Apple: вирусные «черви» в «яблоке соблазна»
Тысяча глаз и миллионы ушей в вашем смартфоне для хакеров и спецслужб

Введение

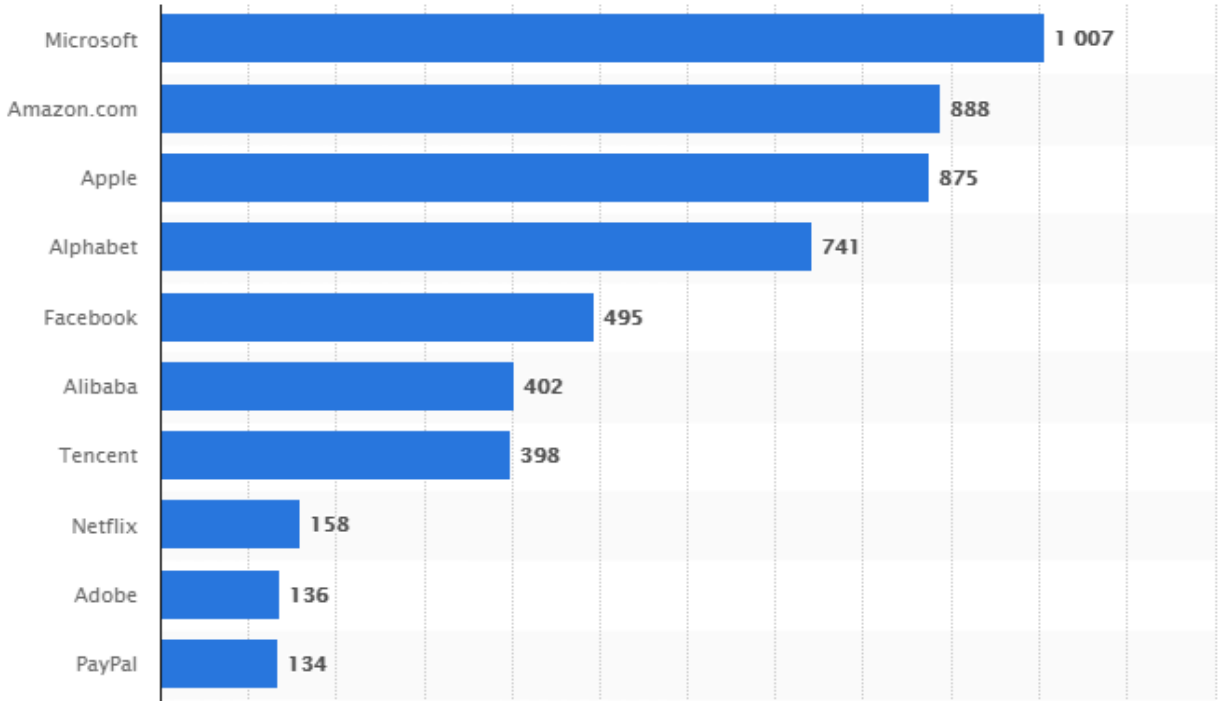
На сегодняшний день корпорация Apple является одним из ведущих акторов мировой экономики. Стоимость одноименного брэнда, по данным за февраль 2019 г., составляла $309,5 млрд. В 2019 финансовом году (с октября 2018 по сентябрь 2019 гг.) выручка Apple составила в общей сложности $260,2 млрд.[1]

По состоянию на июнь 2019 г., рыночная капитализация Apple достигла $875 млрд. Из числа мировых интернет-компаний по данному показателю базирующаяся в Купертино корпорация уступает лишь MicrosoftAmazon.

[1] Apple - Statistics & Facts. https://www.statista.com/topics/847/apple/

Рис. 1

Рыночная капитализация крупнейших интернет-компаний мира по состоянию на июнь 2019 года ($ млрд.)[2]



По данным за 2018 г., Apple занимала вторую позицию в рейтинге наиболее прибыльных компаний в мире (ее чистая прибыль составила $59,5 млрд.).

[2] Market capitalization of the biggest internet companies worldwide as of June 2019. https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/

Рис. 2

Рейтинг наиболее прибыльных компаний в мире за 2018 г.[3]

Продукция компании является неотъемлемой частью повседневной жизни сотен миллионов клиентов. В общей сложности за период 2007 – 2018 гг. количество одних лишь смартфонов iPhone, проданных потребителям, составило почти 1,5 млрд.[4]

Важно отметить, что на протяжении всего периода 2008 – 2018 гг. доходы Apple от продажи компьютеров, ноутбуков, смартфонов и мобильных гаджетов намного превышают выручку основных конкурентов компании (Google/Alphabet и Microsoft) от реализации аналогичной продукции.

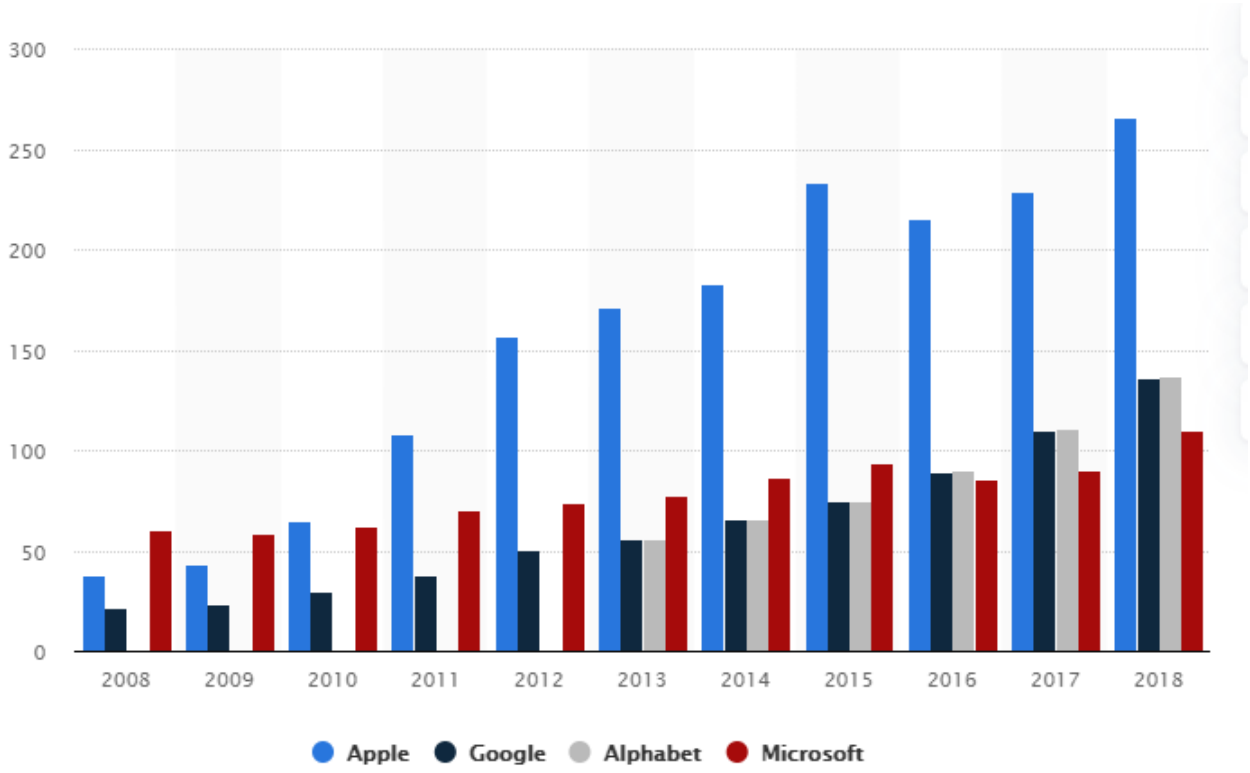
---

[3] The Most Profitable Companies in the World. https://www.statista.com/chart/17545/worlds-most-profitable-companies/

[4] Apple - Statistics & Facts. https://www.statista.com/topics/847/apple/

Рис. 3

Доходы Apple, Google/Alphabet и Microsoft за 2008-2018 гг. ($ млрд.)[5]



Таким образом, поднимая вопрос о безопасности владельцев продукции Apple, мы фактически ведем речь о предотвращении глобальных информационных угроз. Масштабы присутствия корпорации на рынке IT-продукции, равно как и престижный характер обладания ее изделиями, превращают надежность и конфиденциальность коммуникации посредством «яблочных» гаджетов в фактор, напрямую определяющий уровень национальной безопасности целых государств.

Уязвимость устройств Apple и безопасность персональных данных

В январе 2017 г. стало известно об обнаружении в

[5] Revenue comparison of Apple, Google, Alphabet, and Microsoft from 2008 to 2018. https://www.statista.com/statistics/234529/comparison-of-apple-and-google-revenues/

операционной системе Mac уязвимости, позволявшей настройки App Store без пароля, понизить безопасность системы и даже взять устройство под свой контроль[6].

В январе 2018 г. в iOS обнаружили ошибку, позволявшую удаленно блокировать смартфоны, управляемые операционными системами iOS 10 и 11, а также компьютеры Mac. Для осуществления блокировки было необходимо лишь отправить сообщение со специальной ссылкой[7].

В феврале 2018 г. в СМИ появилась информация об утечке исходного кода iBoot – ключевой программой операционной системы iOS, отвечающей за ее загрузку. Как выяснилось, утечка имела место за 2 года до этого, когда один из стажеров компании решил поделиться исходным кодом со своими друзьями. Один из последних передал код в третьи руки, в результате чего данные были размещены в публичном доступе. Последнее заметно облегчило труд хакеров, занимающихся «джейлбрейком» - взломом iPhone с целью получения доступа к файловой системе устройства[8].

В июне 2018 г. стало известно о том, что в ОС Mac была устранена уязвимость, позволявшая хакерам получить доступ к критически важным частям прошивки и получить полный контроль над компьютером или ноутбуком[9].

В сентябре 2018 г. в открытом доступе была обнаружена база данных, включавшая в себя данные нескольких миллионов

---

[6] Incident Of The Week: ‘We Stumbled’ On Root Access, Apple Says. https://www.cshub.com/network/news/incident-of-the-week-%E2%80%98we-stumbled%E2%80%99-on-root-access

[7] В iOS нашли баг, способный заставить "зависнуть" чужой iPhone. https://ria.ru/20180117/1512788655.html?in=t

[8] Обнаружен источник «крупнейшей утечки в истории iPhone». https://www.gazeta.ru/tech/2018/02/12/11646847/intern_leaked.shtml

[9] Безопасность macOS. http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_macOS

пользователей iCloud[10]. Как стало известна, эта база была сформирована компанией mSpy. Последняя занимается разработкой приложений, позволяющих клиентам отслеживать активность на смартфонах членов семьи[11].

В январе 2019 г. появилась информация о наличии серьезной уязвимости в iCloud (в участке настроек для iOS-устройств), позволяющая просматривать содержимое чужих аккаунтов в рамках данного сервиса. Как выяснилось, впервые ее обнаружили еще в октябре 2018 г., а устранили в ноябре, ничего не сообщая пользователямiCloud[12].

Одновременно была вскрыта уязвимость в видеочате FaceTime, позволяющая тайно прослушивать телефоны, указанные в списке контактов. Этот ошибка позволяла подслушивать переговоры владельцев iPhone, iPad или Mac, на которых было установлено соответствующее приложение. Важно отметить, что первоначально в Apple не отреагировали на сообщение об уязвимости. Работы по ее устранению начались лишь после того, как СМИ привлекли к данной проблеме внимание общественности[13]. Как выяснилось впоследствии, ошибка в работе приложения позволила неизвестным лицам подслушать беседу адвоката Ларри Уильямса II с его доверителем. Последняя стало поводом для начала судебного разбирательства[14].

В феврале 2019 г. сотрудники исследовательского проекта

---

[10] iCloud – сервис хранения данных для устройств Apple.
[11] Spyware maker mSpy exposes iCloud info as part of massive data breach. https://appleinsider.com/articles/18/09/06/spyware-maker-mspy-exposes-icloud-info-as-part-of-massive-data-breach
[12] iCloud Possibly Suffered A Privacy Breach Last Year That Apple Kept a Secret. https://thehackernews.com/2019/01/icloud-privacy-breach.html
[13] Прослушка в айфонах: Apple признала шпионскую уязвимость. https://www.gazeta.ru/tech/2019/01/29/12149587/facetime.shtml
[14] Адвокат подал в суд на Apple из-за подслушанных показаний его клиента. https://www.rbc.ru/rbcfreenews/5c5141c79a7947cab51e893d

Google Zero Security обнаружили 5 эксплойт-цепочек[15], использовавших 14 дефектов в программном обеспечении смартфонов Apple, позволявших хакерам обходить все уровни безопасности ПО устройства. Угроза была актуальной для всех устройств, оснащенных программным обеспечением iOS (от 10-й до 12-й версий). При помощи обнаруженных уязвимостей злоумышленники могли получить полный доступ к файловой системе смартфона, если его владелец использовал устройство для посещения одного из специально зараженных сайтов. Им также была доступна вся переписка пользователя, сведения о местоположении устройства, пароли и сертификаты, а также базы данных использующих шифрование мессенджеров, таких как WhatsApp и iMessage. Как было установлено, данная угроза сохраняла актуальность, как минимум, в течение 2-х лет[16].

В том же месяце исследователи портала TechCrunch установили, что посредством сервис Glassbox ряд приложений для iPhone тайно собирали с экрана информацию о действиях владельцев[17].

В апреле 2019 г. была обнаружена вредоносная программа-бэкдор[18] позволяющая загружать и исполнять на устройствах,

---

[15] Эксплойт - подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

[16] Incident Of The Week: Apple iPhones Affected By Data Breach Discovered By Google's Project Zero Security Researchers. https://www.cshub.com/malware/articles/incident-of-the-week-apple-iphones-affected-by-data-breach-discovered-by-googles-project-zero-security-researchers; A very deep dive into iOS Exploit chains found in the wild. https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html; В iOS нашли критические уязвимости, позволявшие сайтам взламывать айфоны. https://yandex.ru/turbo?text=https%3A%2F%2Ftjournal.ru%2Ftech%2F113904-v-ios-nashli-kriticheskie-uyazvimosti-pozvolyavshie-saytam-vzlamyvat-ayfony

[17] Тайная запись: как iPhone следит за владельцем. https://infonewsportal.ru/tajjnaya-zapis-kak-iphone-sledit-za-vladelcem.html/amp

[18] Бэкдор - дефект программного алгоритма, преднамеренно встроенный разработчиком. Позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.

управляемыхОС Mac, любой код на языке программирования Python[19].

В июле 2019 г. в СМИ появилась информация о том, что в «умных часах» Apple Watch имеется уязвимость, позволяющая прослушивать iPhone владельца. Последнее стало возможным за счет ошибки в работе приложения Walkie-Talkie («Рация»)[20].

В августе 2019 года против Apple был подан иск, связанный спрослушкой подрядчиками компании запросов, заданных владельцами гаджетов голосовому помощнику Siri. Как выяснилось, аудиозапись необязательно начиналась с момента произнесения фразы «привет, Siri». Для запуска процесса было достаточно поднять руку или застегнуть молнию. При этом подрядчик прослушивал в том числе аудиозаписи, содержащие конфиденциальную информацию (адреса клиентов, медицинские назначения и т.д.). Одновременно подрядчикам поступали данные о местоположении пользователей и их контактах[21].

В сентябре 2019 г. владельцев устройств Apple предупредили об угрозе для безопасности данных, выявленной в операционной системе iOS 13. Уязвимость позволяла злоумышленникам получить полный доступ к iPhone, iPad и iPod touch в результате установки сторонних приложений для клавиатуры. Почти одновременно стало известно о существовании в ОС уязвимости, позволяющей получить доступ к списку контактов и информации о последних звонках без ввода пароля или биометрической идентификации. Следует отметить, что компании стало известно о наличии данной уязвимости еще в

[19] Безопасность macOS. http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_macOS

[20] В Apple Watch нашли уязвимость, позволяющую прослушивать разговоры. https://snob.ru/science/v-apple-watch-nashli-uyazvimost-pozvolyayushuyu-proslushivat-razgovory/

[21] Apple объяснила сканирование фото в iCloud жестоким обращением с детьми. https://www.rbc.ru/technology_and_media/09/01/2020/5e1721789a79472a05a679f7

июле 2019 г., однако она была устранена лишь 24 сентября[22].

В ноябре 2019 г. в почтовом клиенте Apple Mail была выявлена уязвимость, позволявшая просматривать электронные письма в файле базы данных в незашифрованном виде[23].

В декабре 2019 г. было установлено, что на смартфонах iPhone 11 и iPhone 11 Pro, управляемых операционной системой iOS 13.2.3, GPS-модули собирают сведения о местоположении владельца даже тогда, когда функция отслеживания геолокации отключена. Соответствующий функционал был отключен Apple лишь в январе 2020 г.[24]

В январе 2020 г. журналистам Financial Times стало известно об уязвимости в программном коде Intelligent Tracking Prevention - системы избирательной блокировки межсайтового отслеживания привычек пользователей браузера Safari, предустановленного на продукции Apple. За счет этой уязвимости хакеры получили возможность собирать информацию о поисковой активности владельца устройства, включая перечень посещенных им сайтов и список запросов. По информации Financial Times, представители Apple получили информацию об ошибке в работе системы и еще в декабре 2019 г. устранили ее. Однако официально компания не сообщала пользователям ни о наличии этой проблемы, ни о ее устранении[25].

В 2020 г. на инновационной выставке CES в Лас-Вегасе стало известно о том, что Apple начал использовать программный

---

[22] Apple warns that iOS 13 keyboards can leak your data. https://edition.cnn.com/2019/09/25/tech/ios-13-keyboard-warning-trnd/index.html

[23] Безопасность macOS. http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_macOS

[24] СМИ узнали об отключении функции отслеживания местоположения в iPhone. https://www.rbc.ru/technology_and_media/19/01/2020/5e241ec79a794702a27571a5

[25] FT: Google обнаружила проблемы с безопасностью в браузере Safari. https://tass.ru/obschestvo/7584779.

алгоритм, использующий технологию хэширования и автоматически сканирующий загружаемые в iCloud фотографии. Официально целью данной программы является выявление фактов жестокого обращения с детьми[26].

Серьезные вопросы вызывает и легальная обработка Apple персональных данных пользователей. Все гаджеты Apple, управляемые версиями iOS, начиная с 10-й, поддерживают технологию дифференциальной безопасности. Последняя позволяет собирать данные пользователей, которыми они согласны делиться с компанией, для отслеживания шаблонов поведения клиентов. Вся собранная информация хранится до 18 месяцев и обезличивается посредством добавления «математического шума». Последнее дает возможность разорвать связь между устройством и конкретным набором данных. Однако исследования, проведенные сотрудниками университетов Южной Калифорнии, Индианы и Цинхуа показали, что на практике на сервера Apple отправляется гораздо больше «незашумленной» информации данных, чем заявлено официально.Значение эпсилона (параметра «зашумление» данных) больше 1 рассматривается как угроза для безопасности. Однако для macOS 10.12 значение эпсилон достигало 6, а для iOS 10 – 14. В бета-версии iOS 11 значение эпсилон составляло 43. Таким образом, Apple почти не применяет «зашумления» собранных данных и имеет возможность в любой момент привязать набор информации к конкретному устройству и его пользователю[27].

Отдельно необходимо отметить рекордно высокое количество ошибок в последней версии (13-й) версии операционной системы iOS. За первые 2 месяца с момента запуска iOS 13 потребовались 8

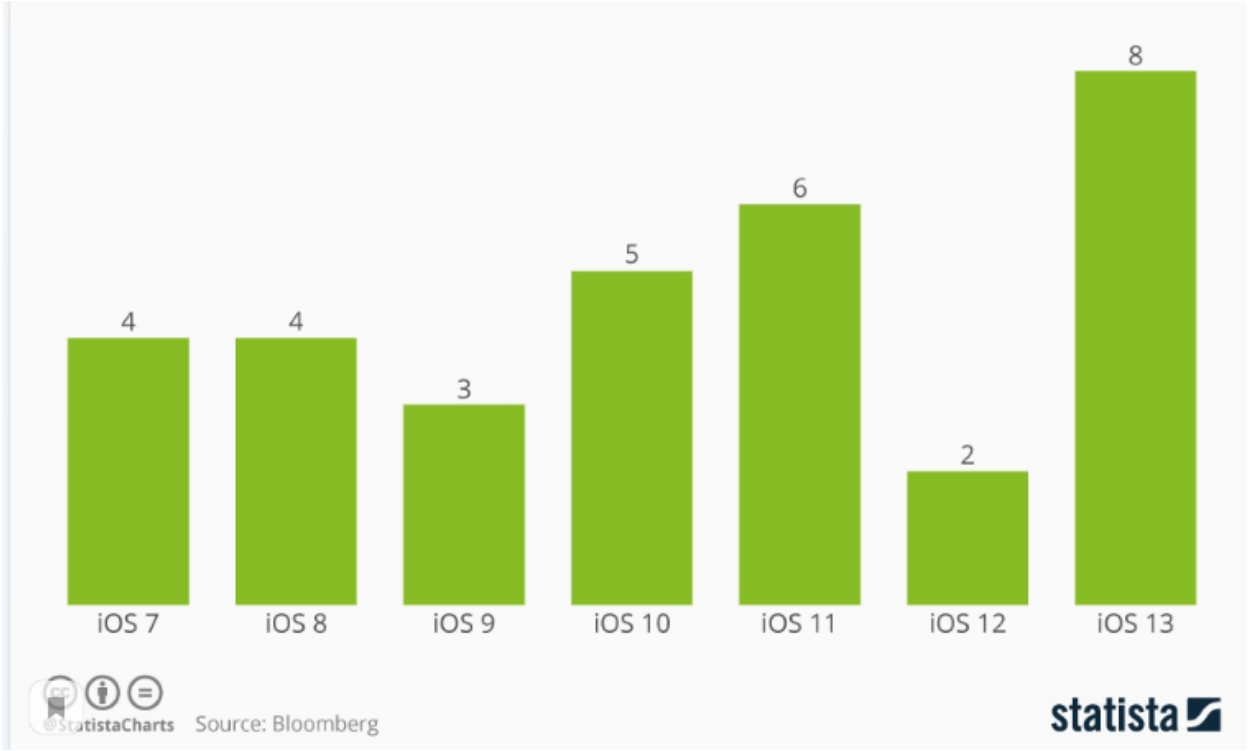
[26] Apple объяснила сканирование фото в iCloud жестоким обращением с детьми. https://www.rbc.ru/technology_and_media/09/01/2020/5e1721789a79472a05a679f7

[27] Apple собирает ваши личные данные и врёт. Как это отключить? https://www.iphones.ru/iNotes/784442

обновлений для устранения уязвимостей и ошибок. Для сравнения, за аналогичный период 12-я версия iOS была обновлена 2 раза, 11-я – 6, 10-я – 5, 9-я – 3.

Рис. 4

Число обновлений операционных систем iOS за первые два месяца после выпуска[28]



Соответственно, мы можем заключить, что на фоне неоднократного возникновения критически значимых уязвимостей компания Apple, вероятно, умалчивала о существующих проблемах, желая избежать падения рыночной стоимости акций, снижения объема продаж и судебных исков о компенсации ущерба. Накопленный опыт показывает, что пользователи не могут доверить самой компании единолично обеспечивать информационную безопасность собственной продукции.

Необходимость контроля за работой компании на данном

[28] Apple's iOS 13 Has Needed More Bug Fix Updates Than Ever. https://www.statista.com/chart/20118/apple-ios-updates-bug-fixes/

направлении подтверждает и очевидная необходимость балансировать коммерческие и общественные интересы. Заинтересованность топ-менеджмента Apple в отдельных случаях приобретает гипертрофированные формы. В качестве наглядного подтверждения в данном случае можно привести вскрывшийся в декабре 2017 г. факт: компания искусственным образом замедляла работу смартфонов старых моделей. Представители корпорации длительное время отрицали это, а после обнародования результатов соответствующих исследований резко изменили позицию, пытаясь оправдать замедление процессоров смартфонов якобы имевшим место желанием продлить «срок жизни» литий-ионных батарей. (Процесс замедления запускался после начала их разрядки). Однако власти большинства государств, как и представители экспертного сообщества, усмотрели в этом попытку подтолкнуть потребителей к приобретению новых смартфонов компании. Власти Италии даже наложили на корпорацию штраф в размере €10 млн.[29]

Сотрудничество со спецслужбами и властями США

В сентябре 2012 г. группа хакеров под названием AntiSec опубликовала базу данных, включавшую в себя более 1 млн. UDID – уникальных идентификаторов устройств Apple, от использования которого разработчикам неоднократно рекомендовали воздержаться по соображениям конфиденциальности. Как было заявлено злоумышленниками, опубликованная база вмещает в себя лишь часть данных о 12 млн. устройств, похищенных с ноутбука сотрудника ФБР в Нью-Йорке. Официально ведомство отрицает свою связь с указанной базой данных. Впоследствии небольшая IT-компания BlueToad заявила о том, что база данных UDID якобы была похищена с ее устройств, не уточняя, однако, откуда фирма могла

[29]Apple и Samsung впервые оштрафовали за замедление старых телефонов. https://habr.com/ru/post/427749/

получить доступ к этой информации[30].

Однако менее чем через год связь Apple со спецслужбами США была официально подтверждена. Первоначально информация о широкомасштабной утечке документов Агентства национальной безопасности, указывающих на сотрудничество корпорации с данным ведомством, повлекла за собой появление резонансных публикаций в изданиях Guardian и Washington Post. 6 июня 2013 г. сенаторы Дайан Файнштейн и Саксби Чамблисс официально подтвердили факт сотрудничества АНБ с крупными технологическими компаниями США. Как выяснилось, сотрудники спецслужбы имеют прямой доступ к серверам Apple, обладая правом собирать данные о клиентах компании, не являющихся гражданами США и проживающих за пределами Соединенных Штатов[31].

Следует отметить, что еще до подключения Apple к соответствующим программам, у компании уже имелись тесные связи с разведывательным сообществом Соединенных Штатов. Достаточно упомянуть тот факт, что служба глобальной безопасности Apple укомплектована преимущественно за счет бывших сотрудников Агентства национальной безопасности США и ушедших в отставку военнослужащих[32].

В пользу сотрудничества Apple со спецслужбами, работающими непосредственно внутри территории США и преимущественно с американскими гражданами, свидетельствует недавняя публикация Reuters. Как стало известно журналистам издания, Apple в течение

---

[30] UDID leak source ID'd: BlueToad mobile firm says it was hacked. https://www.cnet.com/news/udid-leak-source-idd-bluetoad-mobile-firm-says-it-was-hacked/; Why the Apple, FBI and AntiSec UDID debacle won't go away. https://www.cnet.com/news/why-the-apple-fbi-and-antisec-udid-debacle-wont-go-away/

[31] U.S. Confirms That It Gathers Online Data Overseas. https://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.htm

[32] Tech Nations. Welcome to Apple. A one-party state https://members.tortoisemedia.com/2020/01/06/day-1-apple-state-of-the-nation-2/content.html

более чем 2-х лет занималась разработкой системы сквозного шифрования копий iCloud. Однако в итоге руководство компании отказалось от этого проекта со стороны ФБР. В связи с сопутствующим скандалом часть экспертов акцентировали внимание на скрытые риски пользования сервисом iMessage. Хранимая в нем переписка защищена сквозным шифрованием. Однако существует возможность получить доступ к ее копии в iCloud[33].

О наличии у корпорации Apple тесных связей с властями США также свидетельствует активная роль этой компании в осуществлении политической цензуры. Так, в августе 2018 г. Apple удалила все подкасты сайта InfoWars, принадлежащего известному публицисту Алексу Джонсу. В качестве причины удаления контента было указано «разжигание ненависти», хотя все критика Джонса была адресована в адрес истеблишмента США и аффилированных с элитами крупных СМИ. Он не занимался разжиганием вражды на этнической, расовой, религиозной почве. В выступлениях Джонса речь шла лишь о критике политики элит с консервативных позиций. Важно отметить, что решение Apple спровоцировало полномасштабную кампанию американских технологических корпораций, преследующую цель информационной изоляции Алекса Джонса. Вслед за Apple его учетные записи начали блокировать Facebook , YouTube , Spotify и Google[34].

Известны случаи, когда Apple удалял контент по политическим мотивам даже в ситуациях, когда у компании объективно отсутствовал повод обвинить создателей информации в разжигании

[33] ФБР заставило Apple отказаться от шифрования копий iCloud. https://www.iphones.ru/iNotes/fbr-zastavilo-apple-otkazatsya-ot-shifrovaniya-kopiy-icloud-01-21-2020

[34] Alex Jones and Infowars Content Is Removed From Apple, Facebook and YouTube. https://www.nytimes.com/2018/08/06/technology/infowars-alex-jones-apple-facebook-spotify.html

ненависти к каким-либо социальным группам. Например, в декабре 2009 г. Apple был наложен запрет на распространение приложения для создания мультфильмовNewsToons, разработанного при участии карикатуриста Марка Фиоре. Причина наложения санкций была сформулирована следующим образом: посредством приложения пользователи получали возможность высмеивать общественных и политических деятелей США. Запрет был снят лишь после того, как в 2010 г. Фиоре получил Пулитцеровскую премию за свои политические карикатуры, и в защиту его приложения начали выступать крупные лидеры общественного мнения[35].

Равным образом Apple активно содействует властям США в применении санкционных механизмов (когда это напрямую не противоречит бизнес-интересам компании). В частности, в феврале 2017 года Apple ограничила работу платежных сервисов на устройствах, приобретенных покупателями из Ирана. В августе того же года компания удалила многие иранские приложения из App Store, обосновывая это необходимостью соблюдать санкции, наложенные Вашингтоном на Тегеран[36].

С учетом этих фактов становится очевидно, что в целом ряде ситуацийApple выступает не как коммерческая структура, а как ресурс влияния властей Соединенных Штатов. Последнее подразумевает необходимость создания правовых и технологических барьеров для реализации компанией негласных функций, которые она выполняет в интересах политического руководства США.

Апологеты Apple пытаются опровергнуть точку зрения о тесной

---

[35]Apple Rejects Pulitzer Prize Winner's App. https://www.pcworld.com/article/194387/apple_rejects_pulitzer_prize_winners_app.html

[36] Apple, Citing U.S. Sanctions, Removes Popular Apps in Iran. https://www.nytimes.com/2017/08/24/technology/apple-iran.html

связи корпорации со спецслужбами, ссылаясь на отказ руководства компании создать операционную систему с бэкдором. При этом в качестве примера чаще всего приводят отказ руководстваApple выполнить решение суда, предписывавшего отключить встроенную функцию защиты iPhone одного из участников теракта в Сан-Бернардино (Калифорния). Однако защитники Apple предпочитают не упоминать о том, что спецслужбы Соединенных Штатов в принципе не нуждаются в такого рода бэкдорах или согласии корпорации на отключение защиты. Защита смартфона террориста из Сан-Бернардино была взломана ФБР. Проведенное в октябре 2019 г. исследование Национального института стандартов и технологий США показало, что даже созданные частными компаниями (такими как Cellebrite, Grayshift и MSAB) программы для взлома смартфонов пригодны для преодоления защиты устройств Apple. Более того, это программное обеспечение уже активно используют полиция США и ФБР[37].

Заключение

В отличие от многих иных американских технологических компаний, Apple зарегистрировала свои дочерние структуры в России и продемонстрировала готовность соблюдать требования законодательства РФ. Так, Apple локализовала персональные данные пользователей россиян и зарегистрировалась в качестве оператора персональных данных[38]. Это само по себе исключает возможность строго репрессивного подхода в рамках выстраивания

---

[37] Apple отказалась помочь ФБР разблокировать iPhone стрелка из Сан-Бернардино. https://lenta.ru/news/2016/02/17/apple/; Government Report Reveals Its Favorite Way to Hack iPhones, Without Backdoors. https://www.vice.com/en_us/article/n7jevz/government-report-reveals-its-favorite-way-to-hack-iphones-without-backdoors; Test Results for Mobile Device Acquisition. https://www.dhs.gov/publication/st-mobile-device-acquisition.

[38] Apple перенесла в Россию персональные данные россиян. https://cnews.ru/news/top/2019-01-30_apple_stala_operatorom_personalnyh_dannyh_v

взаимоотношений российских властей с компанией. Но также очевидна и недопустимость игнорирования наметившихся угроз.

Их нейтрализации могла бы способствовать реализация следующих мер:

- создание площадки для организации постоянного диалога между представителями Apple, российских IT-компаний, профильных структур исполнительной власти РФ, федеральных законодателей, общественных деятелей и специалистов в области кибербезопасности;

- выпуск протокола информационной безопасности, обязательного к исполнению сотрудниками определенных ведомств и госслужащими, относящимися к числу носителей конфиденциальной информации. Протокол должен охватывать вопросы пользования компьютерами и гаджетами не только на рабочем месте, но и на прилегающей к зданию территории, во время передвижений на определенной дистанции от места работы во время, до начала и после завершения рабочего дня. Также необходимо строго регламентировать возможность наличия определенных гаджетов у участников совещаний, в ходе которых предметом обсуждения выступают вопросы, имеющие отношение к государственной тайне;

- формирование постоянно действующей структуры, целевым образом занимающейся поисками уязвимостей в продукции Apple и иных зарубежных технологических корпораций, занимающих сопоставимую долю на рынке РФ. Данная организация может быть создана путем кооперации усилий государства и крупных российских компаний, специализирующихся на борьбе с киберугрозами;

- создание премиального фонда для российских IT-специалистов, обнаруживших уязвимости в продукции Apple и иных зарубежных технологических корпораций;

- оказание материальной поддержки в грантовой форме объединениям IT-специалистов, на системной основе занимающихся решением вопросов информационной безопасности и популяризацией ее навыков среди населения;

- запуск поэтапных, рассчитанных на долгосрочную перспективу программ по созданию отечественного программного обеспечения и аппаратной базы, сопоставимых по качеству с продукцией Apple;

- увеличение размера штрафов за нарушение действующего законодательства в отношении обращения с персональными данными для юридических лиц, аффилированных с зарубежными коммерческими или государственными структурами;

- общее ужесточение законодательства, регулирующего обращение с персональными данными, по примеру государств Евросоюза;

- внедрение курсов информационной безопасности в учебные программы средней и высшей школы;

- учреждение премии для журналистов и блогеров, специализирующихся на тематике обеспечения кибербезопасности;

- создание на площадках социальных медиа информационно-развлекательного проекта, ориентированного на популяризацию знаний об уязвимостях смартфонов и гаджетов.