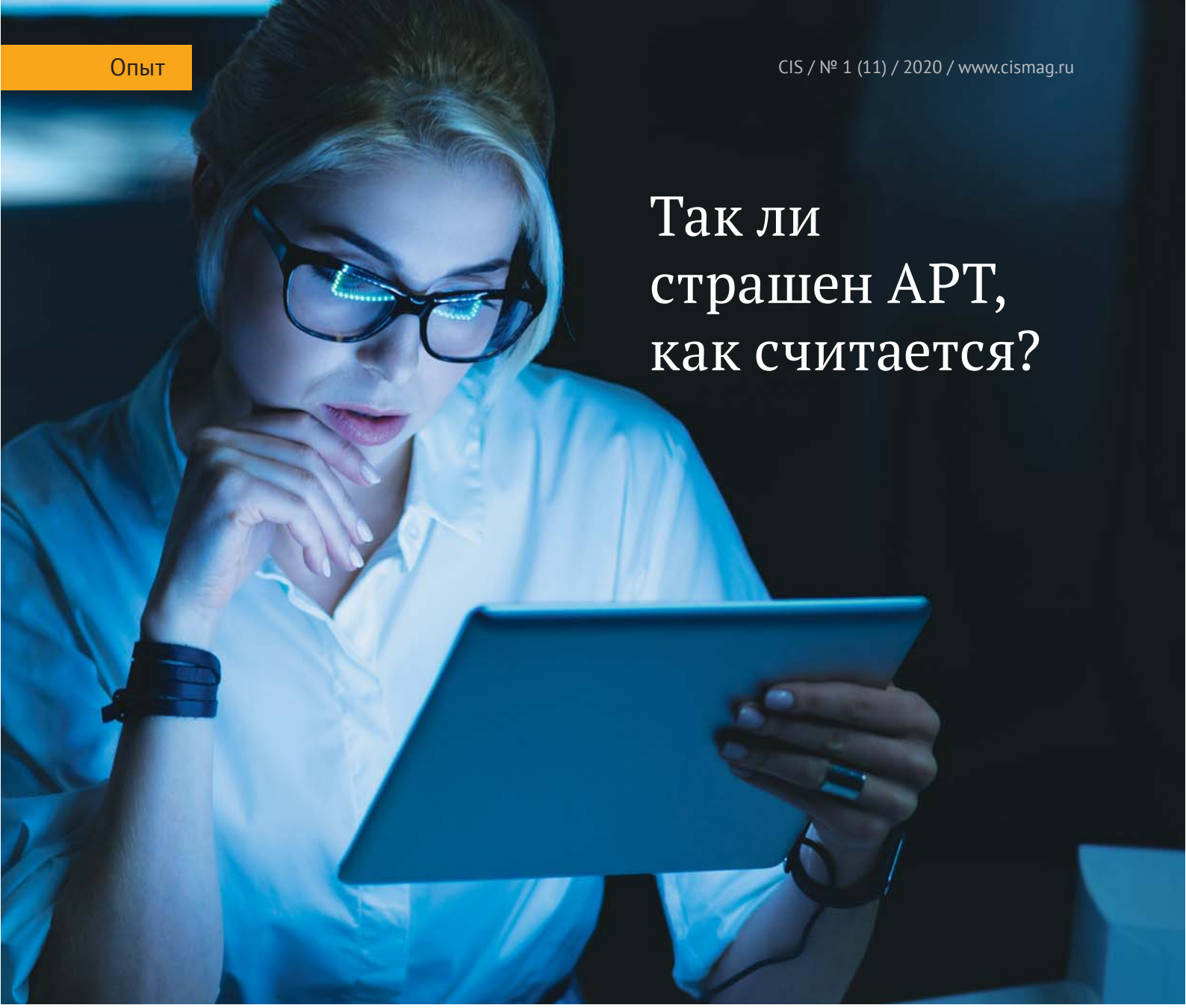
После добавления терминов в пользовательский список запрещённых паролей при проверке они будут объединены с условиями в глобальном списке таких паролей.

Атака паролем и сторонние скомпрометированные списки паролей

Одним из ключевых преимуществ защиты паролем Azure AD является защита от атак с использованием паролей. В большинстве случаев атаки с разбивкой паролей не осуществляются на какую-либо отдельную учётную запись более чем несколько раз, так как такое поведение значительно увеличивает вероятность обнаружения. Поэтому большинство атак с применением паролей основывается на том, что для каждой из учётных записей на предприятии предоставляется только небольшое количество известных слабых паролей. Этот метод позволяет злоумышленнику быстро найти учётную запись со слабым паролем, избегая при этом обнаружения.

Защита паролем Azure AD разработана для эффективной блокировки всех известных слабых паролей, которые, вероятно, будут использоваться при атаках с использованием паролей на основе реальных данных телеметрии безопасности, как это видно из Azure AD. Microsoft знает о сторонних веб-сайтах, которые перечисляют миллионы паролей, которые были скомпрометированы в результате ранее известных нарушений безопасности. Обычно сторонние продукты для проверки паролей основаны на сравнении методом «грубой силы» с этими миллионами паролей. Microsoft считает, что такие методы не лучший способ улучшить общую надёжность пароля, учитывая типичные стратегии, используемые злоумышленниками с распылением паролей.

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



Так ли страшен APT, как считается?

Статистика последних лет показывает, что доля APT-атак[1] в общем массиве атак становится всё больше, а целью злоумышленников перестают быть исключительно деньги: всё большее число атак преследует своей целью получение тех или иных данных.

В частности, по итогам третьего квартала этого года доля целенаправленных атак составила 65% (тогда как во втором квартале их было 59%)[2]. При этом наибольший интерес для злоумышленников сегодня представляют государственные учреждения, промышленные компании, финансовый сектор и организации сферы науки и образования. О том, что такое APT-атака, есть ли у организаций шанс им противостоять и удастся ли когда-нибудь свести эту угрозу к нулю, мы поговорили с Алексеем Новиковым, директором экспертного центра безопасности Positive Technologies (PT Expert Security Center).

– Что такое APT-атаки, и когда они появились?

– Если говорить об APT непосредственно как о термине, то ему около 10 лет. То есть сам термин стал популярным после небезызвестной атаки Stuxnet, которая была организована в 2009 году и совершалась с использованием одноимённого трояна. Цель атаки была в нарушении работы промышленных систем управления газопроводом и энергоустановок для получения доступа к иранской ядерной программе. Однако как сущность APT-атаки существенно старше – первые публичные истории по разным источникам относятся к концу 90-х – началу 2000-х гг. И даже эти истории вполне могут оказаться не первыми, на самом деле, так как результаты таких атак исключительно редко становятся достоянием общественности. Итак, по своей сути APT – это целенаправленная, продуманная, сложно организованная атака, которая направлена

1. Advanced Persistent Threat (APT) или целевая/таргетированная атака – это хорошо организованная, тщательно спланированная кибератака, которая направлена на конкретную компанию или целую отрасль.
2. Актуальные киберугрозы: III квартал 2019 года, Positive Technologies.

на конкретную организацию или отрасль (а в редких случаях – и на конкретную личность).

Изначально считалось, что наиболее вероятным объектом такого рода атак являются какие-то правительственные (или силовые) структуры, однако с течением времени такие атаки видоизменились и стали гораздо более распространёнными. И это можно считать результатом естественного развития цифрового мира: всё большее число процессов мигрируют из мира физического в цифровой, и злоумышленники понимают, что зачастую целенаправленная кибератака приносит им больший эффект, чем её физический аналог. Таким образом, сегодня APT-атакам подвержены самые различные организации по всему миру, а цели у атакующих самые разные: от получения прямой финансовой выгоды до промышленного шпионажа, например (кстати, именно те атаки, которые направлены на получение данных, с точки зрения выявления, можно считать наиболее сложными). Неизменным, однако, осталось следующее: они являются целевыми, то есть злоумышленник чётко знает, куда он хочет попасть и что в итоге получить.

– Какие есть признаки начала вот такой целенаправленной атаки?

– На самом деле, очень сложно понять, что APT-атака началась, потому что злоумышленники готовятся к ней очень долго и тщательно. Наша практика показывает, что подавляющее большинство организаций не в состоянии выявить такую атаку, а среднее время присутствия злоумышленника в сети организации, по оценкам Ponemon Institute, превышает 200 дней. В нашей же практике бывали случаи, когда во время расследований мы выявляли факты гораздо более длительного присутствия злоумышленников в сети (до двух, трёх и даже более лет). Причина в том, что злоумышленники целенаправленно изучают свою цель. И делают это со всевозможной тщательностью: они прекрасно понимают, какие средства защиты информации установлены и, соответственно, как организация будет им противодействовать и каким образом надеется их обнаружить. При этом редкая организация по-настоящему задумывается, что именно она может стать целью APT-атаки. И ещё меньшее их число обладают таким уровнем зрелости в плане ИБ, чтобы использовать специализированные решения класса anti-APT, предназначенные для раннего выявления и предотвращения целевых атак. Поэтому, к сожалению, наша статистика печальна: в большинстве случаев обнаружение начала целенаправленной атаки оказывается для организаций невозможным. В ряде случаев атакуемым удаётся понять это в тот момент, когда атака развивается уже внутри инфраструктуры (и это при условии, что в арсенале компании есть специализированные средства защиты, выстроенные процессы ИБ и достаточное число высококвалифицированных экспертов). Фактически же чаще всего жертвы понимают, что они атакованы ровно в тот момент, когда атака свершилась и злоумышленник достиг своей цели. Например, когда потеряно какое-то количество денег со счётов или внезапно нарушена жизнедеятельность ключевой бизнес-системы – это в качестве признака успешной атаки просто невозможно не заметить. Сложнее ситуация, если злоумышленник был нацелен на хищение данных: львиная доля атакованных организаций даже не знает о том, что значимые для них данные уже давно известны не только им одним. Например, однажды в ходе расследования активности одной из кибергруппировок выяснилось, что группировка присутствовала в инфраструктуре пострадавшей компании порядка 8-ми лет. И злоумышленники в течение этого времени изучали инфраструктуру, имели доступ ко всем данным (а организация при этом даже не догадывалась, что они скомпрометированы). За этот период состав службы информационной безопасности этой компании сменился едва ли не полностью, а группировка продолжала жить вместе с организацией.

– Какова этапность атак такого типа? Есть ли в них что-то общее?

– По своей этапности APT-атака мало чем отличается от атак, которые проводят не столь целенаправленно. Безусловно, следует отметить, что в данном случае злоумышленники более тщательно подходят к выбору цели, как я уже говорил, и к этапу подготовки. Однако сама очерёдность этапов и шагов стандартна: проникновение внутрь, получение привилегий (и их увеличение при необходимости) и перемещение внутри инфраструктуры. У APT-группировок есть ещё один важный признак – они весьма озабочены тем, чтобы остаться в захваченной инфраструктуре как можно дольше и как можно более незаметно. Поэтому они используют множество инструментов, предназначенных для сокрытия их присутствия, маскировки под легитимную активность, а при необходимости – и для запутывания следов и усложнения расследования и атрибуции. И такой инструментарий нередко адаптируется и видоизменяется под конкретные условия инфраструктуры. Например, во время расследований мы неоднократно наблюдали, как злоумышленники, поняв, что их инструментарий начал детектироваться, скажем, антивирусом, буквально в течение 2-3 дней начинали использовать его обновлённый образец, изменённый ровно настолько, чтобы не детектироваться существующей версией антивирусного решения. Ну и финальный этап любой атаки – собственно, хищение денег, данных, нарушение работоспособности систем, остальных бизнес-процессов и прочего, что, по большому счёту, может быть актуально и не только для APT-группировок.

– Мы ознакомились со статистикой, которая показывает, что только 5% промышленных производств имеют специализированные решения для противодействия таким атакам. Почему недостаточно традиционных базовых систем защиты?

– Да, одно из наших исследований показывает, что использование специализированных anti-APT решений было актуально всего лишь для 5% опрошенных респондентов, представляющих промышленные организации.

Алексей Новиков,
директор экспертного центра безопасности Positive Technologies (PT Expert Security Center).

При этом в 100% случаев отмечалось использование антивирусных решений, в 47% – использование IPS\IDS, тогда как использование, скажем, систем класса SIEM или NTA отметили всего 33% и 21% соответственно[3].

С точки зрения эффективного противодействия действительно недостаточно использования только лишь базовых средств защиты, потому что противостояние злоумышленников и защитников – это постоянная гонка вооружений. Как только защитники внедряют какую-то новую технологию, злоумышленники тут же придумывают способы её обхода. Безусловно, традиционные хрестоматийные подходы к информационной безопасности нужны: они позволяют обеспечить базовую гигиену информационной безопасности, и без их использования, пожалуй, никакая суперсовременная интеллектуальная технология защиты не взлетит. Тем не менее остановить целенаправленную атаку они не в состоянии. Для этого нужны специализированные решения, объединяющие такой набор технологий, который позволит им если не выявить активность нападающих прямо в момент начала атаки, то как минимум заметить её спустя незначительное время, когда злоумышленник уже оставил какие-то следы в инфраструктуре, совершает попытки перемещения, но при этом ещё не достиг своей конечной цели.

– Что необходимо учитывать при выборе решения против такого рода атак?

– Во-первых, такое решение должно совмещать в себе максимальное количество различных способов обнаружения APT-атаки, потому что нельзя надеяться только на один источник данных, равно как и на какую-то одну технологию. Необходима их совокупность. Нужно анализировать все файлы, которые циркулируют в сети, причём не только входящие файлы, но и те, которые «живут» внутри организации, не выходя за её пределы. Злоумышленники нередко изменяют вредоносное программное обеспечение уже на этапе горизонтального перемещения, то есть когда они перемещаются от одной рабочей машины к другой.

Далее, необходимо обязательно и пристально изучать и анализировать трафик. Причём недостаточно просто выстроить границу с открытым интернетом. Как бы ни была хороша преграда, её всё равно рано или поздно преодолеют: найдётся какая-то уязвимость, закладка или что-то иное, что позволит злоумышленникам проникнуть внутрь периметра. В среднем, в 92% проектов по тестированию на проникновение наши эксперты преодолевали сетевой периметр и получали доступ к ресурсам ЛВС, и не менее чем в 50% компаний потенциальный злоумышленник может преодолеть сетевой периметр всего за один шаг[4].

Необходимо также мониторить трафик внутри организации. А дальше в игру вступают различные методы machine-learning статического и динамического анализа. Немаловажным становится тот фактор, что о некоторых атаках становится известно спустя некоторое время, и необходимо, чтобы anti-APT-решения могли в прямом смысле слова заглянуть в прошлое и ретроспективно определить, была ли атака актуальна ранее или нет, а если была, то как давно и каков масштаб поражения. Мы, будучи производителем одного из anti-APT решений, выпускаем аналитические отчёты по действиям группировок, выявляем, описываем и публикуем индикаторы, выявление которых при ретроспективном поиске может свидетельствовать об атаке. И, конечно же, все индикаторы появляются в наших соответствующих продуктах: системе выявления инцидентов ИБ в реальном времени (MaxPatrol SIEM), системе анализа трафика (PT Network Attack Discovery) и, соответственно, в комплексе для раннего выявления сложных угроз.

– Какой всё-таки прогноз? Хотелось бы подытожить: группировки постоянно эволюционируют – насколько это страшно? Удастся ли их победить?

– Сомневаюсь, что их удастся победить в прямом смысле слова. Это философский вопрос. И, проводя аналогию с традиционной преступностью, нет такого государства, которое смогло бы искренне заявить, что ему удалось искоренить преступность целиком и полностью. А говоря о киберпреступности, мы всё же ведём речь ни о чём ином, как о преступности. Просто в новой – цифровой форме. И учитывая, что общие темпы развития и глубину проникновения ИТ-технологий и цифровизации в нашу повседневную жизнь, следует ожидать, что киберпреступность будет расти соответствующими темпами и целенаправленные атаки, как подвид, не исключение. Тенденции последних лет показывают, что общее число группировок и их активность с течением времени растёт: если в 2009 году количество известных атак исчислялось штуками, то сегодня число атак ежеквартально исчисляется десятками, а общее число APT-группировок, атакующих отечественные организации, перевалило за два десятка.

3. APT-атаки на промышленные компании в России: обзор техник и тактик, Positive Technologies, 2019 г.
4. Уязвимости корпоративных информационных систем, Positive Technologies, 2019 г.

УНИВЕРСИТЕТ СИНЕРГИЯ

25-26 мая 2020 | Москва | «Крокус Сити Холл»

Конференция о мозге и мышлении

BRAIN 2020

Как изменить свою жизнь? Мозг — как компьютер. Загрузите в него нужную программу и измените свою жизнь. Научитесь управлять им, и вы легко достигнете успеха в любом деле.

Всемирно известные спикеры, исследователи и учёные расскажут, как мозг влияет на ваши решения, как им управлять, как эмоции связаны с целями и как это можно контролировать.

Мероприятие для тех, кто готов работать над собой, а не ждёт, что всё изменится само собой.

BRAIN 2020

2 0 × 2 0

CIS / № 1 (11) / 2020 / www.cismag.ru

Как самостоятельно организовать тестирование сотрудников на целевой фишинг?

Кибератаки на предприятие могут начинаться с поиска оборудования, подключённого к Интернету, например с использованием открытой платформы SHODAN, но эта атака эффективно защищается простой мерой – установкой сложных паролей и исключением паролей по умолчанию.

Наиболее простым способом начала атаки, от которого защититься сложнее, является целевой фишинг. Согласно статистике ведущих аналитических компаний, в том числе российских, целевой фишинг является основным инструментом начала целевой компьютерной атаки.

Рисунок 1.

Использование целевого фишинга как способа проведения целевых атак является одним из самых эффективных. Это связано с тем, что метод использует уязвимости персонала, то есть человеческий фактор. Человек, как известно, является слабым звеном любой системы, так как способен принимать необдуманные и спонтанные решения, в том числе под влиянием эмоций.

Стандартная компьютерная атака начинается с тщательного изучения атакуемого объекта. Точкой входа при целевом фишинге является корпоративная почта. Сотрудник получает письмо на корпоративную почту, при этом текст составлен таким образом, что вызывает желание открыть файл или перейти по ссылке. После этого действия за счёт уязвимостей обычно загружается валидатор, проверяющий версии ПО, ОС, после чего определяется спектр уязвимостей в данной системе.

После фазы фишинга начинается загрузка вредоносного ПО, эксплуатирующего найденные уязвимости, для сбора и хищения информации: настройки (пароли) файерволов, установленные на границе с внутренними (индустриальными) сегментами сети, общие папки с внутренними сетями (например, с обновлениями антивирусных программ). Внедрённое ПО может распространяться по сети также без сохранения на жёсткий диск.

Таким образом, после внедрения в корпоративной сети вредоносное ПО может найти способы проникновения в индустриальную сеть и там установить систему удалённого сбора данных с последующим изменением данных в СУБД управляющего ПО, контроллерах, которые могут привести к неправильному управлению технологическим процессом и аварии.

С целевого фишинга начинались многие известные кибератаки. Последняя атака со значительными последствиями и использованием целевого фишинга произошла в Норвегии в компании по производству алюминия – Norsk Hydro – 18.03.2019 с применением вируса-шифровальщика Locker Coga.

Сотрудники успели изолировать индустриальную сеть от корпоративной и перевести управление части оборудования из автоматического режима в ручной. Тем не менее временная остановка части производственного процесса (в том числе плавильных печей), резервное восстановление ПО, изоляция корпоративной сети, почты, сайта с удалением вируса заняли значительное время и принесли финансовые потери.

Фишинг как способ атаки успешен по большей части из-за человеческого фактора. Человек, как известно, является слабым звеном в любой системе. Концентрация лишь на техническом оснащении системы защиты информации, является большой ошибкой. Осведомлённость пользователя о рисках фишинга и умении идентифицировать целевое фишинговое письмо может существенно повысить уровень защищённости организации.

Как самостоятельно организовать тестирование сотрудников на целевой фишинг?

Обучение и мониторинг готовности персонала на целевой фишинг обычно проводится с использованием 4-х этапов (рис. 1).

Этап 1 – Выбор средств и технологий тестирования

На первом этапе выбираются программы для целевой тестовой рассылки, при этом нашей рекомендацией является бесплатная и поддерживаемая разработчиками программа Gophish. Программа позволяет анализировать открытие письма, файла и переход по ссылке, делать автоматическую загрузку адресов, ФИО. Gophish – бесплатная программа, поддерживается большинством операционных систем, а также имеет простую процедуру установки. Также стоит отметить простое управление созданными шаблонами и пользователями, удобный и наглядный интерфейс, представленный на рисунке 2.

После установки для проверки работоспособности необходимо отправить тестовое письмо (во вкладке **Sending Profiles**).

Во вкладке **Users&Groups** создаётся профиль получателей писем. Данные можно как импортировать, так и ввести вручную в формате:

- first name;
- last name;
- email;
- position (должность).

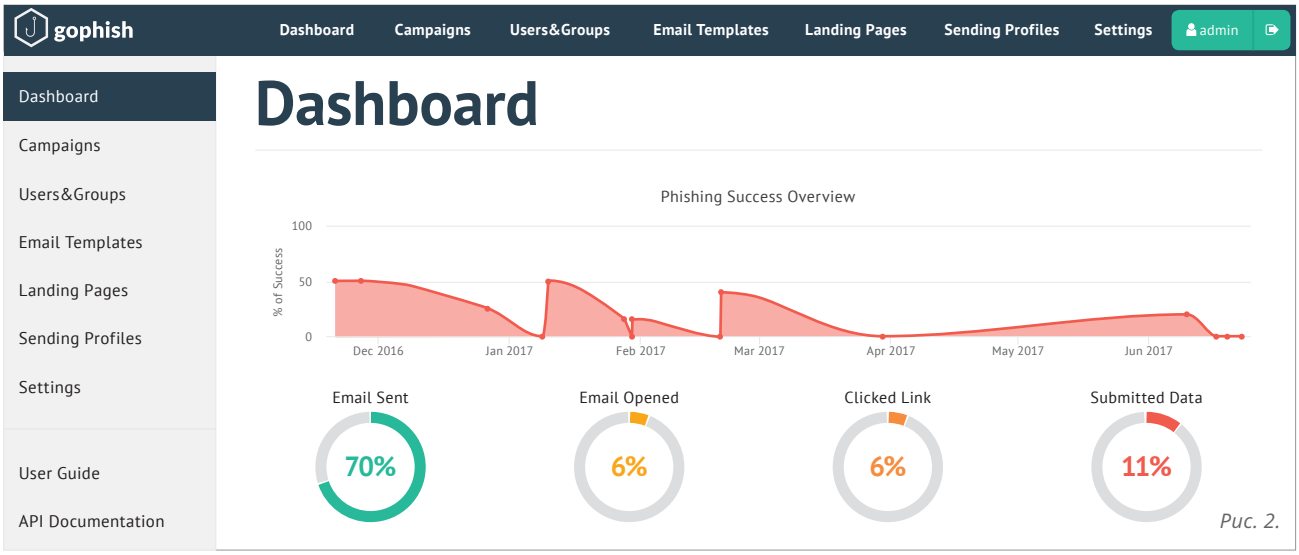


Рис. 2.

Во вкладке **Landing Pages** создаётся страница, на которую будет перенаправлена жертва в случае перехода по ссылке. Страница будет находиться на сервере GoPhish, поэтому запуск отдельного сервера не потребуется. Страницу можно импортировать или написать вручную на HTML.

Для запуска процесса рассылки во вкладке **Campaings** достаточно настроить время и параметры рассылки, после чего во вкладке **Dashboard** следить за её ходом (рис. 2).

GoPhish можно запускать на локальном хосте обычной рабочей машины организации. Этот вариант более прост и удобен в настройке, но позволит работать только с компьютерами в локальной сети.

Для расширения возможностей (управления и рассылок за пределами локальной сети организации) необходимо предоставить GoPhish публичный IP-адрес, на хостинге которого будут размещены как сам инструмент, так и страница, на которую будет перенаправлена жертва в случае перехода по ссылке.

Например, можно разместить на **Amazon Web Services**, расположенного в облаке. Это может быть виртуальный сервер с предустановленной операционной системой Ubuntu, управление которой будет осуществляться посредством SSH.

После установки GoPhish разрабатывается страница жертвы. Обычно это предупреждающая страница о нажатии на фишинговую ссылку (рисунок 3), но может быть и имитация сайта для ввода, например персональных данных. При этом ввод данных контролируется GoPhish (рис. 3).

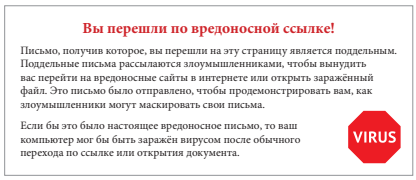


Рисунок 3.

Этап 2 – Обучение персонала

Важным для сотрудников является знание принципов фишинга, методов социальной инженерии, анализ самого письма и особенно обратного адреса письма. В тексте ссылки при подозрении на злонамеренность желательно посмотреть адрес ссылки по буквам, а при необходимости набрать его в ручном режиме для исключения фарминга (подмены 1-2 символов относительно правильного адреса). Важным является обновление системного ПО: ОС, браузеров и прикладного ПО, при этом в обучении должны участвовать и системные администраторы, несущие за это ответственность.

В основном при целевом фишинге идёт акцент на формирование эмоции (например, страх возможного увольнения при получении списка якобы увольняемых сотрудников, желание помочь, в том числе своему сотруднику, о чём упоминалось выше). Поэтому при моём обучении я рекомендую оценивать появление эмоциональной составляющей (страх, сострадание, сочувствие, альтруизм, тревога, готовность поддержать, доверчивость, жалость, желание испытать новое, быть в тренде и т.п.).

Используются также знания о пользователе. Например, бухгалтеру приходит письмо об обновлении бухгалтерской программы с указанием имени и фамилии бухгалтера. В июле 2018 года как раз-таки был использован новый метод: в письме указывался логотип антивирусной компании с просьбой обновить антивирус. Согласитесь, это вызывает определённое доверие.

Этап 3 – Мониторинг готовности персонала

После обучения персонала можно проверить полученные теоретические знания и, выждав 2-3 недели, провести выборочную или полноценную рассылку с помощью GoPhish с оценкой насколько сотрудники запомнили полученную информацию при обучении. Для соревновательности важным является сравнение, например подразделений, кто меньше отреагирует на тестовые спам-письма.

Важным является постепенное усложнение фишинговых писем, для обучения и адаптации персонала к возможному реальному фишингу. Однако не стоит делать слишком сложных писем, чтобы у пользователя не возник страх открытия писем от реальных, но неизвестных ему адресатов.

Письмами повышенной сложности стоит тестировать администраторов, которые обладают максимальными правами доступа, так как заражение их компьютера может быть наиболее интересно нападающим. Пример усложнения писем (уровни 1, 2, 3 рекомендуется для обычных пользователей, уровни 3 и 4 для системных администраторов) приведён в таблице.

При организации тестирования на фишинг необходимо анализировать показатели и их изменение как результат улучшения распознавания сотрудниками фишинговых писем:

	Уровень 1	Уровень 2	Уровень 3	Уровень 4 (администратор)
Приветствие и подпись	Без Ф.И. О. и с ошибками подписи	Персональное с ошибками подписи. Наличие логотипов Компаний с ошибками	Персональное без ошибок. Наличие фирменных логотипов Компаний	Персональное с фокусом на персональный интерес
Характер содержания	Призывы к чувству интереса, любопытства, помощи	Призывы к страху, любопытству с использованием брендинга	Призывы к страху, жадности, выполнению должностных обязанностей с использованием брендинга	Лично персонифицированное письмо с учётом личных интересов, эмоций с учётом уровня 3
Ссылки/прикреплённые файлы	Ошибки в названии	Ошибки в открывающемся сайте/файле	Без ошибок и без персонификации	Без ошибок и с персонификацией адресата
Отправитель (e-mail)	Неизвестный	Сервер и логин близки к контуру общения	Отличие в 3-4 символах	Отличие в 1 символе от реального адреса
Пример	Опрос Лаборатории Касперского / Сбербанка	Письмо об обновлении антивируса от Касперского или 1С-бухгалтерии, список уволенных сотрудников	Смена пароля с интерфейсом Компании, начисление бонусов от Банка	Анкета для участия с частью заполненных данных или автозаполнение перс. данных в web-интерфейсе Банка/компании при смене пароля

- **Персонал:**
  - процент обученных сотрудников среди допущенных к корпоративной почте;
  - результаты тестирования сотрудников (теория);
  - результаты тестирования сотрудников (практика – процент переходов по ссылке, введённых данных на сайтах).
- **Рабочие места:**
  - процент обновлённых операционных систем;
  - процент обновлённых почтовых программ.
- **Антиспам-фильтры почтовых серверов** (наличие настроек от фишинга).

Этап 4 – обратная связь

После проведения тестирования необходимо дать обратную связь, например: разместить на корпоративном сайте и в письмах пользователям информацию о внесённых в тестовые фишинговые письма ошибках.

Как видно, процесс тестирования сотрудников на целевой фишинг является несложным как технически, так и организационно, однако при подготовке к тестированию на фишинг необходимо соблюдать ряд моих личных рекомендаций:

- письменно согласовать с подразделениями предприятия (ИТ-департамент, СБ, режимные подразделения и т. п.) все аспекты тестирования: время, вид фишингового письма, список тестируемых адресов и т. п.;
- использовать все возможности программ для тестирования (например, автоматическую загрузку адресов, ФИО, обратную информацию об ОС на АРМах, где письмо было открыто) для повышения удобства тестирования;
- обеспечить защиту персональных данных (списка всех адресов, ФИО) для исключения их утечки, в том числе минимизировать сбор персональных данных на тест-фишинговых сайтах для исключения их реальной утечки и использовать проверенные облачные сервисы для исключения той же утечки загружаемых персональных данных;
- учитывать, что создание фишинговых страниц, например антивирусной компании или Банка может нарушить авторское право или права использования торговой марки;
- планомерно увеличивать сложность писем с одновременным информированием пользователей об ошибках и результатах;
- периодичность мониторинга – не чаще 2-3 раз в год для одного сотрудника);
- обеспечить наличие общего (корпоративного) информирования (например, на внутреннем портале) о новых угрозах, типовых ошибках пользователей при открытии тестовых фишинговых писем;
- обеспечить непрерывность процесса обучения и тестирования.

Как правило, по личному опыту, процесс подготовки к первому тестированию на фишинг на предприятии занимает около одного месяца с учётом согласования со всеми подразделениями и подготовки программно-технической инфраструктуры.

Обычно, достаточно одного ИТ-специалиста с занятостью 2-3 месяца в первый год и 1-2 месяца в последующие года, чтобы организовать и проводить такой процесс на предприятии. Плюс в месяц будут задействованы от 1 до 3 сотрудников других подразделений. Результатом обычно является повышение осведомлённости пользователей, обновление устаревших версий ПО, настроек анти-спам фильтров.

Организация самостоятельного тестирования позволяет значительно сэкономить бюджет, уменьшить риск утечки персональных данных сотрудников, узнать об их уязвимых местах, данных о технической инфраструктуре организации и её недостатках, а также повысить осведомлённость своих сотрудников в проведении такого тестирования. При этом возможен вариант привлечения одного стороннего эксперта в помощь для быстрого обучения сотрудников по развёртыванию технической инфраструктуры, подготовки фишинговых писем с учётом специфики подразделений без передачи персональных данных и данных о технической инфраструктуре.

Журин С.И., начальник лаборатории разработки информационных систем, АО «ФЦНИВТ «СНПО «Элерон», к. т.н. Доцент кафедры «Криптология и кибербезопасность» НИЯУ МИФИ

CIS / № 1 (11) / 2020 / www.cismag.ru

Практика импортозамещения в МФЦ Курской области

Продолжается практическая реализация политики импортозамещения программного обеспечения в Российской Федерации. Один из примеров успешного внедрения отечественного ПО – проект перехода «Многофункционального центра по предоставлению государственных и муниципальных услуг» Курской области на операционную систему РЕД ОС.

В результате проведённых работ в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 04.07.2018 № 335 был перевыполнен показатель доли применяемых отечественных операционных систем для подведомственных организаций (не менее 50%).

«До 2018 года рабочие станции МФЦ Курской области работали на MS Windows. Обновление правовой базы поставило перед нашим МФЦ задачу обеспечить соответствие используемого программного обеспечения нормативным требованиям и выполнить плановые показатели. Это было реализовано переводом большинства рабочих мест всех подразделений организации на отечественную операционной систему РЕД ОС. Успех проекта свидетельствует о том, что нами был сделан правильный выбор», – комментирует первый заместитель директора «Многофункционального центра по предоставлению государственных и муниципальных услуг» Курской области Заугольников Роман Юрьевич.

В качестве главного критерия выбора операционной системы использовались параметры совместимости с программно-аппаратными средствами, применяемыми в ИТ-инфраструктуре учреждения. Рассматривалось несколько решений из Реестра отечественного ПО. В результате проведённого анализа предпочтение было отдано РЕД ОС.

Проведённые испытания показали, что РЕД ОС полностью совместима с автоматизированной информационной системой МФЦ и поддерживает работу под управлением домена Active Directory, что входило в перечень ключевых требований заказчика. Немаловажную роль в успехе РЕД ОС сыграли простота в использовании и настройки для работы в гетерогенной среде, быстрая интеграция системы в ИТ-инфраструктуру заказчика, а также наличие развитой базы знаний. Наряду с этим специалисты компании «РЕД СОФТ» продемонстрировали свою готовность быстро и качественно исполнять задания в удалённом режиме, в том числе оказывать услуги по технической поддержке.

Опыт предыдущих массовых внедрений Linux-систем позволяет сделать вывод о том, что одна из главных причин, препятствующих их успеху, – непривычный пользователю интерфейс. Разработчики РЕД ОС учли эту проблему. В системе применяется интуитивно понятное окружение рабочего стола, освоение которого не вызывает серьёзных проблем у пользователей Windows. Подобный подход позволил заметно сократить время, требуемое на обучение сотрудников МФЦ.

«Мы уделяем большое внимание вопросам удобства работы пользователей. В состав нашей системы по умолчанию входит большое количество предустановленных программ, позволяющих решать разнообразные задачи: от просмотра сайтов в Интернете до редактирования мультимедийных файлов. Они имеют привычный графический интерфейс, что способствует их быстрому освоению. В репозитории РЕД ОС хранятся дополнительные пакеты, установка которых даёт возможность расширить функциональность решения», – комментирует заместитель генерального директора РЕД СОФТ Рустам Рустамов.

Этапы проекта

В течение **предварительного этапа,** стартовавшего в 2017 году, заказчик проанализировал входящие в реестр ОС и выбрал РЕД ОС как решение, наиболее удовлетворяющее его требованиям. Также была проведена полная ревизия программных средств, уже используемых в ИТ-инфраструктуре МФЦ Курской области. Она показала, что в качестве серверной составляющей в организации применяются 80 физических и виртуальных серверов, работающих под управлением систем Windows Server 2008/2012/2016, CentOS 7, Ubuntu 16.04 и защищаемых средствами защиты от несанкционированного доступа Dallas Lock. Работу МФЦ обеспечивают около 500 рабочих станций.

Проведённый специалистами РЕД СОФТ анализ показал, что операционная система РЕД ОС совместима практически со всеми программно-аппаратными средствами АУ КО МФЦ. Также экспертами заказчика произведена оценка уровня технической поддержки РЕД ОС, которая признана полностью соответствующей всем требованиям государственного учреждения.

В результате предварительного этапа сделано заключение, согласно которому на базе РЕД ОС возможно выполнение всех деловых процессов МФЦ Курской области. В 3-м квартале 2018 года руководство учреждения приняло решение о переводе ИТ-инфраструктуры на РЕД ОС.

В рамках **второго этапа** компания «РЕД СОФТ» предоставила заказчику временные лицензии на 112 рабочих станций для организации пилотной зоны. В течение всего этапа разработчик оказывал МФЦ полноценную техническую поддержку стандартного уровня.

Непосредственно внедрение осуществлялось на **третьем этапе** проекта. РЕД СОФТ поставила заказчику 300 лицензий на РЕД ОС. Таким образом, на момент завершения третьего этапа общий объём внедрения РЕД ОС в МФЦ Курской области составил 55% от рабочих мест всех подразделений.

Результаты проекта

Требуемый плановый показатель 50% был достигнут заказчиком через год после начала проекта. В 2018 году он составил 50,1%.

На момент завершения проекта показатель применения отечественных операционных систем в АУ КО МФЦ достиг 55%. Причём четыре филиала полностью перешли на использование РЕД ОС.

Программное обеспечение и автоматизированные информационные системы применяемые в МФЦ Курской области работают на РЕД ОС без каких-либо функциональных ограничений. Это позволило заметно сократить расходы на иностранное проприетарное ПО, а благодаря тому, что РЕД ОС сертифицирована ФСТЭК России, также снизились затраты на средства защиты информации от несанкционированного доступа.

Планы и перспективы

Благодаря успешному завершению проекта руководство АУ КО МФЦ планирует увеличить долю рабочих станций, функционирующих под управлением российского ПО, до 85%. Это будет реализовано за счёт замещения MS Windows, техническая поддержка которой прекращена, на отечественную РЕД ОС.

Также на 2020 год запланирован перевод на РЕД ОС всех серверов учреждения. Соответствующие лицензии уже закуплены заказчиком.

РЕДСОФТ

«РЕД СОФТ»

www.red-soft.ru

CIS / № 1 (11) / 2020 / www.cismag.ru

Сервисы Google и Privacy

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

Макс Фрай

В современном мире всё чаще и чаще мы сталкиваемся с тем, что наша информация нам не принадлежит. Увы, но стоит признать, что понятия «тайна личной жизни» больше не существует. Можно ли всё же что-то защитить? Думаю, нет, но стоит попробовать. В данной статье мы рассмотрим можно ли что-то предпринять, чтобы сделать ваши данные всё же более защищёнными.

О том, что компания Google собирает данные о нас, мы давно знаем и свыклись с этим. Стоит отметить, что то, что о вас знает Google, – намного больше, чем то, что собирает о вас Android. Почему? А всё просто. Ведь мы используем сервисы Google не только на смартфонах под управлением Android, но и на ПК под управлением Windows, и на смартфонах под управлением iOS. Вспомните: карты Google, браузер Google Chrome и так далее.

Но всё же, что собирает о вас Google? Для того чтобы увидеть это, следует зайти по адресу https://myaccount.google.com. При этом вам потребуется войти в свой аккаунт (рис. 1).

На данной странице вы можете не только настроить конфиденциальность ваших данных, но и узнать какие данные хранятся в аккаунте.

Конфиденциальность и персонализация

Проверка настроек конфиденциальности

Настройки конфиденциальности мы начнём с **Проверки настроек конфиденциальности (рис. 2).**

Если вы включите функцию «История приложений и веб-поиска» – в аккаунте Google будут сохраняться сведения о ваших поисковых запросах и действиях в других сервисах Google. Эти данные позволяют быстрее находить актуальный контент и получать более точные рекомендации.

Учтите, данная опция включена по умолчанию. Но стоит отметить, что вы всегда можете отключить историю приложений и веб-поиска или удалить информацию о своих действиях.

Примечание. Если вы используете **корпоративный аккаунт или выданный вам в учебном заведении, то** включить историю приложений и веб-поиска может только администратор.

История местоположений

В Истории местоположений хранятся данные о том, где вы были со своими устройствами, на которых:

- Выполнен вход в аккаунт Google
- Включена история местоположений
- Разрешена отправка геоданных

С одной стороны, если история включена – вы можете получать дополнительные возможности в следующих сервисах:

- Персонализированные карты
- Рекомендации с учётом тех мест, которые вы уже посетили
- Помощь в розыске своего смартфона
- Сведения о пробках на дороге
- Актуальные рекламные объявления

Вместе с тем необходимо понимать, что в случае хищения вашего смартфона или получения доступа к данным о местоположении все ваши передвижения станут доступными сторонним лицам. А если учесть, что люди в большинстве случаев используют один и тот же маршрут…

По умолчанию история местоположений отключена. Кроме того, запись маршрутов можно приостановить в разделе **Отслеживание действий**.

Однако если вы думаете, что, отключив историю местоположений, вы сумеете сохранить приватность, то, увы, это не правда.

Как говорится в сообщении Associated Press (AP), Google записывает местоположения пользователей, даже когда они не просят об этом.

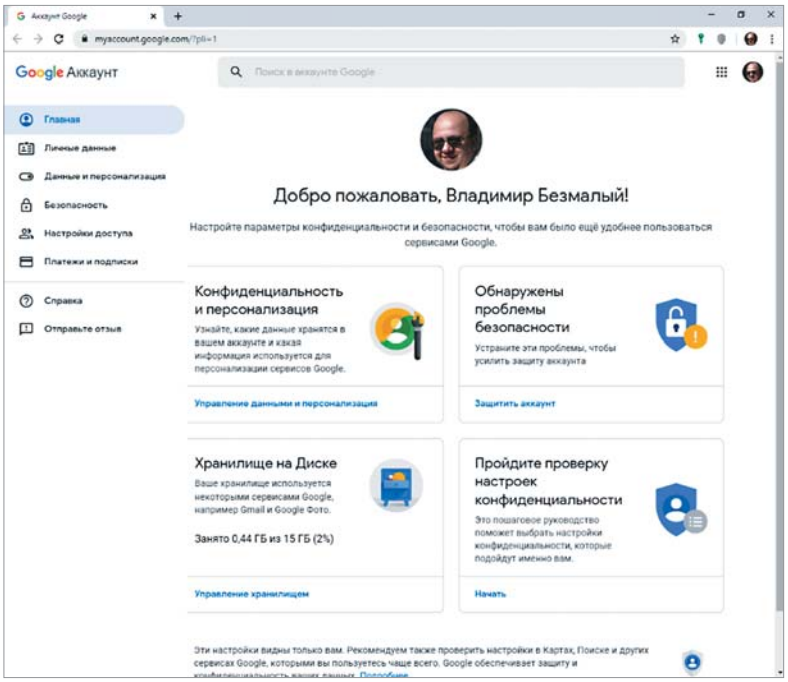


Рисунок 1. Настройка конфиденциальности

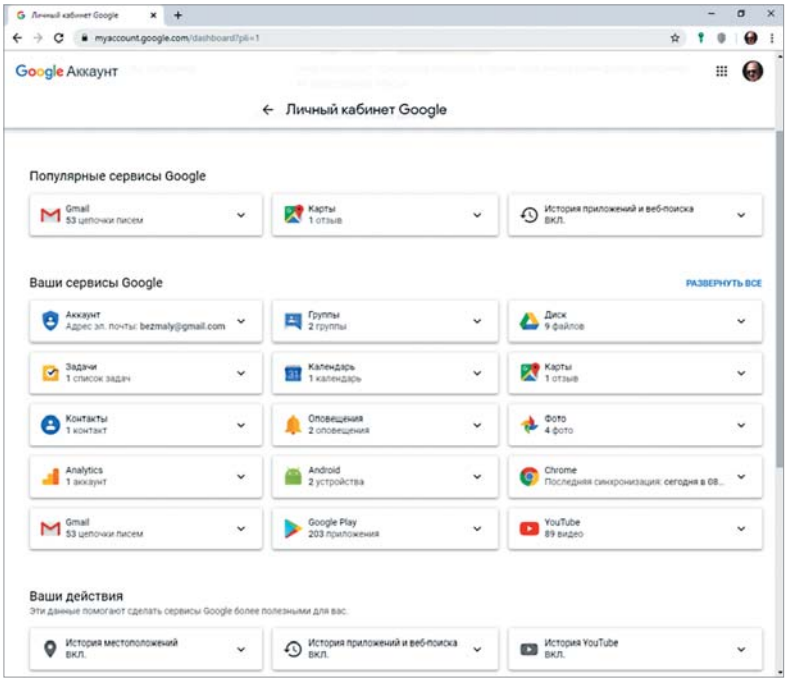


Рисунок 2. Личный кабинет

Эта проблема может затронуть до двух миллиардов устройств Android и Apple, которые используют Google для карт или поиска.

Исследование, проведённое научными сотрудниками из Принстонского университета, показало, что местонахождение пользователей регистрируется даже тогда, когда история местоположений была отключена.

Например:

- Google хранит снимок вашего местоположения при открытии приложения Карты

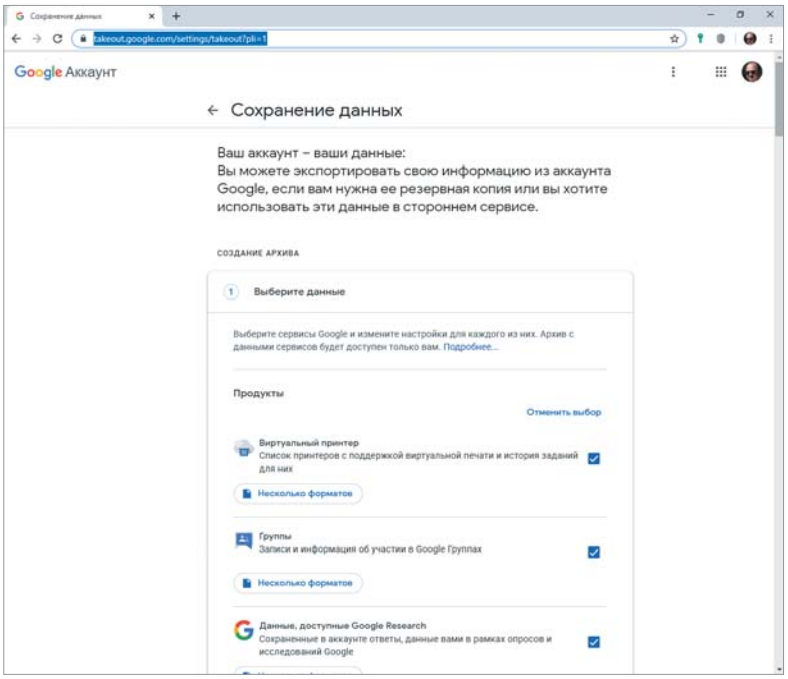


Рисунок 3. Сохранение данных

- Автоматические обновления погоды на телефонах Android точно указывают, где находится пользователь
- Поиски, которые не имеют никакого отношения к местоположению, точно определяют долготу и широту пользователей

Чтобы проиллюстрировать влияние этих маркеров местоположения, AP создала визуальную карту, показывающую движения исследователя из Принстона Гунеса Акара, который использовал телефон Android с отключённой историей местоположений.

Карта показала, что его поезд ездит по Нью-Йорку, а также он сам посещает парк Хай Лайн, рынок Челси, Центральный парк и Гарлем. Это также показало его домашний адрес.

Чтобы Google не сохранял эти маркеры местоположения, пользователи должны отключить другой параметр, который называется «Активность в Интернете и приложениях», который включён по умолчанию и не содержит данных о местоположении.

«Можно подумать, что, если вы скажете Google, что не хотите отслеживать своё местоположение, отключив опцию «История местоположений», это помешает интернет-гиганту хранить данные о вашем местоположении», – пишет исследователь блога Грэм Клули в своём блоге.

После своего исследования **AP создала руководство,** чтобы показать пользователям, как удалять данные о местоположении.

Следует учесть, что с 2014 года Google позволяет рекламодателям отслеживать эффективность онлайн-рекламы с помощью функции, основанной на данных о результатах, которая опирается на историю местоположений.

Независимое тестирование AP подтвердило, что iPhone работает аналогично при использовании приложений Google.

Данные о местоположении, собранные Google, можно найти на myactivity.google.com, но, как указывает точка *доступа,* эта информация разбросана по разным заголовкам, часто не связанным с местоположением.

Чтобы было ясно, Google не занимается незаконным сбором данных о местоположении, но запутывает свои политики в отношении данных о местоположении и собирает данные с помощью функций, которые не содержат информацию о местоположении. Многие люди могут не знать, что эти функции Google вообще включены, так как это настройка по умолчанию.

Единственное упоминание Google о том, что он может продолжать сохранять некоторые данные о местоположении, появляется во всплывающем окне, которое отображается, когда история местоположений отключена в настройках учётной записи Google. В этом всплывающем окне указывается, что «некоторые данные о местоположении могут быть сохранены как часть вашей деятельности в других службах Google, таких как Поиск и Карты».

На iPhone, когда «Журнал местоположений» отключён с помощью настроек в приложениях Google, говорится следующее: «Ни одно из ваших приложений Google не сможет сохранять данные о местоположении в Журнале местоположений». Как указывает AP, это утверждение верно, но вводит в заблуждение, потому что, хотя данные о местоположении не хранятся в истории местоположений, они всё ещё хранятся в разделе «Моя активность».

Информация о местоположении, хранящаяся в разделе «Моя активность», используется для таргетинга объявлений.

Чтобы запретить Google собирать какие-либо данные о местоположении, необходимо отключить «Активность в Интернете и приложениях» и «История местоположений», что можно сделать через пользовательские настройки учётной записи Google. На устройствах iOS неиспользование приложений Google и отключение служб определения местоположения для приложений Google также является эффективным способом предотвращения сбора данных о местоположении.

Для чего Google отслеживает ваше местоположение?

Чтобы лучше вас обслуживать:

- Google / Apple Maps, навигация
- Гораздо более релевантные результаты поиска

• Найти мой телефон / Найти моё устройство

Удобство:

• Знаете, как работает этот ресторан в это время дня или прямо сейчас
• Внутренняя навигация
• Чтобы продать рекламу

Основной источник дохода Google – объявления на основе местоположения (рис. 3).

Кроме того, не стоит забывать о таком сервисе, как Sensorvault.

Sensorvault

В процессе расследования различных преступлений полиция обращается к базе Sensorvault, принадлежащей Google, чтобы отследить местоположение и перемещение смартфонов.

Sensorvault содержит записи геолокации сотен миллионов мобильных устройств по всему миру. Она собирает соответствующую информацию, которую передают продукты Google, чтобы лучше понимать, какую рекламу отображать пользователям и как эта реклама работает.

Как передаёт The New York Times, за последние шесть месяцев подобные запросы резко увечились в количестве – стало приходить по 180 запросов за одну неделю. Сама Google отказалась предоставить развёрнутые данные относительно Sensorvault, однако заявила, что ограничила количество информации, которую предоставляет правоохранительным органам.

Благодаря Sensorvault полиция может отследить местоположение смартфона в определнной местности, а также получить информацию о том, в течение какого времени устройство находилось в этом месте.

Google: источники данных о местоположении

История местоположения: извлечение из облака, online интерфейс. Стоит отметить, что данных о местоположении чрезвычайно много.

Где они хранятся?

Хранятся в облаке (Google Account). При этом нужно учесть, что облако содержит намного больше информации, чем устройство.

Откуда их извлекают?

• Google Maps и My Places
• Фотографии: локальные (извлекаемые из устройства), извлекаемые из Google Photos
• Системные журналы: local (требуется root)
• Данные приложений: local (требуется root), cloud backups (ограниченно)

Как остановить отслеживание вашего местоположения

• Для любого устройства:
  - откройте веб-браузер, перейдите на myactivity.google.com, выберите «Элементы управления активностью» в раскрывающемся меню вверху слева и отключите «Активность в Интернете и приложениях» и «История местоположений»
• Для устройств Android:
  - Перейдите прямо к настройке «Безопасность и местоположение», прокрутите вниз до «Конфиденциальность» и нажмите «Местоположение». Теперь вы можете отключить его для всего устройства
  - Вы также можете использовать «Разрешения на уровне приложений», чтобы отключить доступ к различным приложениям
• Для устройств iOS:
  - если вы используете Карты Google, перейдите в *«Настройки»* → *«Конфиденциальность»* и установите для своего местоположения значение «Во время использования» приложения. Это предотвратит доступ приложения к вашему местоположению, когда оно не активно

История поиска YouTube

Используется как YouTube, так и другими сервисами. Вы можете как удалять историю вручную, так и автоматически через 3 месяца или 18 месяцев (по выбору).

История просмотров YouTube

Вы можете как удалять историю вручную, так и автоматически через 3 месяца или 18 месяцев (по выбору).

Однако если вы думаете, что это всё, вы ошибаетесь. На самом деле следить за вами можно с помощью использования идентификаторов устройств на Android. Поговорим о том, как ими злоупотребляют приложения, чтобы больше зарабатывать на рекламе.

Как приложения зарабатывают на рекламе

Для того, чтобы маркетологи могли составить на вас детальное досье и показать вам персонализированную рекламу, они собирают информацию о вас с помощью мобильных приложений. При этом отправляется даже та информация, использовать которую в рекламных целях Google не разрешает.

Какая информация позволяет отследить ваше Android-устройство

Что могут рассказать приложения рекламной сети о вашем устройстве? В первую очередь то, что они там установлены. Фактически, получив подобную информацию, можно сделать вывод о том, чем вы интересуетесь и какие объявления могут быть вам интересны. Например, если вы пользуетесь селфи-камерой, Instagram и Snapchat – вам покажут приложения с фильтрами и эффектами для фото.

Как убедиться, что то или иное приложение установлено именно на вашем устройстве? Для этого используются специальные коды-

идентификаторы. Как правило, их у смартфона, планшета и любого другого гаджета несколько, и большинство из них придуманы не для рекламы.

Например, уникальный номер IMEI нужен, чтобы распознавать ваш телефон в сотовых сетях и, например, блокировать краденые устройства. А при помощи серийного номера можно определить все гаджеты серии, в которых обнаружен брак, и отозвать их из магазинов.

Ещё один уникальный идентификатор – MAC-адрес – нужен для подключения устройства к сети, а заодно может быть использован, чтобы ограничить набор гаджетов, которые имеют право подключаться к вашему домашнему Wi-Fi. Наконец, Android ID (он же SSAID) разработчики приложений используют, чтобы продавать лицензии на ограниченное количество копий для платных версий своих продуктов.

Теоретически изменить эти номера можно, но стоит помнить, что для этого нужны root-права. А в некоторых странах смена IMEI запрещена законом.

Сменить Android ID проще – достаточно сбросить смартфон или планшет до заводских настроек. Но ведь потом придётся заново задавать все параметры, устанавливать приложения… Желающих это делать совсем не много.

Есть ли выход?

Ещё в 2013 году компания Google ввела специальный рекламный идентификатор. Его задают сервисы Google Play, и пользователь в любой момент может его сбросить и создать новый. Делается это в меню *Настройки → Google → Реклама → Сброс рекламного идентификатора*. С одной стороны, такой идентификатор позволяет рекламным сетям отслеживать привычки и увлечения владельцев устройств. С другой – если же хочется избавиться от слежки рекламщиков, вы можете в любой момент без лишних трудностей его сбросить.

По правилам магазина Google Play, в рекламных целях можно использовать только этот идентификатор. Площадка не запрещает связывать его с другими ID, но для этого приложению нужно получить согласие пользователя.

В теории это должно работать так: если вам нравится реклама по интересам, то вы не трогаете рекламный идентификатор и можете даже разрешить приложениям объединять его с чем угодно. Если же нет, то вы запрещаете связывать эту метку с другими и периодически сбрасываете её, таким образом отвязывая своё устройство от собранного на него досье.

Увы, в действительности всё несколько иначе. По правилам Google Play, в рекламных целях можно использовать только этот идентификатор. Приложение может связывать его с другими ID, но только с явного согласия пользователя.

Рекламный идентификатор – реальность

Как обнаружил исследователь Серж Эгельман (Serge Egelman), более 70% приложений в Google Play используют хотя бы один дополнительный идентификатор без предупреждения. Некоторые из них, например 3D Bowling, Clean Master и CamScanner, скачали многие миллионы человек.

Чаще всего в ход идёт Android ID, хотя IMEI, MAC-адреса и серийные номера разработчики тоже задействуют. Некоторые приложения отправляют партнёрам сразу три идентификатора и более. Так, игра 3D Bowling (видимо, для верности) использует и рекламный идентификатор, и IMEI, и Android ID.

Такой подход делает саму идею специального рекламного идентификатора бессмысленной. Даже если вы против слежки и регулярно сбрасываете его, маркетологи при помощи более стабильной метки легко привяжут к существующему профилю новый идентификатор.

Вместе с тем, начиная с Android Oreo, для каждого приложения задаётся свой Android ID. Однако для IMEI, серийных номеров и MAC-адресов ввести такую защиту нельзя.

Что же делать?

- Регулярно удаляйте программы, которыми вы не пользуетесь: чем меньше на устройстве приложений, тем меньше данных получат рекламные сети
- Не давайте оставшимся программам лишних разрешений. Это не избавит вас от слежки полностью, но не позволит тем же играм отправлять IMEI кому попало. На всякий случай: за этот идентификатор отвечает разрешение «Телефон». Оно же позволит приложению узнать ваш мобильный номер, посмотреть историю вызовов, позвонить (за ваш счёт, разумеется) и многое другое, так что выдавать его в принципе не рекомендуется.

Заключение

Как видно из приведённого в статье материала, вы можете настроить удаление хранимых данных, однако никто не может гарантировать что ваши данные не будут храниться или удаляться. Ведь основной бизнес Google – это торговля данными для показа рекламы.

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

ИТ-конкурс красоты

Beauty & DigITal

Всероссийский ежегодный конкурс красоты «Beauty & DigITal» среди девушек работающих в ИТ-сфере.

Миссия конкурса — определить самых красивых ИТ-девушек на звание Мисс «Beauty & DigITal» и сделать из обладательницы короны символ информационной безопасности России.

CIS Современные Информационные Системы

яИТы

www.cismiss.ru

Екатерина Данилова
Менеджер
по развитию бизнеса
Kaspersky Fraud
Prevention

Каким будет 2020 год для компаний с онлайн-сервисами в разрезе кибермошенничества

Онлайн-сервисы основательно проникли в нашу жизнь – сложно представить её без использования социальных сетей, мобильного банкинга, онлайн-покупок. Цифровое пространство настолько окутало своим удобством и доступностью, что о безопасности думаешь в последний момент. Именно поэтому бизнесу приходится принимать на себя этот удар и нести ответственность за сохранность личных данных своих клиентов, их денежных средств, накопленных баллов в программах лояльности.

Прошлый год можно назвать годом, в котором мошенники сделали очередной шаг в совершенствовании своих инструментов. Развивались технологии по созданию ботов «нового поколения», поведение которых с помощью тонкой настройки становится совсем неотличимо от человеческого. Если раньше компьютерным программам предписывалось следовать линейно и топорно, то усовершенствованные боты отклоняются от прямой линии, «трясут» мышкой и показывают свойственную людям скорость передвижения курсора. Такой бото-человек позволяет массово скупать билеты на спортивные турниры или обогащаться за счёт программ лояльности интернет-магазинов.

Также в 2019 году расширился спектр применяемых методов «социальной инженерии». Согласно статистике, практически каждый десятый россиянин (9%) потерял крупную сумму денег в результате телефонного мошенничества[1]. Для обмана физических и юридических лиц сервисов дистанционного банковского обслуживания использовались не только фишинг, грамотные скрипты разговора «якобы специалистов по безопасности банка» и вредоносное программное обеспечение для перехвата кодов из СМС-сообщений для двухфакторной аутентификации, но и программы удалённого управления (RAT, или Remote Access Tools: TeamViewer, AnyDesc), интерактивное голосовое меню (IVR) с целью получения второго фактора аутентификации, подмена номеров IP/SIP телефонии на красивые и похожие на номера доверенной финансовой организации.

По данным команды Kaspersky Fraud Prevention «Лаборатории Касперского», одной из наиболее распространённых схем мошенничества в 2019 году было использование приложений для удалённого доступа. При проведении такой атаки пользователи полагают, что им звонит сотрудник банка с предложением помочь уменьшить расходы на обслуживание карты или сообщает о попытке взлома аккаунта. Далее клиенту предлагается установить на мобильное устройство приложение, которое позволит мошеннику получить удалённый доступ к устройству. После того, как пользователь установил приложение на своё мобильное устройство, кибермошенник получает доступ ко всем возможностям учётной записи пользователя. Он может переводить и снимать средства, изменять данные учётной записи, похищать личные данные с целью их дальнейшей продажи, подавать заявки на кредиты и многое другое.

Более того, RAT активно применяется для подмены платёжных поручений в системах ДБО для юридических лиц, даже если пользовательская сессия легитимна и используется программно-аппаратный токен для входа в систему. Хотелось бы сказать, что ни один бухгалтер не пострадал при такой схеме мошенничества. Однако, увы, статистика говорит об обратном.

В 2020 сохранятся эти тенденции, но появятся и новые вызовы для департаментов ИБ и ИТ, разработчиков веб- и мобильных приложений, специалистов, отвечающих за развитие цифровых каналов. Кибермошенников всё так же будет привлекать финансовая выгода от кражи банковских аккаунтов, перепродажи бонусов, миль, товаров, купленных на средства или баллы со счёта пользователя онлайн-магазина. Отдельные кибергруппировки будут продолжать эксплуатировать цифровые каналы обслуживания для отмыва-

1. Данные получены в результате исследования, проведённого в июне 2019 года компанией OMI по заказу «Лаборатории Касперского». В ходе исследования было опрошено 1000 россиян.

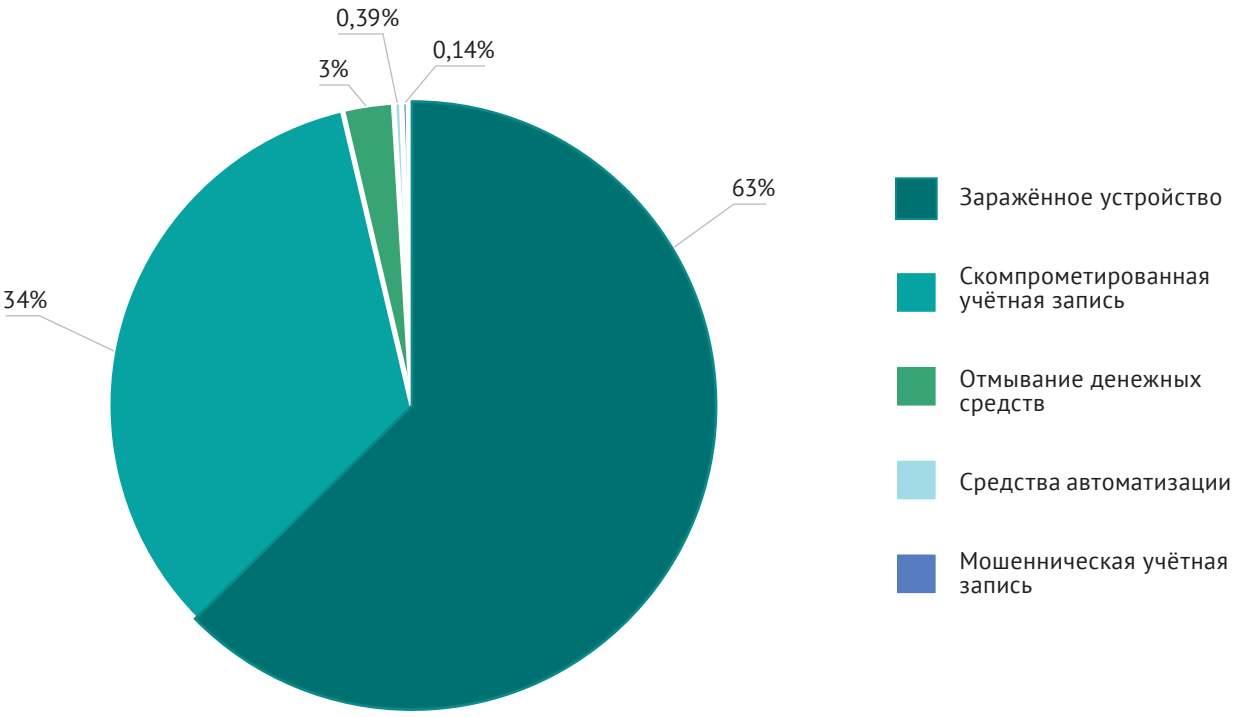


Рисунок 1. Статистика по инцидентам онлайн-мошенничества на веб- и мобильных каналах по данным системы Kaspersky Fraud Prevention.

ния денежных средств, связанных с выводом похищенных средств, уходом от налогообложения, отмыванием доходов, полученных преступным путём. По нашим данным, на инциденты, связанные с отмыванием денежных средств, пришлось 3% атак. Эта цифра, сама по себе небольшая, является показательной, поскольку количество таких попыток выросло по сравнению с 2018 годом почти на 182%. Этот рост объясняется сокращением количества банков, повышением доступности инструментов мошенничества, а также многочисленными утечками данных, в результате которых злоумышленники легко находят в сети огромное количество интересующей их информации (рис. 1).

В новом году появятся и новые тенденции. Это касается в том числе инструментария и методов, которые мошенники активно берут на вооружение. Давайте рассмотрим несколько предсказаний на 2020 год от «Лаборатории Касперского», в частности экспертов команды Kaspersky Fraud Prevention, к чему должны быть готовы компании в разрезе предотвращения мошенничества на их цифровых каналах обслуживания.

Тренд № 1. FaaS – мошенничество как сервис

Набирает популярность такой вид услуг как Fraud as a service, когда любой желающий без специальной технической подготовки за определённую плату может получить набор инструментов для взлома, базы с краденными банковскими данными, персональными данными, тренинги и консультации по обходу защитных систем и не только. Цифровая трансформация многих секторов экономики – электронной коммерции, государственных сервисов, банковских услуг – подтолкнёт дальнейшее развитие FaaS-концепции. Прогнозируется рост количества поставщиков подобных услуг и расширение портфеля услуг. Мы уже наблюдаем развитие рынков цифровых отпечатков устройств (device fingerprint), совершенствование анонимайзеров и ботов, новые подходы в применении социальной инженерии.

Тренд № 2. Перепродажа доступа к банковскому аккаунту

Зачастую жертвами целенаправленных атак становятся небольшие банки и финансовые организации, недавно купленные крупными игроками и приводящие свои системы безопасности в соответствии со стандартами новых штаб-квартир. Анализируя форумы и чат-мониторинги в даркнете в прошлом году, специалисты «Лаборатории Касперского» наблюдали случаи, когда группы, специализирующиеся на целенаправленных атаках на финансовые учреждения, появлялись в сетях жертв после вторжений других групп, которые специализируются на продаже доступа rdp / vnc, таких как FXMSP и TA505.

В этом году активность групп, продающих сетевой доступ, повысится в регионах Африки и Азии, а также в Восточной Европе.

Тренд № 3. Агрессивные «целевые» программы-вымогатели, написанные под банки

В случае, когда киберпреступники понимают, что перепродать доступ не удастся или низкая вероятность возможности обналичить деньги, то выходом для получения финансовой выгоды выступает использование программ-вымогателей. Важно отметить, что последние годы мы наблюдали снижение количества массовых атак, проводимых с помощью универсальных программ-вымогателей, и тенденцию на проведение направленных атак с конкретными мишенями. Злоумышленники становятся более избирательными и останавливают своё внимание на организациях, готовых заплатить значительные суммы, чтобы восстановить данные. К таким организациям относятся банки, крупные предприятия, энергетические компании, простой рабочих процессов и репутация на рынке которых стоит дорого.

В будущем, по нашему мнению, «целевые» атаки будут всё агрессивнее. Возможно также, что вместо блокировки файлов злоумышленники начнут угрожать публикацией конфиденциальной информации.

Кроме того, злоумышленники продолжат попытки выйти за рамки компьютеров, серверов и мобильных устройств, масштабируя свои атаки для монетизации доступа к «умным» устройствам: смарт-ТВ, часы, машины, дома, города и прочим элементам, подключённым к интернету.

Тренд № 4. Фокус на мобильные атаки и трояны мобильного банкинга

Предсказания о росте числа атак на мобильные устройства повторяются из года в год. Это не удивительно, ведь всё чаще пользователи выполняют задачи именно на своём «карманном помощнике», и, как следствие, на мобильных девайсах хранится всё больше и больше данных. С каждым годом мы видим, как злоумышленники продвигаются в направлении развития мобильных атак.

Однако наши исследования и мониторинг подпольных форумов позволяют предположить, что исходный код некоторых популярных троянов мобильного банкинга уже попал в открытый доступ. Учитывая популярность таких троянов, мы ожидаем повторения ситуации, когда произошла утечка исходного кода троянов ZeuS и SpyEye: количество попыток атаковать пользователей в разы увеличится, а география атак расширится почти до каждой страны в мире.

Тренд № 5. Утечки чувствительных пользовательских данных и применение deepfake

Объёмы хранящихся личных данных на различных онлайн-сервисах постоянно растут. К сожалению, нередки случаи утечек этих данных в больших количествах. В 2019 году в СМИ не было и месяца без новости о крупной утечке в банках, телеком-провайдерах, сетях отелей, авиакомпаниях как по всему миру, так и в России, и СНГ. Однако сейчас ситуация осложняется тем, что возникает опасность утечек особо чувствительных данных, в частности биометрических. Случаи создания подделок с помощью нейросетей – так называемых, deepfake[2] – повышают вероятность инцидентов. Deepfake может использоваться для замены элементов изображения на желаемые образы как в фото-, так и видео-форматах. Эта технология уже используется; рано или поздно злоумышленники начнут её эксплуатировать.

Заключение

Разумеется, точно спрогнозировать, что конкретно случится в будущем невозможно. Специалисты по безопасности могут лишь регулярно проводить мониторинг текущей ситуации, анализировать действия киберпреступников и вредоносных кампаний (не только в своей компании, но и за её пределами), понимать используемые ими методы и возможные последствия и принимать соответствующие меры в рамках комплексного подхода к защите онлайн- и мобильных сервисов. Лучший подход – хорошая стратегия кибербезопасности, основанная на здравом смысле и заложенная в архитектуру сервиса на первоначальном уровне, а также применение технологий защиты от доверенных поставщиков решений и услуг.

Полный список предсказаний на 2020 год и отчёт об основных угрозах кибермошенничества за период январь-декабрь 2019 с акцентом на сценариях в банковском секторе и электронной коммерции вы найдёте по ссылке: www.kaspersky.ru/fraud-prevention-report-2019.

2. Сочетание слов «глубинное обучение» (англ. Deep learning) и «подделка» (англ. Fake), методика синтеза изображения, основанная на искусственном интеллекте.

Екатерина Данилова
Менеджер по развитию бизнеса
Kaspersky Fraud Prevention

kaspersky

***«Лаборатория Касперского»** – международная компания, работающая в сфере информационной безопасности.*

www.kaspersky.com

kfp.kaspersky.com/ru

Российские ИТ-эксперты о «горячих» технологиях на 2020 год

«Горячими» технологиями в 2019 году были 5G, Wi-Fi 6, квантовые вычисления, искусственный интеллект, цифровая трансформация и некоторые другие. Консалтинговые компании охотно делали глобальные прогнозы по развитию этих направлений. Редакция CIS опросила отечественных ИТ-директоров и экспертов, чтобы составить представление о развитии «горячих» технологий именно в России.

Виталий Мосеев,
ИТ-журналист.

В 2019 году в мире активно обсуждали как развитие хорошо знакомых технологий, так и тех, с которыми российским предприятиям предстоит столкнуться. Например, 5G активно шагала по планете, но в корпоративных целях частную сеть 5G в России построили в январе 2020 года. Отечественные компании в 2019 году продолжали экспериментировать с блокчейном, а в 2020 году они вполне смогут испытать квантовые технологии. Российские эксперты говорят, что развитие уже знакомых технологий откроет для предприятий новые возможности.

5G и Wi-Fi 6 дополнят друг друга

В 2019 году сети 5G заработали в нескольких городах США, Китая и Европы. Тогда, по оценкам Juniper Research, к новой технологии подключилось 5 млн пользователей, а к 2025 году количество соединений 5G достигнет 1,5 млрд.

К концу 2019 года около 40 сетей в 22 странах подключали абонентов к 5G. В 2020 году уже 125 операторов предложат 5G-сервисы, прогнозирует Кестер Манн, директор направления «Потребители и связь» компании CCS Insight.

Услугами нового поколения воспользовались предприятия. В январе 2020 года китайская компания ZTE организовала при помощи 5G телемедицинскую связь между больницами и медицинскими центрами. Технологии обеспечат повышенную безопасность для лечащих врачей в условиях неясности условий для передачи коронавируса. В конце января в России на предприятии «КамАЗ» запустили первую частную промышленную сеть 5G. К ней подключат системы видеонаблюдения, организуют удалённое обучение сотрудников с использованием виртуальной и дополненной реальности.

В 2019 году предприятиям стала доступна ещё одна технология – Wi-Fi 6. Стандарт утвердили в августе, а первые устройства стали появляться недавно. К 2024 году, по данным ABI Research, на Wi-Fi 6 придётся более половины устройств в семействе Wi-Fi. Для предприятий новая технология – это хорошая возможность подключить тысячи устройств к одной сети и обеспечить каждому оптимальную скорость.

По оценке IDC, 5G и Wi-Fi 6 будут дополнять друг друга, а не конкурировать между собой. Возможно, эти две технологии получат бесшовную интеграцию. По мнению российских экспертов, 5G и Wi-Fi 6 окажут наибольшее влияние на телеком-рынок на горизонте 5-10 лет.

В 2020 году в России будут доминировать сети 3G/4G и стандарты Wi-Fi ниже шестого. Эти технологии не исчерпали свой потенциал. Полноценные коммерческие сети 5G могут появиться только в 2021 году, полагает **Александр Рожков**, директор управления продаж сервисов компании Softline. «2020 год пройдёт под эгидой урегулирования технологических подходов к созданию сетей и сервисов на основе 5G. Необходимо разрешить вопросы обеспечения информационной безопасности, расширения географии пилотных сетей, а также разработки отечественных платформ и оборудования в соответствии с концепцией OpenRAN и дорожной картой развития сетей 5G», – отметил он.

От внедрения 5G в России выиграют многие отрасли, рассказал **Владимир Шапоров**, руководитель направления Центра развития телекоммуникационных решений компании «Техносерв». «5G позволит фактически предугадывать потребности абонентов. Появятся новые сценарии для промышленности и IoT в банковской сфере, ритейле, медицине, сельском хозяйстве и т.д.»

2020 год станет переломным для квантовых вычислений

2020 год – это переломный момент для квантовых технологий: они станут доступны бизнесу. В этом уверены эксперты CB Insights. «В 2020 году крупнейшие ИТ-компании продолжат показывать, как применять такую технологию на практике. Нам ещё предстоит увидеть потенциал её вычислительных возможностей для решения реальных проблем», – соглашается **Калян Кумар**, технический директор HCL Technologies.

Квантовые компьютеры пригодятся предприятиям для быстрого отсеивания больших наборов данных. Например, многие приложения на базе искусственного интеллекта для бизнеса могут работать быстрее, надо только применить квантовые вычисления.

По оценкам Markets&Markets, объём глобального рынка квантовых вычислений вырастет с $93 млн в 2019 году до $283 млн в 2024 году. Поддержать становление российского рынка планируется инвестициями в 23,7 млрд рублей до 2024 года. Об этом в минувшем декабре рассказали в Росатоме, отвечающем за разработку дорожной карты по развитию квантовых технологий.

Пока же рынок квантовых вычислений находится «на низком старте», считает **Дмитрий Рогов**, директор по технологическому развитию компании «АйДи – Технологии управления». «Ведущие ИТ-компании уже сегодня активно работают с абстрактными моделями квантового процессора с помощью прототипов соответствующих языков программирования. Думаю, в 2020 году вполне может произойти переход от прототипирования к первым этапам прикладной разработки в квантовой перспективе. Это приведёт

к росту спроса на программистов с соответствующими компетенциями», – считает он.

«Ожидается, что наибольшее количество программистов, которые будут их использовать, придёт из сферы Data Science, так как у них уже частично есть необходимая математическая подготовка. Наибольший эффект от квантовых вычислений ожидается в сфере искусственного интеллекта», – прогнозирует **Сергей Ширкин**, декан факультетов искусственного интеллекта и аналитики Big Data в GeekUniversity.

90% корпоративных приложений оснастят искусственным интеллектом

59% респондентов внедрили технологии искусственного интеллекта (AI) и машинного обучения, сообщали в 2019 году аналитики Gartner. К 2025 году не менее 90% новых корпоративных приложений будут использовать AI, считают в IDC.

Технологии AI год от года во всём мире становятся лишь доступнее, подтверждают эксперты. «Создаются нишевые инструменты с искусственным интеллектом. Ранее такое было невозможным из-за высокой стоимости и недостатка данных. Искусственный интеллект применят во многих новых продуктах. Технология, наример, улучшит качество изображения видеокамер и мониторов, повысит эффективность работы устройств. Элементы AI будут широко применяться для обеспечения кибербезопасности для поиска новых точек атак», – рассказал **Макс Литвин**, соучредитель Grammarly.

Наиболее востребованной в России остаётся аналитика больших данных, считает **Иван Прошин**, ведущий специалист data science в Bell Integrator, д. т. н. «Продолжится развитие видеотехнологий, разработка и практическое применение видеокамер со встроенным интеллектом. Расширится применение искусственного интеллекта в реальном секторе производства. Темпы роста рынка AI-решений в 2020 году, скорее всего, будут одними из самых высоких. Положительно на развитии рынка искусственного интеллекта в России может сказаться и принятая в стране стратегия развития искусственного интеллекта», – комментирует он.

Высоким спросом в ближайшие несколько лет у заказчиков будут пользоваться проактивные и комплексные системы с технологиями AI, сочетающие в себе широкий функционал: видеонаблюдение, охранная сигнализация, контроль доступа, противопожарная защита, бизнес-аналитика и т. д. «Проактивные и комплексные системы особенно эффективны для раннего реагирования на события, предупреждения инцидентов благодаря мгновенному анализу данных, получаемых из разных источников. Также растёт экономический эффект», – считает **Антон Голубев**, директор департамента управления проектами Hikvision Russia.

«Но рост реального объёма рынка в России сдерживается отсутствием достаточного количества квалифицированных специалистов, высоким порогом входа и относительно небольшим количеством законченных индустриальных решений. Ситуация должна значительно улучшиться в 2020 году», – прогнозирует **Иван Кровяков**, менеджер по развитию бизнеса Huawei Enterprise в России.

Цифровизация предприятий обеспечит 52% мирового ВВП

К 2023 году более половины (52%) мирового ВВП придётся на предприятия с цифровой трансформацией, подсчитали в IDC. Обеспечение цифрового превосходства – это слишком дорогое мероприятие. Компания должна направлять на поддержку цифровых инноваций около половины своего бюджета, полагают эксперты.

В России многие предприятия вкладываются в цифровизацию. Например, Магнитогорский металлургический комбинат с 2020 по 2024 годы инвестирует в цифровые проекты 5 млрд рублей (это 2% от капитальных затрат), а в итоге рассчитывает получить дополнительную прибыль в 6,2 млрд рублей.

«Во многих крупнейших российских компаниях и государственных структурах запрос на изменения в работе на основе ИТ в 2019 году отразился на организационной структуре и распределении бюджетов между CIO и CDO. При этом в разговорах чаще всего всплывало желание руководителей не просто увеличить степень оцифровки внутренних процессов организаций, повысить скорость принятия решений и качество управленческой отчётности, но и выделить полученные результаты в новые услуги для рынка: «открытые данные», партнёрские экосистемы на основе API и маркетплейсы. В 2020 году произойдёт дальнейшее развитие этих трендов, усиленное и подкреплённое поддержкой со стороны государства в рамках национальной программы «Цифровая экономика», – считает **Иван Кровяков**.

Продолжится развитие технологий, связанных с обеспечением цифровой непрерывности (Digital Continuity). Они объединяют реальный мир проектирования и производства с виртуальным миром цифровых технологий. «Такие технологии позволяют проектировать, управлять и обоснованно выбирать оптимальные решения в единой цифровой среде. Цифровая информационная модель становится всё более востребована. Заказчикам нужен не только произведённый и построенный объект. Теперь вместе с ним необходимо представить его цифровую модель, которая будет использоваться на протяжении всего жизненного цикла. Продолжат активное расширение рынок и спектр применения аддитивных технологий», – прокомментировал **Андрей Бубнов**, начальник отдела центра отраслевой экспертизы компании «Техносерв».

Ценность блокчейна оценили в $1,55 трлн.

К 2023 году только 10% компаний в мире добьются радикальной трансформации с использованием блокчейна. К 2025 году технология может принести деловую ценность в размере $1,55 трлн. Об этом сообщали аналитики Gartner.

Они считают: ИТ-директора скоро убедятся, что с помощью технологии можно проследить активы до их происхождения. Это сократит возможности замены подлинных товаров контрафактом и способствует большему доверию.

По оценкам Mindsmith, в России в первом полугодии 2019 года количество корпоративных блокчейн-проектов в России выросло на 45% по срав-

нению с 2018 годом. Перспективными направлениями для применения технологии (за исключением криптовалюты) эксперты назвали сектора с обширной документацией, таких как платежи, страхование, здравоохранение и финансы.

Выходу на масштаб текущим блокчейн-проектам в России, по мнению **Дениса Реймера**, вице-президента ЛАНИТ по цифровой трансформации, руководителя интегратора цифровых экосистем DTG, мешают три фактора:

- проблемы с мотивацией участников (чьи интересы нужно принимать во внимание, когда речь идёт о совместном управлении данными и ресурсами);
- вопросы конфиденциальности данных и соблюдение требований к информационной безопасности внутри каждой организации-участника (это очень актуально для уровня enterprise);
- ожидание готовности законодательной базы, то есть гарантий легальности операционной деятельности участников с использованием блокчейн (особенно в сфере движения документов).

В 2019 году в России не было громких прорывов, но интерес к технологии подогревался успешными зарубежными примерами. «Иностранный опыт показал: более перспективны проекты, запускаемые и поддерживаемые консорциумами компаний. В России примеров формирования подобных работающих блокчейн-консорциумов почти нет. И создание подобных консорциумов сильным отраслевым игроком или государством может стать в 2020 году драйвером рынка блокчейн-проектов», – полагает **Дмитрий Петров**, генеральный директор компании «Кометрика».

Дмитрий Паршин, директор центра разработки компании Artezio, предположил, что крупные государственные заказчики не будут настаивать на применении блокчейна в глобальных проектах, связанных с обеспечением безопасной записи и хранения данных. «Также следует учитывать расширение действия норм и регламентов по обработке персональных данных. При условии, что пользователи должны иметь возможность удалять данные, использование блокчейн теряет смысл во многих проектах, на которые влияют упомянутые регламенты», – отметил эксперт.

Эксперты ждут перехода к распределённому облаку

К 2023 году предприятия разработают и развернут более 500 млн цифровых приложений и служб с использованием облачных подходов, прогнозируют в IDC. Многие компании, по оценке Gartner, перейдут от централизованного к распределённому публичному облаку. Такая трансформация откроет новую эру облачных вычислений. Что касается российского рынка облачных услуг, то к 2023 году его объём достигнет 196 млрд рублей (против 86 млрд рублей в 2019 году). Среднегодовой темп прироста рынка составит 23,5%. Такие оценки приводит iKS-Consulting.

«Для российского рынка сейчас актуальны облачные хранилища данных и облачные сервисы, особенно при неимении собственной инфраструктуры или желании на ней сэкономить. При работе с персональными данными воспользоваться зарубежными облачными сервисами невозможно по причине законодательного запрета размещения персональных данных на серверах за рубежом. Сейчас такие сервисы развивают крупные российские ИТ-компании. Ожидается, что многие компании будут их тестировать и постепенно переходить к использованию», – рассказал **Сергей Ширкин**, декан факультетов искусственного интеллекта и аналитики Big Data в GeekUniversity.

При этом сохранится консервативное отношение к облачным сервисам у госсектора и военной промышленности. Но всё больше заказчиков с консервативным подходом переносят часть сервисов в гибридные среды, замечает **Юрий Новиков**, руководитель направления развития облачных технологий Softline. «Ещё одна тенденция – это интерес вендоров к предоставлению сервисов в режиме единого окна. На это сейчас ориентируются все крупные компании-разработчики (VMWare, Google, IBM, Microsoft и другие). Заказчик должен получать всё, что ему необходимо, посредством решений одного вендора, например: сервисы виртуализации, бэкапа, различные сетевые решения. Набирают популярность также так называемые «панели оркестрации», когда через панель одного оператора клиент подключается к облакам разных провайдеров и выстраивает мультиоблачность», – добавил эксперт.

Рынок Интернета вещей наполняется устройствами

Gartner прогнозирует, что в 2020 году к IoT будет подключено 5,8 млрд точек (+21% по сравнению с 2019 годом). Крупнейшие сценарии использования в 2020 году следующие: интеллектуальный учёт (1,17 млрд устройств), безопасность зданий и наблюдение (1,09 млрд). По оценкам IDC, объём российского рынка Интернета вещей в 2019 году достиг $3,7 млрд. При этом более 50% компаний внедрили или планируют в течение 12 месяцев завершить проекты, в которых используется IoT. Эксперты считают, что ускорит этот процесс стандартизация. Так, в январе 2020 года в России разработаны проекты национальных стандартов в сфере IoT.

Директор по развитию ООО компании «Кометрика» **Дарья Котлярова** рассказала, что основными отраслями для внедрения IoT остаются транспорт, товарное и технологическое производство. Но сфера учёта ресурсов – «умных» счётчиков и платформ мониторинга в ЖКХ – пока очень консервативна и не отличается особой динамикой. «Этот фактор не помешает раскачивать рынок ЖКХ пилотными проектами цифровых кварталов, интеллектуальных энергосистем, наружного освещения и стационарного видеонаблюдения. Очевидным витком развития рынка IoT в 2020 году мы видим в серии объединений и поглощений среди отечественных игроков», – добавила эксперт.

«Прорыв в Интернете вещей произойдёт, когда будут выработаны единые стандарты его внедрения. Это возможно только с участием крупных компаний-разработчиков. Немаловажную роль играют успешные бизнес-кейсы, на основе которых представители бизнеса будут решать, какую выгоду им принесёт такое внедрение», – подытожил **Сергей Ширкин**.

Виталий Мосеев
ИТ-журналист.
Автор телеграм-канала @iotdaily.
Телеграм @vitalii_mo,
vitalik@Ymail.com

Музей МГТУ им. Н. Э. Баумана

В МГТУ имени Н. Э. Баумана есть исключительное место, вместившее в себя всю его многолетнюю историю, традиции. Это музей, который по праву можно назвать душой и сердцем ВУЗа. Здесь удивительным образом удалось сберечь наследие десятков поколений выдающихся выпускников знаменитого во всём мире святилища науки и техники.

Действительно, почти вся история МГТУ – основателя фундаментальной инженерной школы в России – представлена в его музее, который 6 ноября 2017 отметил своё 50-летие. Между тем, история музея имеет гораздо более глубокие корни.

История музея МГТУ имени Н.Э. Баумана

Предлагаем совершить увлекательный исторический экскурс вместе с редакцией журнала CIS (Современные Информационные Системы). Тем более, что не так давно нам посчастливилось лично побывать в музее МГТУ им. Н.Э. Баумана в г. Москве и поверьте, нам есть что вам рассказать.

А начнём с того, что впервые о тогда ещё техническом музее машиностроения упоминается в издании «Известия Императорского московского технического училища» выпуска 1905 года. В те времена музей преимущественно служил хранилищем для прототипов деталей, всевозможных конструкций. Курировал его А.И. Сидоров – русский и советский учёный-механик, заслуженный деятель науки и техники РСФСР, профессор, специалист в области инженерного проектирования. Музейные экспонаты профессор часто использовал в качестве наглядного пособия, демонстрируя своим студентам на лекциях.

Коллекция экспонатов увеличивалась, как и интерес к музею, поэтому уже в 1920-30-х годах функционировало три технических музея при кафедрах на базе университета. Это были узкопрофильные экспозиции, которые, тем не менее, вызывали неподдельный интерес у гостей и студентов университета.

1995 год ознаменовался не только 165-летием МВТУ, но и организацией первой масштабной выставки музея.

Историческое событие произошло также и 18 ноября 1967 года. По приказу Минвуза СССР в этот день состоялось торжественное открытие музея истории МВТУ имени Н.Э. Баумана. В «Книге почётных гостей» до сих пор хранится запись-пожелание одного из лучших студентов, окончивших МВТУ – лётчика-космонавта К.П. Феоктистова. В ней он ещё раз напомнил о том, как важно ценить и помнить пройденный путь и выразил надежду на процветающее будущее музея. Как видим, его слова оказались пророческими.

Руководство

Впрочем, сложно представить другую судьбу для музея, который возглавляли поистине выдающиеся деятели науки.

Больше 40 лет главой Совета музея выступал академик РАН, советский и российский учёный, работающий в сфере механики и ракетостроения – Константин Сергеевич Колесников (27 декабря 1919-13 мая 2016).

С 1969 по 1998 годы музеем руководила заслуженный деятель культуры РФ, его основатель и первый директор – Галина Николаевна Анцупова (6 ноября 1939-4 февраля 1998). Этот период с полной уверенностью и без тени сомнения можно считать наиболее продуктивным. Благодаря усилиям Галины Николаевны и её высокой самоотдаче музей постепенно превратился в один из лучших технических музеев России.

С 1998 года музей возглавляет Галина Алексеевна Базанчук.

Выставочные экспонаты

Основная экспозиция расположилась на территории двух просторных залов площадью около 450 квадратных метров.

В 1992 году для посещения был открыт первый экспозиционный зал, а спустя восемь лет, 21 ноября 2000 года произошло открытие второго выставочного зала. Событие приурочили к 170 годовщине основания Университета. Почётное право первым ознакомиться с экспозицией второго зала было предоставлено Президенту РФ.

Нужно сказать, что со дня создания и по сегодняшний день экспозиция музея успела несколько раз поменяться. Однако неизменно её лейтмотивом остаётся история развития МГТУ от организации в 1930 году Московского ремесленного учебного заведения – МРУЗа до первого в России технического университета. Как говорят сами сотрудники музея, их цель – продемонстрировать всем гостям без исключения, что выпускники Университета МГТУ всегда выбирали активную государственную позицию и никогда не оставались в стороне от происходящих в стране событий.

Прогуливаясь по залам музея, понимаешь, что это не просто слова из презентации экспонатов членами рабочего коллектива. Несомненно, каждый экспонат демонстрирует свою причастность к процессу становления отечественной высшей школы, к развитию российской науки, техники и промышленности в целом.

Экспозиции

Сокровищница музейных экспонатов содержит свыше 10 тысяч уникальных экземпляров, отражающих не просто историю науки и техники, а её глубочайший нравственный и, что особенно значимо, человеческий потенциал. Один только книжный фонд насчитывает близко 3 тысяч изданий! Раритетные фолианты, уникальные литографированные учебники конца XIX века, первые отечественные учебные пособия по таким точным наукам как кибернетика, ракетостроение, машиностроение.

В коллекции музея присутствуют экспонаты с присвоенным статусом памятников науки и техники I категории. Так, памятником I ранга признана дипломная работа студента Николая Алексеевича Пилюгина – будущего «ракетного» академика АН СССР. Дипломным проектом Николая Алексеевича стал авиационный прибор – «Жирограф». Почти полвека он служил верой и правдой в ЦАГИ (Центральный аэрогидродинамический институт им. профессора Н.Е. Жуковского) при лётных испытаниях. Нужно ли говорить о колоссальной важности этой работы для развития ракетной техники и авиации в России, а возможно и мире? Уверены, что нет.

Одно из главных достояний музея – подлинные вещи, принадлежавшие выдающимся выпускникам и преподавателям МГТУ, любезно переданные в дар музею их родными и близкими.

Внимательный, заинтересованный зритель непременно обратит внимание на ценный экспонат в центре первого зала – скафандр, принадлежавший советскому лётчику-космонавту, почётному выпускнику университета Владимиру Алексеевичу Соловьёву. Именно в нём Владимир Алексеевич совершил два полёта на станциях «Салют-7» и «Мир» в период с 1984 по 1986 гг.

Уникальную возможность воочию увидеть главные вехи становления российской космической инженерии открывает коллаж, составленный из макетов-прототипов космических установок, размещённых по мере совершенствования от первого искусственного спутника Земли до советской орбитальной станции «Салют-6» – «Союз».

В музее представлены портреты тех, кто стоял у истоков создания известной во всём мире так называемой «русской» системы высшего технического образования. Здесь же представлены портреты их талантливейших потомков, воспитанников новой системы – основоположника гидро- и аэродинамики Н.Е. Жуковского, одного из главных создателей советской ракетно-космической техники С.П. Королёва.

Ничто не забыто, и никто не забыт...

Большое уважение и восхищение вызывают экспозиции, посвящённые неоценимому вкладу воспитанников вуза, педагогов в Великую Победу. Члены 7-й Бауманской дивизии народного ополчения принимали активное участие в сражениях Великой Отечественной войны и проявили свои лучшие патриотические качества. Участники 3 Коммунистической дивизии помогали в сооружении защитного форта для обороны Москвы.

Заметная часть разделов экспозиции знакомит посетителей с разработками в сфере вооружения, боевого оснащения, спецтехники, повествует о создании «самолётов Победы». Перед училищем стояла важнейшая, первоочередная на тот момент задача подготовки технических кадров для оборонной промышленности. Сразу после начала войны здесь в экстренном порядке начали работу дополнительные специализированные артиллерийский, танковый факультеты и факультет боеприпасов.

Вниманию гостей также представлены археологические памятники, обнаруженные группами студентов по программе «Поиск» во время раскопок на местах сражений на окраине города Вязьма с непосредственным участием Бауманской дивизии. К сожалению, большая часть бойцов погибла в этих кровопролитных жестоких боях первого периода войны, не вернувшись домой к родным.

Заслуженное признание

Растёт не только коллекция экспонатов, но и география музея. Филиалы учреждения принимают гостей в Мытищах, в городе Калуге.

Сегодня музей МГТУ имени Н.Э. Баумана заслуженно признан лучшим показательным музеем технических вузов и гордо именуется просветительским научно-исследовательским учреждением. Трудно переоценить его огромный вклад в становление культурных традиций университета, который, как показало время, стал alma mater для целой плеяды выдающихся учёных и инженеров нескольких поколений.

За годы существования музей получил множество наград, дипломов, регулярно становился призёром городских смотров-конкурсов города Москвы, отмечен почётными грамотами, благодарственными письмами, награждён медалью ЮНЕСКО, удостоен звания «Народного музея». И это далеко не все награды и достижения!

Редакция журнала CIS (Современные Информационные Системы) с большим интересом и удовольствием посетила Бауманский музей и настоятельно рекомендует всем последовать нашему примеру. Обязательно выделите время и отправляйтесь на экскурсию в музей с друзьями, семьёй, а если окажется не с кем, смело идите в одиночку. Время совершенно точно будет потрачено не зря!

Мы в свою очередь желаем музею МГТУ имени Н.Э. Баумана дальнейшего развития и процветания. Мы верим, что ещё ни одно поколение неравнодушных к технической истории России людей откроет двери поистине бесценной сокровищницы нации.

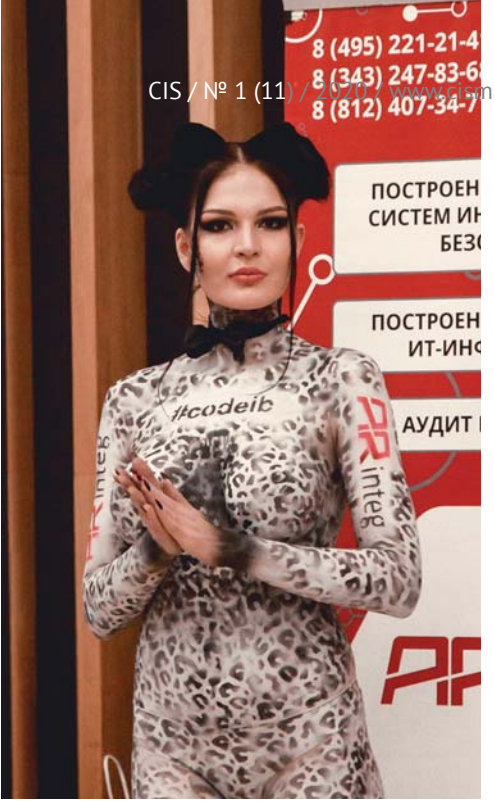

Инженерные
решения


#soctorum
CIS
Современные Информационные Системы
«Мобильная» электронная подпись
В «Сколково» объявили победителей

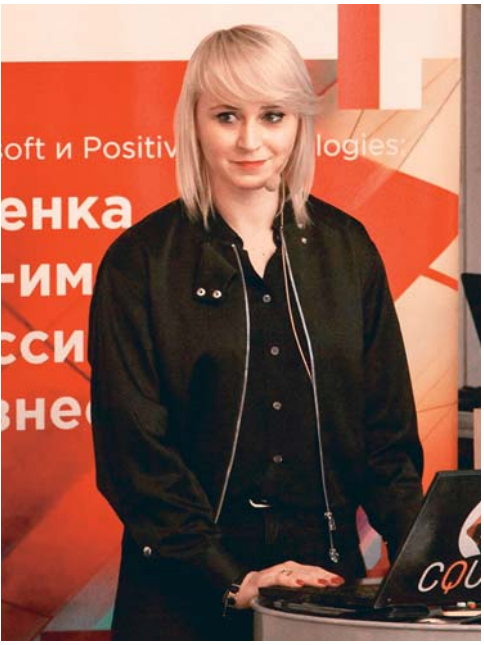

ДАННЫЕ
ПЕРСОНАЛ
ТЕХНОЛОГИИ


#socforum

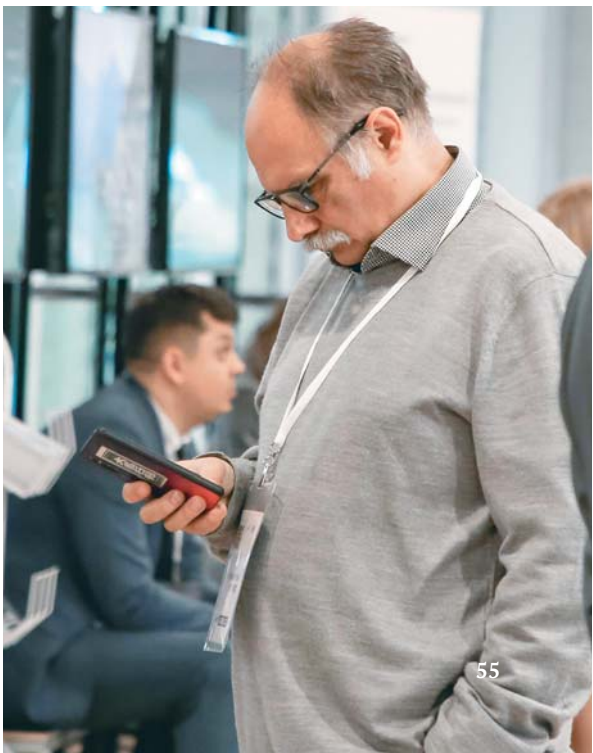

erART
ПОЛНЫЙ СПЕКТР
КИБЕРБЕЗОП

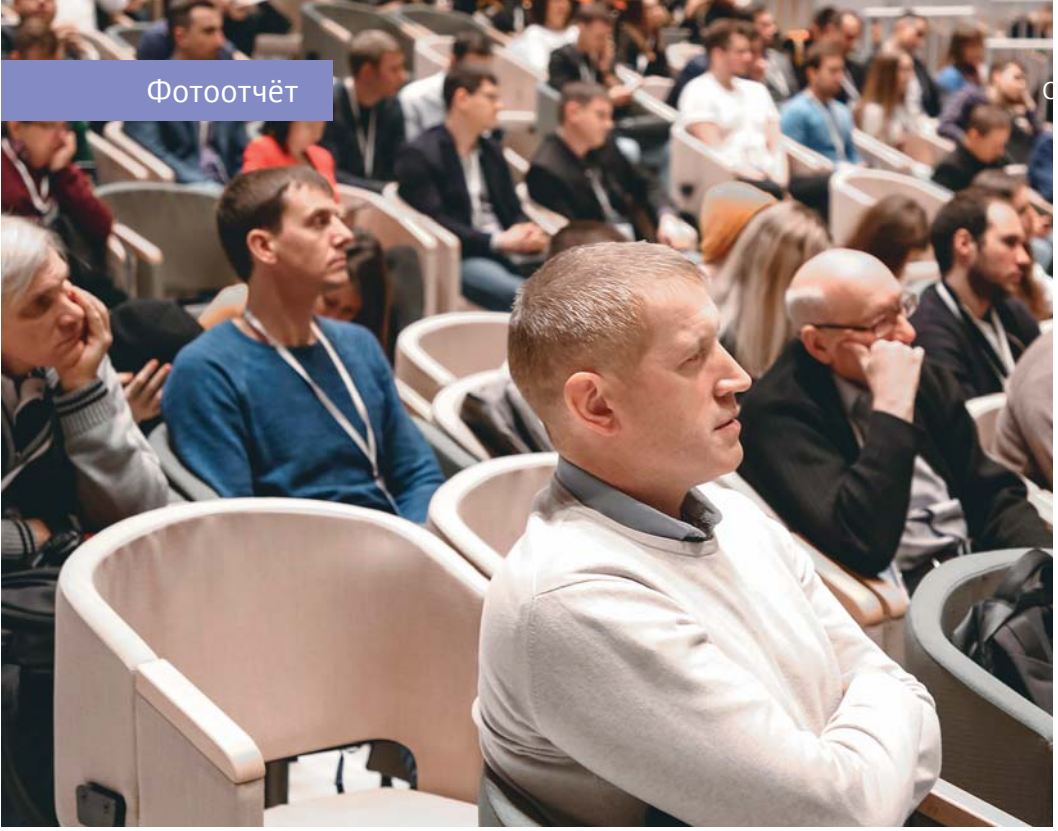

8 (495) 221-21-4
8 (343) 247-83-6
8 (812) 407-34-7
ПОСТРОЕН
СИСТЕМ ИН
БЕЗ
ПОСТРОЕН
ИТ-ИНФ
АУДИТ
#codeib

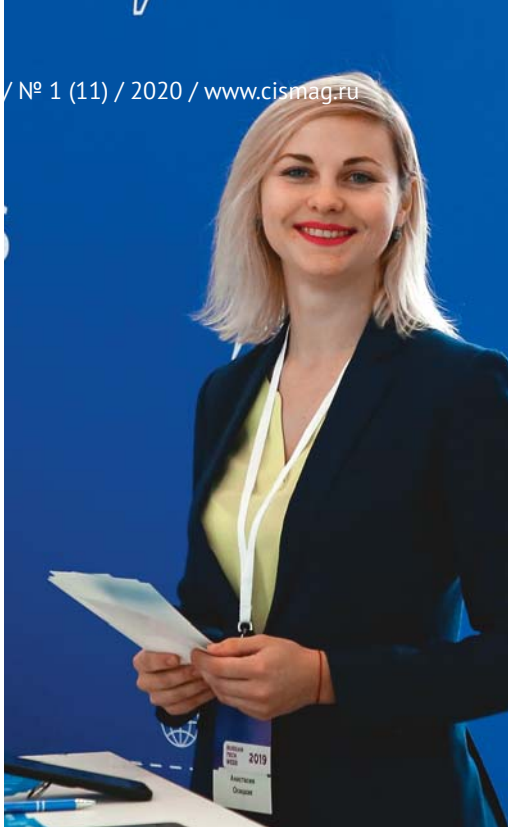

SOC
ФОРУМ


oft и Positiv
logies
енка
-им
сси
зне


SOC
ФОРУМ






2019


СПИКЕР
2019


OFFZONE


THALES

CIS / № 1 (11) / 2020 / www.cismag.ru

Законодательные изменения рынка электронной подписи

Новая технология использования ЭП и ужесточение требований к УЦ

Потребность рынка электронной подписи в законодательных изменениях назрела давно. Перечень аккредитованных Минкомсвязью России удостоверяющих центров разросся практически до 500 участников, что усложнило реализацию мер по контролю и регулированию отрасли.

В связи с развитием технологий участники рынка нуждались в нормативном закреплении таких понятий, как **облачная электронная подпись и дистанционная идентификация**. Из-за участившихся случаев мошеннического выпуска на граждан без их ведома и последующего использования ЭП в преступных схемах пользователям не хватало **инструмента отслеживания оформленных на них сертификатов**. Эти и прочие проблемы рынка пытается решить федеральный закон, подписанный президентом РФ в конце 2019 года.

Федеральный закон от 27 декабря 2019 N 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» **вступает в силу 1 июля 2020 года**, за исключением некоторых положений.

КСКПЭП*	Получатель ЭП: ФЛ	Получатель ЭП: представитель ЮЛ, ИП («руководитель»** или сотрудник)
Может использоваться	только от имени ФЛ	только для представления интересов ЮЛ, ИП
Кто выпускает	коммерческий УЦ	коммерческий УЦ

Блок-схема «Получатель ЭП, её выпуск и использование», действующая в настоящий момент.

КСКПЭП*	Получатель ЭП: ФЛ	Получатель ЭП: «руководитель»** ЮЛ, ИП
Может использоваться	1. От имени ФЛ, 2. От имени сотрудника ЮЛ, ИП при наличии машиночитаемой доверенности	только для представления интересов ЮЛ, ИП
Кто выпускает	коммерческий УЦ	УЦ ФНС

Блок-схема «Получатель ЭП, её выпуск и использование», которая начнёт действовать после вступления в силу соответствующих норм закона.

* КСКПЭП – квалифицированный сертификат ключа проверки электронной подписи.

** Под «руководителем» подразумевается единоличный исполнительный орган – физическое лицо, имеющее право действовать от имени организации без доверенности, или физическое лицо, зарегистрированное в качестве ИП.

Эксперты юридической службы портала iEcp.ru подготовили **анализ основных изменений** рынка электронной подписи, которые содержит указанный закон. Как можно будет узнать о выпуске квалифицированного сертификата на своё имя? Как изменится технология использования электронной подписи? Что ждёт коммерческие удостоверяющие центры (УЦ)?

Технологические аспекты

Получение и использование электронной подписи

Два главных нововведения:

1) с 1 июля 2020 года электронные подписи для ЮЛ и ИП будет уполномочен выдавать только УЦ ФНС;

2) для представления интересов ЮЛ, ИП их работники будут получать электронные подписи как физические лица в коммерческих аккредитованных УЦ, а при подписании электронных документов прикладывать также машиночитаемые доверенности от своих работодателей, которые должны будут быть подписаны КЭП, сертификаты которых выдаст УЦ ФНС (с 1 января 2021 года).

Формы доверенностей определят и разместят на официальных сайтах операторы государственных и муниципальных информационных систем (ИС), для целей которых будут представляться электронные документы. При отсутствии образцов от обозначенных ИС формы определит Минкомсвязь России.

Способы идентификации при получении ЭП

Допускается идентификация получателя электронной подписи не только при его личном присутствии, но **и удалённым способом** при помощи **КЭП, загранпаспорта нового образца,** Единой системы идентификации и аутентификации (**ЕСИА**), Единой биометрической системы (**ЕБС**).

«Облачная» электронная подпись

Законопроект легализует **«облачную» КЭП** – юридически значимую электронную подпись, реализованную с помощью технологии, которая все вычислительные операции с использованием ЭП переносит на внешний сервис («облако»), на стороне пользователя оставляя лишь необходимость подтвердить свою личность и совершение операции.

Информирование о выпущенных сертификатах

Правительство РФ установит требования к порядку предоставления владельцам КСКПЭП данных о выданных им сертификатах **посредством портала «Госуслуги»**. Сроки реализации пока неизвестны.

Реформирование системы аккредитации удостоверяющих центров

Требования к УЦ

С 1 июля 2020 года для получения аккредитации коммерческие УЦ должны будут **соответствовать следующим требованиям:**

- **минимальный размер собственных средств (капитала)** не менее 1 млрд рублей либо 500 млн рублей при наличии не менее чем в 3/4 субъектов РФ одного или более филиала или представительства УЦ;
- **наличие финансового обеспечения ответственности** в сумме не менее чем 100 млн и 500 тысяч рублей за каждое место осуществления лицензируемого вида деятельности (всего на сумму не более 200 млн рублей);
- соответствие требованиям **к деловой репутации** руководителя и учредителей (участников) УЦ;
- в отношении УЦ, претендующего на получение аккредитации, **не была досрочно прекращена его аккредитация** в течение 3-х лет до подачи заявления (аналогично в отношении единоличного исполнительного органа УЦ-претендента на аккредитацию).

Аккредитация коммерческих УЦ будет осуществляться не на 5 лет, как в настоящий момент, а только **на 3 года.**

Аккредитация для работы с «облачной» ЭП

Коммерческие АУЦ смогут осуществлять «облачное» хранение ключей электронных подписей, создание и проверку «облачной» ЭП по поручению их владельцев, если будут соответствовать следующим **«повышенным» требованиям аккредитации:**

- **наличие финансового обеспечения ответственности** в сумме не менее чем 200 млн и 500 тысяч рублей за каждое место осуществления лицензируемого вида деятельности (всего на сумму не более 300 млн рублей);
- **наличие в собственности УЦ и применение им средств,** имеющих подтверждение соответствия требованиям, установленным ФСБ России.

Как коммерческим УЦ сохранить свой бизнес?

В свете столь глобальных изменений рынка электронной подписи особенно важно позаботиться о том, чтобы не потерять высококвалифицированные кадры коммерческих удостоверяющих центров, сберечь их бизнес. Подобную задачу поставил перед собой удостоверяющий центр «Основание», созданный **госкорпорацией «Ростех» и группой компаний «Селдон»**. Добиться её решения можно только при помощи использования современных технологий, чёткого соблюдения правил регуляторов и высокого уровня финансовой и экономической стабильности.

Соответствие предъявляемым высоким требованиям и успешная адаптация к новым обеспечиваются опытом госкорпорации «Ростех» по внедрению новых сервисов в рамках национального проекта «Цифровая экономика» и группы компаний «Селдон» – разработчика ИТ-решений в сфере электронных торгов на базе аналитических и лингвистических технологий.

Удостоверяющий центр «Основание» предлагает коммерческим УЦ, не имеющим достаточного количества собственных средств и прочих необходимых «бизнес-мощностей», **присоединиться к своей партнёрской сети.** К сотрудничеству также приглашаются прочие лицензиаты ФСБ в области криптографии.

Компания сможет не просто **сохранить свой бизнес,** но **и поднять его на новый уровень.** Удостоверяющий центр «Основание» распространяет на партнёрскую сеть ИТ-решение по автоматизации рабочих процессов (web-кабинет), гибко настраиваемое API, обеспечивает достойный уровень вознаграждения, осуществляет координацию и таргетинг дополнительных клиентских потоков.

Основание
Удостоверяющий центр

uc-osnovanie.ru

*Подробнее о партнёрской программе **удостоверяющего центра «Основание»** можно узнать:*

- отправив заявку на электронную почту partners@iecp.ru;
- позвонив по телефону 8-800-511-70-50.

С полной версией анализа законодательных изменений, включающей:

- *характеристику доверенной третьей стороны (ДТС) – нового участника рынка электронной подписи;*
- *требования к аккредитации ДТС;*
- *аспекты организации «единого пространства КЭП» и прочие нюансы;*

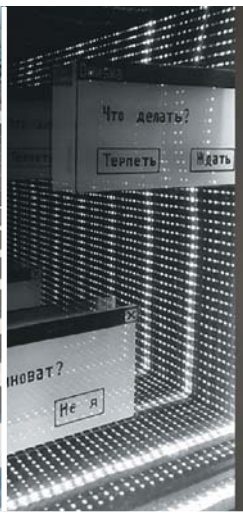
можно ознакомиться на Едином портале Электронной подписи, считав QR-code.

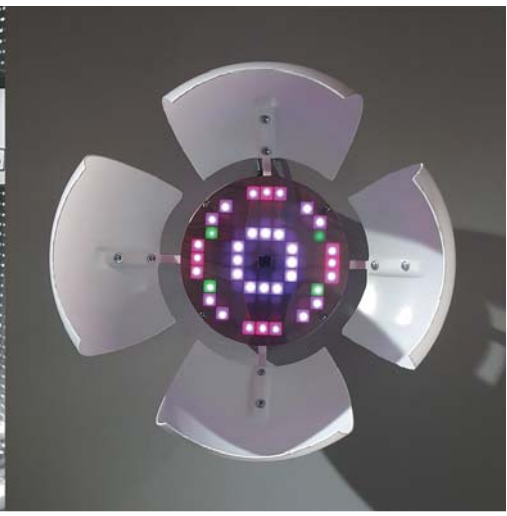
Выставка «Открытый музей – 2020»

7 февраля в галерее «Электромузей» Объединения «Выставочные залы Москвы» открылся выставочный проект «Открытый музей – 2020».

Выставка «Открытый музей – 2020» – продолжение «Антимузея» выставочного проекта 2016 года, привлёкшего более 70 участников из разных стран. «Открытый музей» – это площадка для свободного творческого высказывания, намеренно не ограниченная дискурсивными рамками и функционирующая без кураторского контроля. Цель проекта – показать актуальные тренды современного медиа- и технологического искусства и смежных пространств творческого высказывания, способствовать их развитию и стимулировать творческую активность в сфере медиа-арта.

Проект «Открытый музей» основан на проведённом open-call среди художников, дизайнеров, инженеров, программистов, музыкантов, учёных и всех тех, кто исследует художественную и коммуникационную природу новых медиа. На выставке будут показаны все поданные проекты, удовлетворяющие одному или нескольким из критериев, определяющих современное медийное и технологическое искусство: интерактивные инсталляции и объекты, дополненная реальность, видео, аудиовизуальные перформансы, документация интервенций в городской среде, 3D глитчи, и другое.





Департамент культуры города Москвы

Выставочные залы Москвы
Объединение
Электро музей

Место проведения:
«Электромузей в Ростокино»
(Ростокинская ул., 1, м. ВДНХ, МЦК «Ростокино»)
Тел: 8 (499) 187-10-45
electromuseum@vzmoscow.ru | www.vzmoscow.ru

CIS / № 1 (11) / 2020 / www.cismag.ru

Применение российской интеллектуальной карты для защиты IoT-устройств

Высокая конкуренция вынуждает производителей ускорять выпуск IoT-устройств на рынок, при этом зачастую жертвуя временем и средствами на разработку и тестирование систем безопасности.

Такие тенденции привели нас к вопросу создания готового решения для защиты IoT-устройств, которое соответствовало бы необходимым требованиям безопасности, могло быть встроено в устройства и интегрировано в экосистему в целом. В качестве такого средства защиты ГК «МультиСофт» создала решение на базе микроконтроллера интеллектуальной карты.

Мы начали разработку с выбора качественного микроконтроллера. ГК «МультиСофт» отдала предпочтение микроконтроллеру стандарта ISO 7816, который выдерживает не менее 500 тысяч циклов перезаписи памяти EEPROM, позволяет производить самотестирование структуры чипа, обеспечивает противодействие подключению зондами, а также имеет следующие внутренние механизмы защиты:

- от стирания области RAM при сбросе или срабатывании датчиков;
- от высокочастотных помех;
- от чтения областей ROM, EEPROM;
- от накопления статистических данных по энергопотреблению и времени выполнения команд.

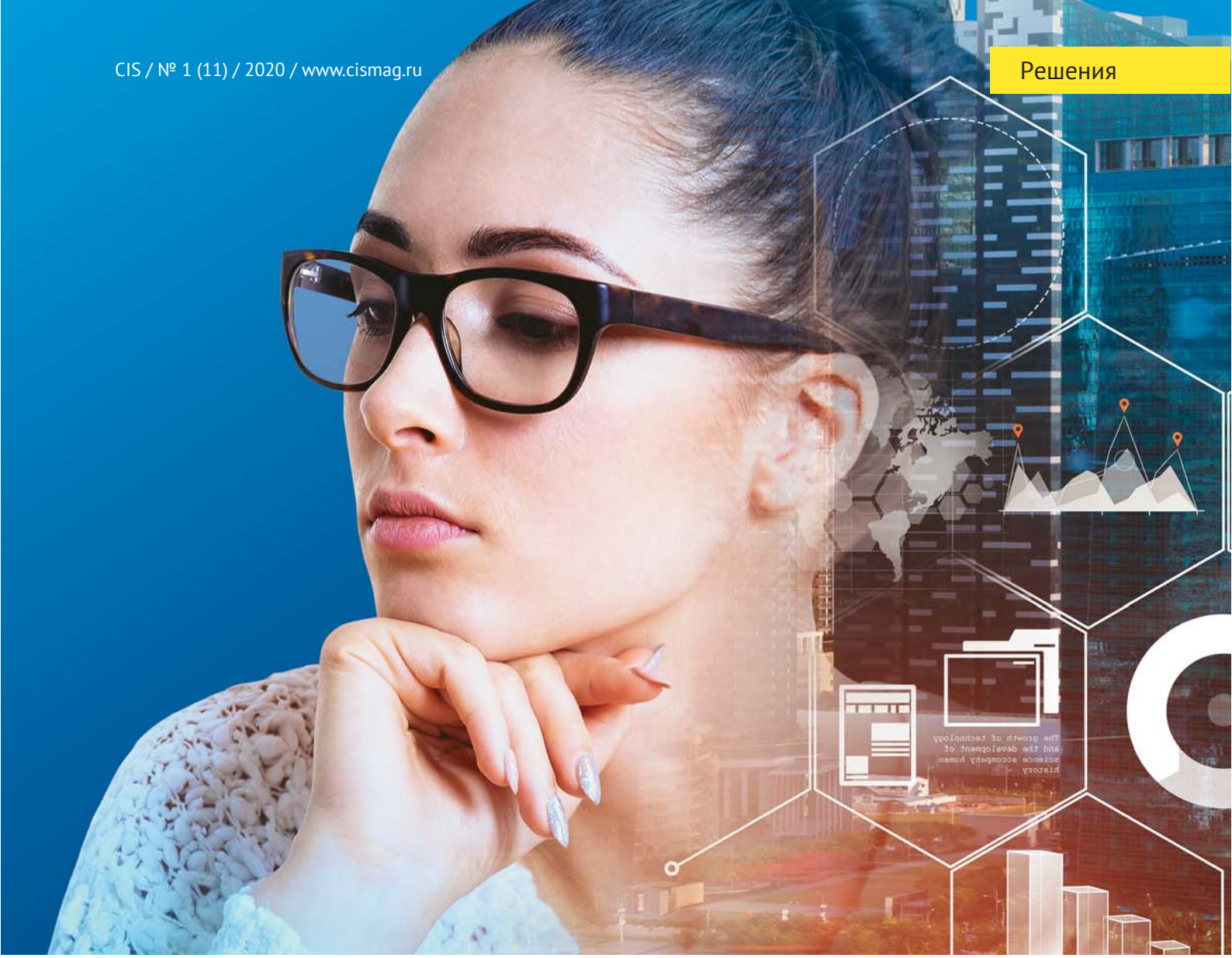
Кроме того, микроконтроллер соответствует международным стандартам безопасности Common Criteria по уровню EAL5+.

Низкое энергопотребление являлось дополнительным преимуществом при выборе смарт-карточного микроконтроллера, так как к устройствам могут предъявляться требования поддержки режима энергосбережения и ограничения доступа к электропитанию.

Следующим шагом стало написание собственной операционной системы для интеллектуальной карты – ОС «Вигрид» (VIGRID-Verification Interoperability GRID) версии 2.0. В ней реализованы отечественные криптографические стандарты:

- шифрование по ГОСТ Р 34.12-2015-Магма, ГОСТ Р 34.12-2015-Кузнечик, ГОСТ 34.12/13-2018, ГОСТ 28147-89;
- вычисление хеш-функции ГОСТ Р 34.11-2012 (режимы 256 и 512 бит), ГОСТ Р 34.11-94;
- вычисление и проверка электронной подписи по ГОСТ Р 34.10-2012-256 и 512, ГОСТ 34.10-2018;
- генерация сессионных ключей VKO (RFC 4357, RFC 7836),

а также технология работы с неизвлекаемыми ключами. Таким образом было создано средство криптографической защиты информации (СКЗИ) «MS_KEY K» – «АНГАРА». Готовое устройство было сертифицировано ФСБ России на соответствие требованиям к СКЗИ и средствам электронной подписи по классам защиты КС1 и КС2.



СКЗИ «MS_KEY K» – «АНГАРА» нашло широкое применение в сфере дистанционного банковского обслуживания (ДБО), электронного документооборота (ЭДО), ЕГАИС, налоговой и статистической отчётности, Web-сервисах с двухфакторной аутентификацией. В последнее время СКЗИ «АНГАРА» начало активно применяться в системах межмашинного взаимодействия (M2M) и Интернета вещей (IoT).

Для использования в IoT-системах в конечное устройство устанавливается элемент безопасности, который может быть представлен в виде полноразмерной смарт-карты, либо коммуникационной карты меньшего размера, либо в виде корпусаQFN для монтажа на плату. Помимо микроконтроллера, который устанавливается в конечное устройство, серверная часть оснащается отдельным аппаратным модулем безопасности – HSM (Hardware Security Module), применяемым в том числе для генерации сессионных ключей, а также ключевых пар. При этом закрытые/секретные ключи остаются неизвлекаемыми.

Для защищённого обмена данными конечных устройств с базовой станцией нами был разработан универсальный протокол с применением стойких криптографических механизмов, реализуемых элементом безопасности. Применяемый протокол взаимодействия позволяет осуществлять шифрование/расшифрование дискретных пакетов данных/управляющих команд, передаваемых или принимаемых конечными устройствами, их имитозащиту, подпись/проверку подписи под данными.

Применение указанного подхода решает проблемы безопасности передачи данных в среде Интернет вещей: защищает конфиденциальность, целостность, достоверность передаваемой информации, защищает канал управления конечными устройствами, а также данные сенсоров. Может применяться как в сетях LoRaWAN, так и в сетях NB-IoT на базе сетей операторов сотовой связи.

СКЗИ «MS_KEY K» – «АНГАРА» соответствует высоким требованиям безопасности, предъявляемым к IoT-системам. Может применяться в проектах федерального, а также международного значения. Для этих целей было разработано и сертифицировано экспортное исполнение, где реализованы как алгоритмы шифрования по ГОСТ Р 34.12-2015 (режимы Магма и Кузнечик), ГОСТ 28147-89 и алгоритмы электронной подписи ГОСТ Р 34.10-2012 (режимы 256 и 512 бит). А благодаря написанию собственной операционной системы ОС «Вигрид» 2.0 СКЗИ «MS_KEY K» – «АНГАРА» может оперативно дорабатываться под задачи клиента.

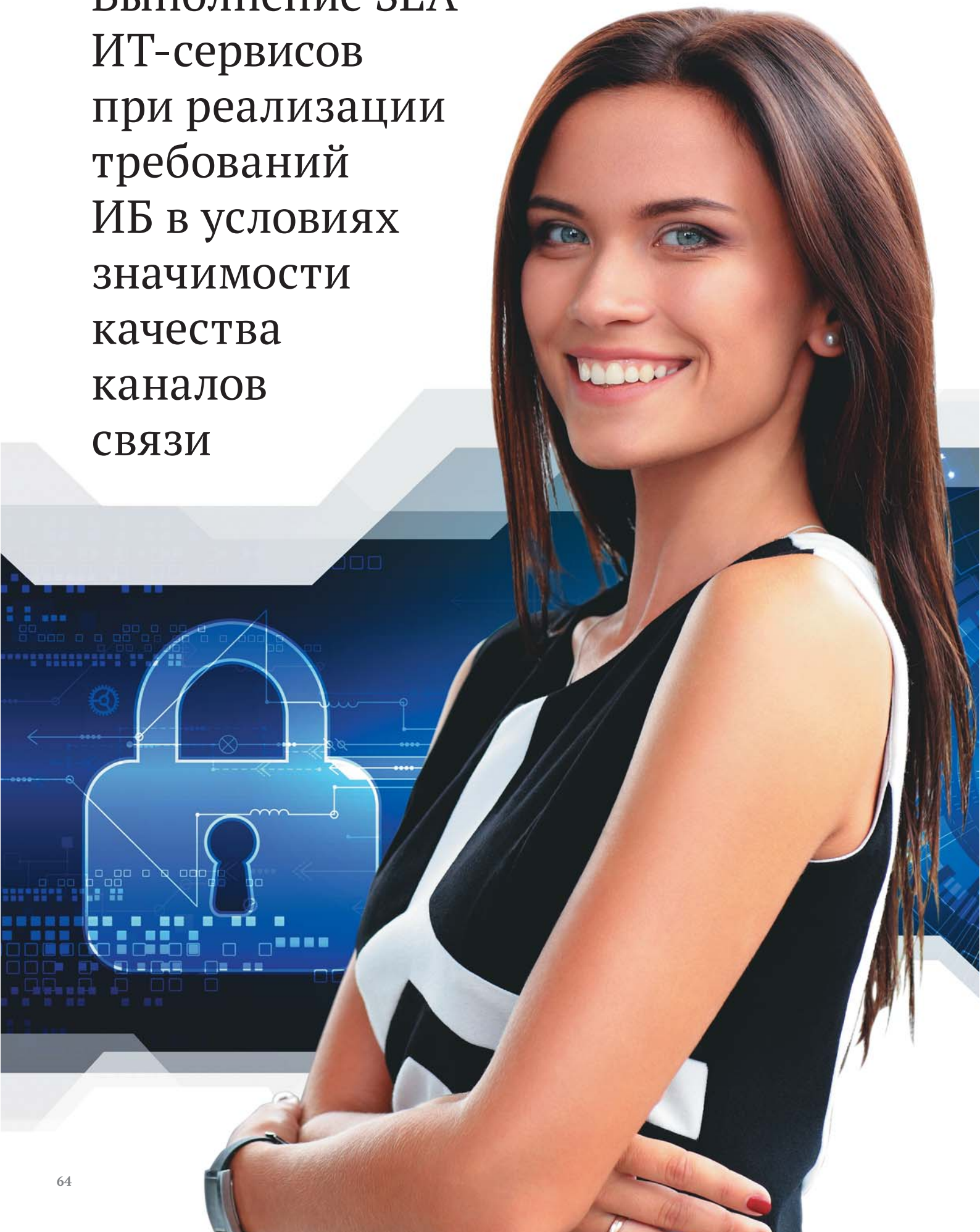
Николай Кашин,
Руководитель проекта
ООО «МультиСофт Системз»

MultiSoft

multisoft.ru

CIS / № 1 (11) / 2020 / www.cismag.ru

Выполнение SLA ИТ-сервисов при реализации требований ИБ в условиях значимости качества каналов связи



В статье мы решили рассмотреть влияние применения средств криптографической защиты информации (далее – СКЗИ) на параметры каналов связи и работу ИТ-сервисов. Полагаем, что материал, изложенный в статье, поможет пересмотреть подход к выбору средств защиты и проектированию защищённых сетей передачи данных.

Введение

С момента перехода от постиндустриального к информационному обществу требования к системам обработки, хранению и передачи данных непрерывно растут. Новые технологии (виртуализация, облачные решения, Big Data, системы реального времени и др.) накладывают жёсткие требования к техническим характеристикам и функциональности. Дата-центры стали неотъемлемым атрибутом нашего времени, предоставляя ИТ-услуги для решения задач крупного, среднего и малого бизнеса и государственных заказчиков. Операторы связи за последние годы существенно модернизировали каналы передачи данных и свою технологическую инфраструктуру для предоставления услуг связи, передачи данных и доступа к сети Интернет. Появление новых и развитие действующих территориально распределённых ресурсов утвердили необходимость соответствия высоким требованиям качества, надёжности и защиты информации и инфраструктуры.

Стало очевидным, что в современных реалиях скорость работы инфраструктуры, время отклика компьютерных программ и бизнес-приложений является важным параметром в условиях выполнения SLA ИТ-сервисов. Высокая конкуренция на ИТ-рынке позволила поднять планку качества и приучить пользователей к высокому качеству обслуживания. Когда для получения желаемого результата от приложения необходимо подождать, мы испытываем неудовлетворение и желание отказаться от использования программы в пользу других вариантов. Если рассмотреть ситуацию на уровне бизнеса, производственных процессов или работы персонала, в том числе руководства, где важно своевременно получить информацию для выполнения бизнес-задач и принятия решений, когда минуты и даже секунды влияют на результат, – это становится реальной проблемой, которую надо разрешать, ведь на кону могут стоять не только финансовые успехи, но и жизни людей. Воздействие на работу приложений оказывают все компоненты архитектуры ИТ-сервиса. Это мощность серверов и СХД, настройка СУБД, правильность исполняемого кода приложения, производительность и надёжность сетей передачи данных. Настройка этого технологического «оркестра» под параметры SLA – весьма непростая задача. В условиях необходимости обеспечения защиты данных сложность многократно возрастает. В силу специфики направления деятельности нашей компании мы сегодня поговорим о влиянии применения СКЗИ при защите каналов связи на сетевые параметры инфраструктуры.

СКЗИ на каналах связи

За последнее время регуляторы в лице ФСТЭК России, ФСБ России, ЦБ России, Минкомсвязь выпустили достаточно большой перечень новых требований по обеспечению информационной безопасности и защите инфраструктуры, предписывающие обязательное применение сертифицированных СЗИ и СКЗИ, таким образом, не оставляя шансов для применения иностранных средств защиты, зачастую встроенных в используемое оборудование. В этой связи возникает ситуация, когда в выверенную инфраструктуру с сервисом, работающим с необходимым качеством, требуется внести дополнительный компонент в виде сертифицированного СЗИ или СКЗИ. В результате внесения (формального, без учёта применяемой технологии) таких изменений защищённость сервисов и данных, в соответствии с нормативным документами, возрастает, а вот качество работы сервисов может резко ухудшиться. Это связано с тем, что применение СЗИ и СКЗИ на каналах связи существенно влияет на такие сетевые параметры как:

- **Пропускная способность** (bandwidth). В случае, когда на сети применяются СКЗИ, необходимо говорить о скорости шифрования, т. к. именно этот параметр в основном определят пропускную способность, а не номинальная скорость сетевого интерфейса. Применение СКЗИ не должно уменьшать пропускную способность, в противном случае появляются потери информации при передаче и её повторная передача при использовании протоколов с гарантией доведения
- **Кол-во потерянных пакетов (Packet loss)**
- **Различные виды задержки** (RTT, OWD)
- **Изменение задержки**, сетевой джиттер (Jitter)

Это важные показатели надёжности и производительности сетей передачи данных, а, следовательно, и работающих поверх этих сетей приложений и сервисов.

Потери на канале связи приводят к существенному замедлению и нестабильной работе сложных протоколов прикладного уровня.

Скорость работы приложений, использующих «болтливые» протоколы, замедляется нелинейно по отношению к росту задержки в сети, из-за тайм-аута рвутся сессии, и цикл вопрос-ответ между клиентом и сер-

Figure 3 • Network Throughput vs. Encrypted Frame Size (Bytes)

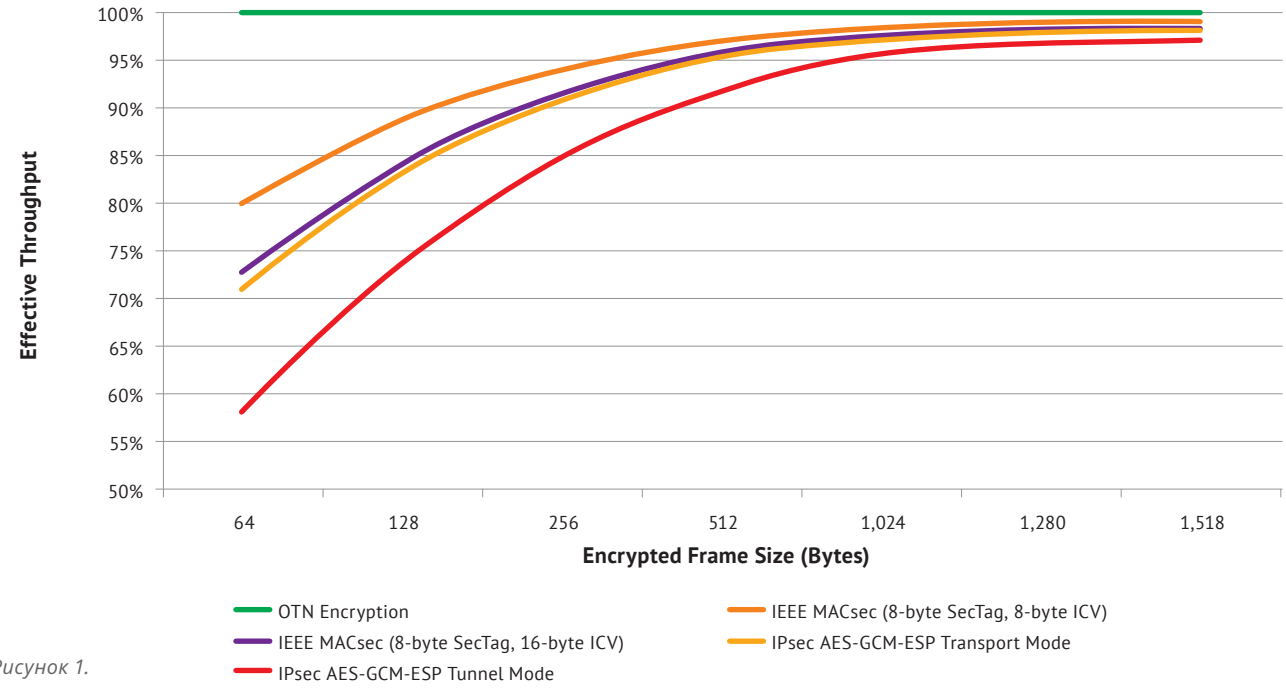


Рисунок 1.

вером начинается снова. Приложения реального времени, стриминга, транзакционные схемы, сервисы синхронизации СУБД и СХД сильно зависят от времени ожидания отклика системы. Увеличение задержки всего на несколько миллисекунд может привести к неверной реакции на предоставленные данные. Изображение и голос искажаются, приложения «зависают». Высокие показатели джиттера не дают возможности системам подстроиться под текущий уровень задержки и стабилизировать работу сервиса.

О важности этих показателей сегодня говорят нам и значимые события, освещённые в мировых СМИ. В борьбе за сокращение задержек Cisco поглощает Exablaze – разработчика сетевых решений с ультранизкими задержками, а провайдер Colt Technology Services построил сеть между Токио и Гонконгом со временем отклика до 40 миллисекунд.

Причины, по которым СКЗИ наделены теми или иными характеристиками производительности, различны.

- Выбор между СКЗИ, выполняющими только целевые функции криптоимитозащиты и многофункциональными СКЗИ, выполняющими ряд дополнительных функций (например, маршрутизацию, межсетевое экранирование, шлюзование). На рынке присутствуют как узконаправленные устройства, так и сочетающие в себе несколько функций.
- Режим защиты (шифрования) данных. В транспортном (native) режиме шифруется только блок данных, а сетевые заголовки остаются, незашифрованными. В тунельном режиме весь протокольный блок данных (то есть сам пакет) шифруется и инкапсулируется в блок данных того же или более высокого уровня.
- Уровень сетевой модели OSI, на котором выполняется защита. В сочетании с режимом шифрования мы получаем совершенно разные теоретические максимумы производительности (рис. 1).

Сервисы наиболее чувствительные к сетевым параметрам:

- IP-телефония и видеконференцсвязь
- Потокового видео
- Кластеры серверов баз данных
- Приложения на протоколах с избыточной информативностью
- Распределённые базы данных
- Онлайн-сервисы
- Сервисы на сетях с большим значением MTU

- Так же производительность СКЗИ зависит от способа реализации криптографических алгоритмов (процессор или ПЛИС) и сложности сетевых операций, выполняемых на устройстве, от производительности оборудования (процессор или ПЛИС).

Методы минимизации влияния

Решение для защиты каналов передачи данных необходимо подбирать в зависимости от заданного уровня сервисов, использующих эти каналы, оперируя перечисленными выше параметрами. Естественно, это не полный список параметров для оценки влияния

СКЗИ на сетевые сервисы. В числе важных характеристик для принятия решения среди похожих моделей можно рассматривать, в частности, возможность масштабирования, совместимость, влияние на сетевую топологию, надёжность и наличие имитозащиты.

Что же делать, если данные параметры всё равно не удовлетворяют требованиям приложений? Вариантов немного, но они есть.

- Уделить внимание корректной работе протоколов приоритизации трафика **(QoS)**. Тут важно отметить, что в данном случае средства защиты не должны скрывать служебные заголовки, по которым она осуществляется. При выборе туннельного режима это будет проблематично.
- Использование кэширования (различные **WAN-оптимизаторы**). Весьма полезные устройства для ускорения работы приложений, в том числе в рамках задачи по минимизации влияния от СКЗИ, однако подходит не для всех типов трафика.
- **Сжатие (компрессия) данных** перед передачей. Уменьшение размера передаваемых данных без потери полезной информации увеличит пропускную способность, но только в ряде случаев может сократить задержку.
- **Применение средств криптографической защиты каналов связи L1.** Подобные решения не распространены на рынке, т. к. для их применения необходимо, чтобы клиент имел собственный выход на оптические. Необходимость защиты на данном уровне оптики до сих пор вызывает вопросы у некоторых. Но те, кто знает, что оптика так же уязвима, как и другие среды передачи информации, уже применяют для своих сетей решения зарубежных производителей, таких как PocketLigth или Ciena. Для тех же, кто обязан по требованиям, действующим в РФ, применять для криптографии только СКЗИ, реализующие ГОСТ алгоритмы защиты, подобные средства были не доступны, поэтому широкополосные каналы передачи данных защищали, применяя сложные кластерные решения СКЗИ уровней L2 или L3. Но теперь и в России есть линейка устройств криптографической защиты информации уровня L1 «Квазар» производства компании «Системы практической безопасности».

СКЗИ Квазар

В терминах, приводимых выше, Квазар – это СКЗИ, которое реализует алгоритмы криптографической защиты информации, указанные в ГОСТ, работающее в туннельном режиме на уровне L1, использующее для передачи трафика оптические линии. За счёт того, что Квазар использует для работы по оптическим линиям протокол OTN, а криптография реализована на ПЛИС, он имеет ряд преимуществ и характеристик, на сегодняшний день уникальных среди **СКЗИ, прошедших сертификации ФСБ России по классу защиты КС-3.**

Благодаря тому, что для управления не применяется операционная система, а реализация криптоалгоритмов на ПЛИС и её конфигурация позволяют достичь значения задержки **Latency RTD (us)** в диапазоне от **0,173** миллисекунды до **0,204** миллисекунд на Jambo Frame 9600 байт при полном отсутствии потерь **(Packet loss)** и при любом типе трафика (рис. 2). Для передачи данных Квазар использует синхронный протокол (OTN), поэтому параметр **изменения задержки** джиттер (Jitter) стремится к **0**, а пропускная способность соответствует скорости линии – 10 Гбит/с (рис. 3).

Квазар работает в прозрачном режиме. Участие в сетевой маршрутизации или коммутации не требуется. Благодаря этому, встав в «разрыв», Квазар не влияет на сетевую архитектуру, а его внедрение относительно несложно, хотя и требует специальных компетенций.

Квазар совместим с ведущими производителями DWDM систем за счёт поддержки формата OTU2e, что снимает любые ограничения на длину защищённого канала. Но и без применения DWDM Квазар может обеспечить защиту линии до 80 км при нормальных условиях (теоретический максимум).

Квазар является мультисервисным устройством, характеристики которого не зависят от использующихся выше протоколов. В качестве клиентского трафика вы можете использовать не только Ethernet 10G, но и Fiber Channel 8G и STM 1-4-16.

За счёт наличия второго линейного интерфейса, работающего в параллельном режиме, Квазар поддерживает резервирование линии без дополнительных устройств. Скорость переключения между основным и резервным каналом не превышает 50 миллисекунд, что соответствует стандартам, предъявляемым провайдерами связи к сетевым устройствам.

Технологии и методы, применяемые в реализации Квазара, накладывают и некоторые ограничения.

- Квазар работает в режиме точка-точка и не поддерживает режимов мультисайта или клиентские подключения (VPN-client)
- Масштабируется только парами независимых устройств, не объединяясь в кластеры

На сегодняшний день применение Квазаров эффективно (в том числе и с экономической

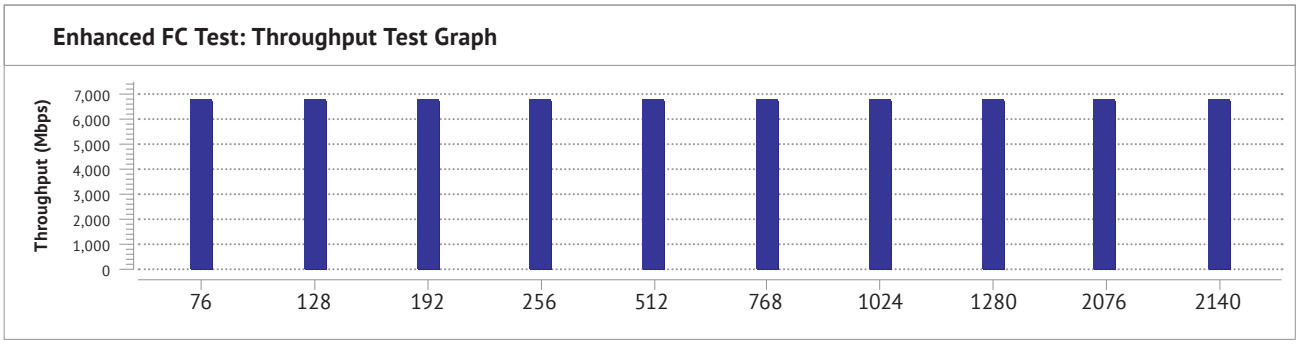


Рисунок 2.

точки зрения) для реализации защиты каналов передачи данных пропускной способностью 10 Гбит/с, построения защищённых опорных, региональных и магистральных сетей в условиях значимости сохранения высоких параметров производительности.

Заключение

Рассматривая устройства различных уровней криптографической защиты, некорректно говорить об однозначно лучшем или худшем решении, т. к. совокупность функций и характеристик индивидуальна для каждой ситуации.

Приняв решение о применении средств защиты, необходимо определить допустимый диапазон значений параметров, влияющих на параметры сети и сетевую архитектуру, и далее в этих рамках проводить выбор СКЗИ.

До принятия решения о внедрении тех или иных средств защиты, желательно провести стендовые испытания для подтверждения заявленных характеристик и получения чёткой картины влияния применения СКЗИ, а также выбора средств компенсации их применения, если таковые понадобятся.

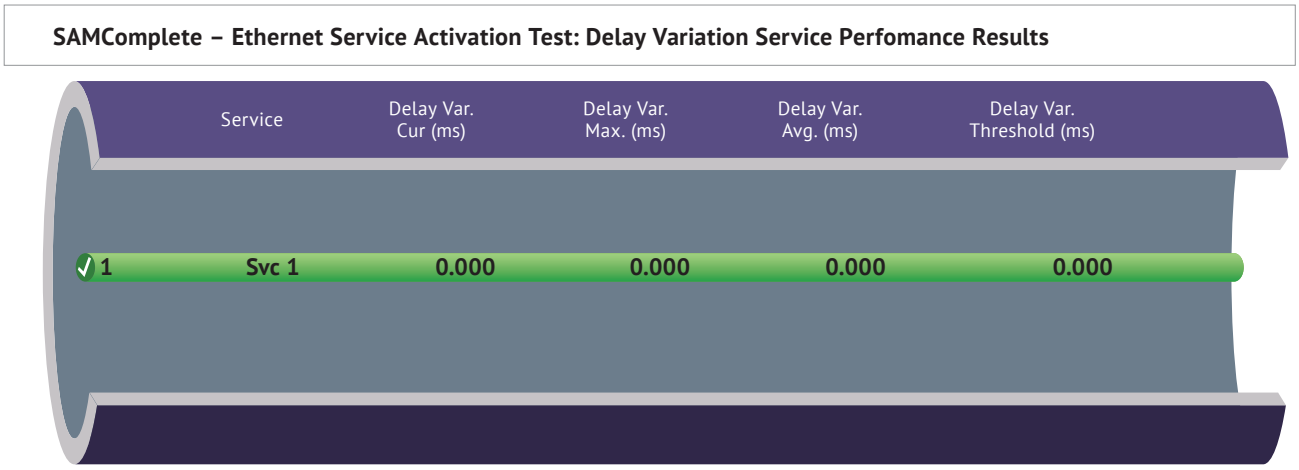


Рисунок 3.

Компания ООО «Системы практической безопасности» регулярно проводит тематические испытания СКЗИ Квазар и публикует подробные результаты на своём сайте http://systempb.ru

Все приводимые в статье характеристики отражены в отчётах тестов, проведённых по методикам RFC 2544, RFC 6349 TrueSpeed для протокола Ethernet 10G и RFC 2544 для протокола Fiber Channel 8G.

Также на сайте размещены типовые схемы применения Квазара, а используя окно «задать вопрос», сможете направить нам ваши вопросы или оставить заявку на проведение стендовых испытаний.

Маркевич Кирилл Викторович
Руководитель направления ООО «Системы практической безопасности»
www.systempb.ru

СПБ

Материалы, использованные при подготовке статьи:
Описание RFC 2544
habr.com/ru/post/475912
habr.com/ru/company/it-grad/blog/312038
Новостные материалы: servernews.ru

Японский кроссворд

Пришлите разгаданный японский кроссворд на почту info@sovinfosystems.ru
и получите приз от редакции журнала «CIS».

																7	6																																
						15									8	1	1																																
				16	17	5									1	4	2	5																															
		40	36	12	8	3	14								4	2	1	4	3	1						1	2									16	14												
	40	3	2	2	1	3	2	13	12	13				11	1	1	5	1	5	4				6	16	16	17	3							16	7	4	12											
41	3	2	3	3	2	1	9	1	1	2	14	14	15	4	13	13	15	1	1	1	2			16	10	2	1	16	26	26	25	25	25	26	6	5	4	2	8	3							3		
3	1	1	2	2	1	1	3	15	15	16	21	16	17	14	1	3	5	26	26	26	28	28	31	9	2	7	6	5	5	4	5	10	16	16	22	16	10	7	2	1	1	1	1	1	1	1	2	6	

				21	12
				20	12
				20	11
				16	11
				16	11
				16	12
				17	12
				16	12
				15	11
				16	12
			15	1	13
			14	2	12
		9	6	3	13
			8	11	13
			7	9	13
		6	3	2	13
			6	4	13
				5	13
				5	12
				4	11
				4	10
				4	11
				4	12
				4	12
				4	12
			5	7	3
			5	6	2
			5	4	2
			6	3	2
		7	9	1	1
7	3	4	1	2	1
		8	10	3	1
		8	9	4	1
		7	1	15	1
		6	1	12	2
		6	1	12	3
		5	2	11	3
		4	2	11	2
		4	3	11	3
			3	16	2
		1	1	15	3
			3	15	4
			3	16	7
			3	16	12
		2	16	8	1
		1	16	8	1
		1	17	8	1
		3	17	8	1
			24	8	1
			21	6	2
		11	7	6	1
		8	7	6	1
	1	7	8	5	1
	1	6	8	4	1
	1	7	9	4	1
	2	6	10	4	1
	2	6	11	3	1

Календарь мероприятий

2 марта
Казань • Митап
Представление 5-й международной программы акселерации Pulsar VC

2 марта – 10 апреля
Москва • Онлайн-трансляция • Курс
Обновленный • Курс повышения квалификации Blockchain Lawyers

2 марта – 9 апреля
Москва • Онлайн-трансляция • Курс
Контекстная реклама – подготовка профессионалов

3 марта
Москва • Форум
БИЗНЕС-ВИДЕО 2020

3 марта
Воронеж • Конференция
Семинар о TrueConf Server 4.5 и новинках AV-оборудования в Воронеже

3 марта
Казань • Митап
Представление 5-й международной программы акселерации Pulsar VC

3 марта
Онлайн-трансляция • Вебинар
Unit-тестирование Angular приложений

4 марта
Онлайн-трансляция • Мастер-класс
Бизнес-завтрак «Как подружить SEO и продажи»

5 марта
Белгород • Конференция
Семинар о TrueConf Server 4.5 и новинках AV-оборудования в Белгороде

5 марта
Онлайн-трансляция • Вебинар
JS больше не нужен?! Blazor – революция в веб-разработке

6-7 марта
Москва • Конференция
День открытых данных в Москве 2020

9-30 марта
Москва • Онлайн-трансляция • Хакатон
Хакатон Changellenge >> Cup IT 2020

11 марта – 29 апреля
Москва • Онлайн-трансляция • Курс
Практический Курс интернет-маркетолога

13 марта
Казань • Митап
INFOSTART MEETUP Kazan

13 марта
Москва • Соревнование
CDO Award 2020

14 марта
Новосибирск • Конференция
GameDev CityFest 2020

14 марта
Санкт-Петербург • Турнир
Турнир по гигантскому слалому «IT Snow Fest St. Petersburg 2020»

14-22 марта
Санкт-Петербург • Курс
Product Owner

16-20 марта
Москва • Онлайн-трансляция • Курс
Школа инвестиций ФРИИ

17 марта
Ижевск • Конференция
Семинар о TrueConf Server 4.5 и новинках AV-оборудования в Ижевске

17 марта
Москва • Форум
FORUM. DIGITAL RETAIL 2020

17 марта
Москва • Конференция
MCOM 2020

18-20 марта
Москва • Курс
BDAM: Большие данные Big Data для руководителей

18 марта
Казань • Конференция
CRMDAY в Казани

18 марта – 18 мая
Санкт-Петербург • Курс
Введение в автоматизацию тестирования ПО

19 марта
Киров • Конференция
Семинар о TrueConf Server 4.5 и новинках AV-оборудования в Кирове

19 марта – 26 августа
Тренинг
Официальные Курсы UBIQUITI

19 марта
Санкт-Петербург • Митап
Monitoring Meetup. CI/CD процессы

19 марта – 28 мая
Москва • Курс
Профессия продакт-менеджер

21 марта
Омск • Конференция
Web@Cafe #21

21 марта
Москва • Турнир
Турнир по кикеру «IT's KICKER Moscow 2020»

22-29 марта
Санкт-Петербург • Курс
Весенний лагерь Sanak-lab πITερ

23-27 марта
Москва • Онлайн-трансляция • Курс
Венчурные фонды и бизнес-ангелы. Курс для продвинутых инвесторов

25 марта
Москва • Форум
BIG DATA 2020

26 марта
Онлайн-трансляция • Вебинар
Управление талантами на платформе 1С: Предприятие: оценка персонала по компетенциям, управление развитием персонала и кадровый резерв

27 марта
Екатеринбург • Конференция
FailConf 2020 (конференция про ошибки в IT-бизнесе)

27-29 марта
Санкт-Петербург • Хакатон
BioHack 2020 | Хакатон по биоинформатике

28 марта – 1 августа
Санкт-Петербург • Онлайн-трансляция • Курс
Академия IT-лидерства

28 марта
Санкт-Петербург • Турнир
Турнир по волейболу на паркете «IT Match Ball St. Petersburg 2020»

28 марта
Москва • Мастер-класс
Оранжевый Океан

28 марта
Ульяновск • Митап
Управление проектами

31 марта – 2 апреля
Москва • Онлайн-трансляция • Конференция
TestCon Moscow 2020

2-3 апреля
Нижний Новгород • Конференция
Digital-Оттепель V

2 апреля
Москва • Конференция
HotelCIO Exchange

3 апреля 2020
Москва • Онлайн-трансляция • Конференция
Data Start Conference 2020

3 апреля 2020
Сочи • Митап
Nutratech Сочи 2020

3-4 апреля
Москва • Форум
Форум технологических лидеров BreakPoint в Москве

3-4 апреля 2020
Москва • Курс
AIRF: Apache AirFlow

5 апреля 2020
Санкт-Петербург • Турнир
Турнир по настольному теннису «IT Match Point St.Petersburg 2020»

23 апреля
Москва • Конференция
Благотворительная ИТ-конференция «Digital Hearts - 2020»

CISummIT

Ежегодное мероприятие журнала CIS

Благотворительная ИТ-конференция Digital Hearts 2020

23 апреля, 2020

Площадка
«Москва-Сити»

Фонд Хабенского

Мероприятие журнала CIS
в поддержку Фонда Константина Хабенского

Заполните регистрационную форму для участия на мероприятии

Ждём вас на благотворительной ИТ-конференции CISummIT Digital Hearts, которая объединит самых активных участников ИТ-рынка, ведущих производителей и экспертов, чтобы собрать средства для помощи детям с заболеваниями головного мозга.

CIS Современные Информационные Системы

www.cisevent.ru
www.cismag.news