СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17.01–30.01)

2019 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17.01–30.01)
№ 2

Засновники:
Національна бібліотека України імені В. І. Вернадського
Служба інформаційно-аналітичного забезпечення
органів державної влади (СІАЗ)

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
І. Терещенко

Заснований у 2011 році
Виходить двічі на місяць

Київ 2019

ЗМІСТ

Орфографія та стилістика матеріалів – авторські

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

19.01.2019
В Facebook появится сервис гифок и мемов LOL

В социальной сети Facebook в ближайшее время может появиться новый раздел под названием LOL, который будет посвящен мемам и гифкам. По данным издания TechCrunch, компания уже приступила к его тестированию (IGate).

Как рассказали приближенные к Facebook источники, работы над созданием специальной развлекательной ленты велись на протяжении нескольких месяцев. В нее будут автоматически попадать веселые короткие видео, популярные мемы и гифки, опубликованные в Facebook. LOL будет разделена на несколько тематических категорий, вроде «Животные», «Школа», «Для тебя» и тому подобное. Известно, что в новом разделе будет предусмотрена кнопка «Поделиться», а также возможность загружать свой контент.

На данный момент LOL проходит обкатку. Для тестирования были задействованы около 100 старшеклассников. В компании подтвердила изданию испытания нового сервиса, отметив, что вне зависимости от результатов тестирования, LOL не станет частью видеораздела Watch.

Собеседники TechCrunch считают, что появление LOL можно расценивать как попытку Facebook оставаться «модным и молодёжным». Однако некоторые из них указывают, что данный формат выглядит несколько устаревшим.

***

22.01.2019
Telegram для Windows получил обновление

На Windows, Android и iOS вышла новая версия мессенджера Telegram. Для компьютеров на операционной системе от Microsoft доступно обновление 1.5.8. В нем разработчики сфокусировались на улучшении настроек групп, а также различных доработках, которые в целом улучшат взаимодействие с приложением. К примеру, появилась возможность выбрать тип используемых эмоджи. На выбор доступно четыре варианта (Apple, Android, Twitter и EmojiOne). К сожалению, эмоджи Windows 10 не поддерживаются (InternetUA).

Список изменений в новой версии:

– Глобальные настройки для групп. Ограничивайте всех членов групп и все группы одновременно, запрещая или разрешая публикацию определенного типа контента. К примеру, группа, где запрещены гифки или стикеры.

– Объединенные настройки групп. Делайте группы публичными, устанавливайте права Администраторов, настраивайте историю и другие параметры всего в пару кликов в любой группе.

– Появилась возможность выбрать один из четырех наборов эмоджи в настройках чата.

– Появилась возможность настроить устройства ввода и вывода для звонков в Telegram в настройках приложения.

– Появилась автоматическая загрузка файлов и музыки.

Обновление получила версия из официального сайта Telegram.

***

22.01.2019

Facebook позволит создавать политические петиции

Facebook готовит новую функцию для социальной сети, получившей название Community Actions («Действия сообщества»). Она позволит пользователям создавать онлайновые петиции, чтобы привлечь внимание политиков к тем или иным проблемам (InternetUA).

Авторы смогут придумать заголовок, добавить описание и необходимые изображения, а также отметить соответствующие государственные органы и должностных лиц, которые будут уведомлены о существовании петиции. Чем больше людей нажмут кнопку «Поддержка», тем выше вероятность того, что предложение станет вирусным.

Каждое «действие сообщества» получит собственную ленту обсуждений, где поддержавшие его пользователи смогут оставлять комментарии, организовывать сборы средств, а также мероприятия или кампании. Более того, все желающие смогут создавать контракции в знак протеста против определенной петиции.

Community Actions в скором времени станут доступны американским пользователям Facebook. Компания пока не сообщает, станет ли доступно нововведение жителям других регионов.

***

23.01.2019

Netflix переходит в Instagram

В Instagram появится возможность делиться любыми фильмами Netflix в Stories (Телекритика).

Хотите обновить ленту в Instagram, но все, чем вы были заняты в прошедшие выходные, – просмотр сериалов в Netflix?

Теперь появилась возможность практически проводить собственную промокампанию в поддержку любимого сериала на своей странице в Instagram. Как удачно подметил TechCrunch, появилась новая функция, позволяющая делиться постером или ссылкой любимого Netflix шоу в Stories всего лишь

двойным кликом на кнопку Share. После этого другие пользователи Netflix смогут увидеть вашу «стори» вместе с линком watch on Netflix, который переведет на страничку любимого сериала. Первыми протестировать новую функцию смогут пользователи iOS. Android-версия пока в разработке, но мы очень ждем.

***

23.01.2019
Twitter показал новый дизайн

Twitter сообщил, что часть пользователей теперь может переключиться на новый интерфейс веб-версии сервиса (InternetUA).

Среди основных изменений – общее упрощение дизайна, сокращение числа колонок с контентом до двух, увеличенные кнопки для отправки твита или ответа, появление кнопки для добавления emoji. Также в новом дизайне увеличили шрифты, скрыли подписи у иконок в меню и перенесли блок с трендами в правую часть сайта.

Текущее обновление дизайна не принесло никаких ранее анонсированных изменений.

***

25.01.2019
Facebook закрывает сервис Moments

Компания Facebook решила закрыть свой не самый успешный сервис Moments, при помощи которого можно было обмениваться фотографиями, не загружая их в социальную сеть. Приложение прекратит работу 25 февраля, сообщает издание Cnet (IGate).

Разработчики запустили специальный сайт для того, чтобы пользователи смогли выгрузить свои фотографии на устройство или же перенести их в закрытый альбом на Facebook.

Отметим, что Moments начал свою работу в июне 2015 года. За три с половиной года своего существования сервису так не удалось стать популярным среди пользователей Facebook: по данным исследователей Sensor Tower, с момента запуска приложение установили лишь 87 миллионов человек, тогда как ежемесячная аудитория Facebook превышает 2 миллиарда.

***

26.01.2019
Facebook объединит функции Messenger, Instagram и WhatsApp

Об этом заявила The New York Times. Три сервиса останутся отдельными приложениями, но позволят совершать коммуникацию между ними. К примеру, пользователь Messenger сможет поделиться информацией с другом на

WhatsApp. Все три приложения предложат сквозное шифрование, отметил представитель компании CNBC. The Times отмечает, что интеграция между WhatsApp, Messenger и Instagram была разработана, чтобы удержать пользователей от миграции в другие конкурирующие сервисы (Marketing Media Review).

***

26.01.2019

Twitter тестирует отметку для оригинальных постов

Сервис микроблогов Twitter тестирует новую отметку, которая обозначает автора первоначальной публикации. По мнению разработчиков, это позволит пользователям быстрее находить комментарии автора поста, сообщает издание TechCrunch (InternetUA).

Новая опция также позволит бороться с распространением дезинформации и мошенничеством – часто мошенники регистрируются под похожими никнеймами и распространяют ложную информацию.

В начале недели Twitter сообщил, что тестирует новый дизайн десктопной версии сервиса. Например, появится большая кнопка с эмодзи и обновится раздел с самыми популярными твитами.

***

27.01.2019

В Skype теперь можно поделиться файлами из OneDrive

Отправка файлов через мессенджер Skype отныне будет гораздо проще, поскольку в приложении появилась интеграция с облачным хранилищем Microsoft OneDrive. Доступ к этой функции дали инсайдерам еще в ноябре, а теперь все пользователи стабильных версий Skype могут воспользоваться возможностью отправки файлов любого размера (InternetUA).

OneDrive можно найти в списке дополнений для Skype наряду с To-Do, Spotify, YouTube, Giphy, MSN Погода и другими. Вам надо нажать на кнопку с плюсом, выбрать OneDrive и войти в свою учетную запись. При отправке больших файлов из OneDrive Skype сгенерирует ссылку на этот объект, после чего получатель сможет загрузить файл, перейдя по ссылке. Нативная система отправки файлов в Skype поддерживает объекты только до 300 Мб.

Интеграция с OneDrive доступна на всех платформах, где поддерживается Skype, за исключением лишь macOS и Linux, но эти операционные системы получат дополнение OneDrive для Skype в ближайшем будущем.

***

27.01.2019

Половина активных пользователей Facebook – боты

Аарон Гринспен называет себя создателем одного из прототипов самой большой соцсети мира – которым позже и воспользовался Марк Цукерберг. В 70-страничном отчете он утверждает, что сейчас Facebook – не лидер IT-отрасли, а колосс на глиняных ногах. И соцсеть ожидает судьба MySpace и AOL.

Докладніше

***

30.01.2019
В Skype добавили возможность отправки sms-сообщений

Microsoft выпустила новую версию мессенджера Skype 8.37.0.98, которая получила ряд дополнений и улучшений, например отправку смс-сообщений и функции быстрого доступа, сообщает Android Police (InternetUA).

В Skype теперь можно получать SMS-сообщения. Для этого пользователю нужно иметь зарегистрированный номер в мессенджере и настроить идентификацию вызывающего абонента. Функция пока доступна в США, но в ближайшие недели достигнет и другие страны.

Новая панель контактов стала более удобной и получила больше возможностей для настройки контактов, а в «Чатах» появилась возможность легче находить людей, с которыми пользователь может быть знаком. Также можно добавлять телефонный номер к существующему контакту через его профиль.

Для мобильных устройств с Android 6 и выше появилась возможность открывать недавние чаты, изменять статус, начинать новый диалог или звонок, нажав и удерживая иконку приложения на дисплее. Помимо этого, в новом Skype можно выбирать тип подключения – Wi-Fi или сотовую связь – для автоматического скачивания новых фотографий.

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

24.01.2019
Зеленський з лопатою запустив черговий флешмоб

Шоумен Володимир Зеленський закликав українців брати лопати та розчищати Україну від снігу, «допоки політики на сніданку в Давосі» (Espreso.tv).

Відповідне відео Зеленський опублікував у своєму Facebook.

Відео опубліковано із закликом «Давайте почистимо країну. Розпочнемо зі снігу» і має свій хештег #lopatachallenge.

***

28.01.2019

Українсько-кримськотатарський флешмоб перед палацом англійської королеви

У неділю, 27 січня, представники української і кримськотатарської діаспори в Лондоні провели перед Букінгемським палацом флешмоб в рамках акції «Об'єднані прапором – #LIBERATECRIMEA», на якому розгорнули і підписали кримськотатарський прапор, який протягом 9 місяців подорожує по всьому світу і 26 червня, на день кримськотатарського прапора, повернеться до Києва (Український погляд).

***

30.01.2019

В сети показали яркое видео флешмоба военных на вокзале Киева в память о героях Крут

Наталия Митрофанова

29 января на железнодорожном вокзале военный оркестр Киевского гарнизона и сводного хора организовал яркое выступление. Флешмоб был посвящен Дню памяти Героев Крут (Україна нова).

О мероприятии рассказал пресс-центр «Укрзализныци». «29 января в 17:00 на Центральном железнодорожном вокзале Киева, в вестибюле, прошел флешмоб в память о погибших героях битвы под Крутами», – сказано в сообщении.

В акции приняли участие военный оркестр Киевского гарнизона и сводного хора.

Пассажиры наблюдали за происходящим и снимали мероприятие на видео.

***

30.01.2019

Сервісні центри МВС запустили чат-бота в Facebook

30 січня головний сервісний центр МВС запустив чат-бота «Автобот» у Facebook (Espreso.tv).

Про це повідомила прес-служба у Facebook.

«Ми запустили чат-бота на ім'я "Автобот", який консультуватиме громадян на сторінці Facebook Головного сервісного центру МВС», – йдеться у повідомленні.

Тепер бота можна запитати про те, як зареєструвати машину, отримати довідку про несудимість. Можна також оформити або замінити водійське посвідчення, зареєструватися в електронному кабінеті водія, замовити

індивідуальні номерні знаки і дізнатися про роботу мобільних сервісних центрів МВС.

Чат-бот будуть вдосконалювати для того, щоб він міг відповідати на усі запити користувачів.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

18.01.2019
Павел Дуров поделился планами по развитию Telegram в 2019 году

Основатель и глава мессенджера Telegram Павел Дуров решил подвести итого прошлого года и поделится планами на 2019-ый (IGate).

На своем канале в Telegram Дуров написал, что 2018 год был выдающимся для его компании, однако нынешний должен стать «самым важным в истории мессенджера». В первую очередь, пользователям следует ждать значительного расширения функционала сервиса: «2019 год станет временем, когда пожелания пользователей станут реальностью», – написал Дуров, намекая на появления долгожданных функции.

Руководитель Telegram также отметил рост популярности мессенджера: «Telegram – один из немногих сервисов для обмена сообщениями, у которого в минувшем году наблюдался заметный рост по всему миру».

Отметим, что в 2018 году активная аудитория мессенджера увеличилась на треть, а финансирование возросло более чем в 10 раз. И это все при том, что в России, где продукт был особо популярен, была введена блокировка.

***

21.01.2019
Facebook занялся исследованиями этики искусственного интеллекта

Facebook очень хочет избавиться от клейма компании, шпионящей за пользователями, которое привязалось к ней в 2018 году после нескольких громких скандалов с утечками данных. Для этого крупнейшая социальная сеть заключила договор с Техническим университетом Мюнхена, в рамках которого стороны займутся созданием независимого исследовательского центра по этике искусственного интеллекта (IGate).

Facebook выделит на изучение данного вопроса грант в размере $7,5 миллионов. Он будет потрачен в течение пяти лет. Компания также предоставит специалистам центра доступ базам данных и инструментам, связанным с ИИ.

В Facebook заявляют, что на решение инвестировать в исследования в сфере этики искусственного интеллекта компанию побудили обвинения в

предвзятости алгоритмов соцсети, которые отвечают за формирование пользовательской ленты и фильтрацию контента.

***

22.01.2019

Как экономить время на создание публикаций в соцсетях: постинг на автопилоте

Посты в социальных сетях – отличный инструмент для привлечения подписчиков и рекламы своего блога, бренда товаров и услуг, публичной личности, в конце концов. О том, как не тратить лишних усилий и времени на создание и публикацию контента, мы спросили у настоящих профессионалов медиа маркетинга (IGate).

Так, автоматический постинг в социальных сетях является лучшим решением для всех, кто планирует свои публикации, а не постит время от времени, под настроение. Фишкой продвижения в социальных сетях можно считать особые часы, когда активность вашей аудитории наибольшая, так что вам лучше выпускать пост именно в это время, даже если оно для вас не удобно. Так вы охватите больше пользователей и привлечете переходы в профиль, что положительно отразится на вашем рейтинге.

«И тут на помощь приходит сервис отложенного постинга. Вы создаете контент для постов тогда, когда вам удобно, затем загружаете его на сервис и задаете дату и время публикации. Таким образом можно спланировать недели и месяцы контента вперед, это очень удобно», – рассказали смм-эксперты сервиса PublBox.

Отложенный постинг хорош еще и тем, что позволяет создавать контент по определенному плану, что делает его более продуманным и эффективным. А специальные сервисы, такие как PublBox, помогают оформить и организовать посты для всех социальных сетей, предлагая готовые контент-планы и шаблоны публикаций.

***

22.01.2019

State of Social: на каких форматах сфокусируются маркетологи в 2019 году

Buffer выпустила результаты ежегодного исследования. Многие бренды используют формат Stories. Мессенджеры все еще недооценены. Несмотря на популярность таких платформ, как WhatsApp и Messenger, почти 71 % брендов не используют мессенджеры для маркетинга. 50 % маркетологов не планируют использовать мессенджеры в 2019 году.

Докладніше

***

22.01.2019

Facebook возобновил испытания беспилотников для раздачи интернета в труднодоступных районах

Facebook возобновил тестирование своих беспилотных летательных аппаратов на солнечных батареях для раздачи интернета в труднодоступных районах Земли. Теперь компания заручилась поддержкой Airbus, а испытания дронов проходят в Австралии, пишет TechCrunch (InternetUA).

По данным издания NetzPolitik, Facebook и Airbus дорабатывали систему в течение прошлого года, а первые испытания новых летательных аппаратов Zefir T прошли в ноябре и декабре.

Представитель Facebook подтвердил, что компаний продолжает разработку системы раздачи интернета вместе с партнерами, однако отказался уточнить детали.

Ранее Facebook закрыл проект Aquila по разработке небольших беспилотных самолетов на солнечных батареях. Планировалось, что аппараты должны летать на высоте в 18 км и обеспечивать подключение к интернету в труднодоступных районах мира при помощи лазерного луча.

***

24.01.2019

Покупатели скептически относятся к дополненной реальности, ботам и соцсетям

Согласно новому исследованию, проведенному Oracle NetSuite в партнерстве с Wakefield Research и The Retail Doctor, пользователи не хотят разговаривать с роботами при совершении покупок в магазине или через Интернет.

Докладніше

***

28.01.2019

Facebook в 27 % случаев неверно определяет интересы пользователей

Около трети (27 %) пользователей Facebook в США считают, что соцсеть неправильно определяет их интересы в разделе «Рекламные предпочтения». Об этом свидетельствуют результаты опроса Pew Research Center (InternetUA).

Более того, 74 % респондентов не знают о том, что Facebook составляет списки их предпочтений, и лишь 51 % пользователей не беспокоит тот факт, что соцсеть собирает эту информацию.

При переходе на страницу «Рекламные предпочтения» 88 % опрошенных пользователей увидели, что сайт определил их интересы. Тем не менее, лишь 59 % респондентов заявили, что эти категории отражают их реальные интересы.

Интересы, которые Facebook фиксирует в разделе «Рекламные предпочтения», используются для таргетинга. Однако, судя по результатам опроса, 100 %-го попадания ожидать не стоит. Вполне разумно ожидать, что какой-то процент объявлений будет показан неподходящим людям.

Исходя из полученных результатов, в Pew Research Center пришли к выводу, что алгоритмы Facebook не всегда точно «угадывают» интересы пользователей на основании данных об их активности.

Опрос среди пользователей соцсети проводился с сентября по октябрь 2018 года. В нём приняли участие 963 респондента старше 18 лет.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

20.01.2019

Британские ученые выяснили, что гаджеты влияют на психическое состояние подростков не больше, чем картофель

Психологи из Оксфордского университета, воспользовавшись большим (более 355 тысяч участников) датасетом с информацией о жизни и здоровье подростков, родившихся в начале 2000-х годов в США и Великобритании, изучили, как использование гаджетов связано с психическим состоянием молодежи.

Докладніше

***

24.01.2019

Почему нужно ограничивать себя в использовании смартфонов

Учёные рассказали, какой вред психическому здоровью человека наносит длительное использование смартфонов (InternetUA).

В частности, исследованием данного факта занимались психолог Университета Вирджинии Костадин Кушелёв и сотрудники Университета Британской Колумбии. Так, они провели наблюдение за студентами-добровольцами. Последних разделили на группы: их попросили поставить смартфоны на вибрацию, беззвучный режим и полную громкость. Как показало исследование, те, кто бросался к гаджету при каждом сигнале, имели симптомы дефицита внимания, а также страдали от гиперактивности.

Кроме того, специалисты предложили студентам посетить кафе. Здесь добровольцев также разделили на группы. Представители первой могли беспрепятственно пользоваться смартфонами. А вторая группа должна была вовсе убрать гаджеты на период дружеской встречи. По итогу эксперимента добровольцы поделились своими эмоциями от пребывания в кафе с близкими людьми. Те, кто не имел возможности пользоваться гаджетами, признались, что провели время намного веселее, чем обычно. Они отметили, что прямая коммуникация с людьми намного эффективней и интересней, чем виртуальная.

***

24.01.2019

Привязанность к смартфону может указывать на психические нарушения

Ученые Университета Вирджинии заявили о том, что привязанность к смартфону может указывать на психические нарушения – чем интенсивнее человек использует гаджет, тем выше вероятность того, что его психика не стабильна. В частности, установлена связь между привязанностью к своему телефону и риском СДВГ – синдрома дефицита внимания и гиперактивности (InternetUA).

Исследователями был проведен эксперимент с участием студентов, которые были произвольно поделены на группы: в одной добровольцы должны были переключать смартфон на режим вибрации, в другой – на беззвучный режим, в третьей – на полную громкость. Спустя несколько недель ученые заключили: люди, которые постоянно отвлекаются на свой телефон, чаще других имеют симптомы дефицита внимания и гиперактивности (СДВГ).

Следующий эксперимент был проведен в музее науки в Ванкувере. В нем участвовали родители с детьми. Часть из них по просьбе ученых должна была использовать смартфон во время экскурсии как можно чаще, другая часть – сократить до минимума. В результате наиболее привязанные к своим смартфонам пользователи заявили в финале, что вышли из музея с чувством абсолютно бессмысленного времяпровождения.

Ученые считают, что смартфоны перестали выполнять свою главную функцию – объединять людей. Вместо этого они способствуют социальной изоляции и развитию психических нарушений, которые из незначительных становятся более существенными.

«Чем чаще люди обращаются за информацией к смартфонам и чем сильнее привязаны к ним, тем меньше они доверяют незнакомцам, а также соседям и представителям других конфессий и национальностей», – сообщили специалисты.

***

28.01.2019

Почему нельзя публиковать детские фото в Интернете

Многие считают, что соцсети – это своего рода семейный альбом, который можно показывать всем. Увы, последствия могут быть ужасающими.

Докладніше

Маніпулятивні технології

22.01.2019
Система манипуляций Google и Facebook выходит из-под контроля

Гиганты ИТ-индустрии превращают действия человека в товар. Они незаметно контролируют каждый шаг пользователя и управляют его поведением. Система сбора информации и последующих манипуляций – это новый капитализм. О феномене новых бизнес-моделей, построенных на основе слежки, рассказывает исследовательница Гарвардской школы бизнеса Шошанна Зубофф.

Докладніше

***

21.01.2019
WhatsApp обмежує пересилання повідомлень для боротьби з фейками

Раніше одне повідомлення можна було переслати 20 раз, відтепер – 5 (Espreso.tv). Про це повідомляє BBC.

Раніше подібне обмеження запровадили Індії. Тоді місцева влада звинуватила WhatsApp у тиражуванні фейкових новин, які спричинили негативні настрої у суспільстві.

Компанія визнала експеримент успішним і вирішила поширити його на всіх користувачів.

BBC зазначає, що новий ліміт дозволить відправити одне і те ж повідомлення не більше ніж 1280 користувачам, тоді як раніше ця цифра становила понад 5 тис. чоловік (в групі в WhatsApp може бути максимум 256 осіб).

***

28.01.2019
Выявлена растущая опасность знакомств в Интернете

Британская полиция зафиксировала беспрецедентный рост сообщений об обманах и преступлениях, совершаемых с помощью приложения для знакомств Tinder (InternetUA).

Данные приводит Daily Mail. За последние три года число пострадавших от любовников, найденных в сети, увеличилось более чем в два раза. В 2015-м

правоохранители зафиксировали 442 обращения, а в 2018 году – почти 1,1 тысячи.

Полиция не уточнила характер обращений от жертв. Издание отмечает, что известны случаи, когда в приложении для знакомств орудовали мошенники, насильники и убийцы. Около трети нарушений закона, связанных с сервисами, приходится на преступления сексуального характера.

Местные власти обратили внимание на эту проблему после того, как 44-летняя британка Анна Роу обнародовала свою историю. Она была обманута женатым мужчиной по имени Энтони Рэй, с которым познакомилась в Tinder.

Когда любовник исчез после полугода отношений, Роу выяснила, что он использовал чужие фото и выдумал себе биографию. Она просит правительство законодательно запретить фейковые аккаунты в приложении.

***

30.01.2019

Еврокомиссия призвала Facebook и Twitter активизировать борьбу с дезинформацией

29 января Еврокомиссия сообщила, что получила первые отчеты от интернет-компаний, в том числе Google, Facebook и Twitter, о выполнении ими требований по борьбе с дезинформацией в сети, чиновники констатировали определенный прогресс в удалении фейковых аккаунтов, но ждут от компаний дополнительных мер.

Докладніше

Спецслужби і технології «соціального контролю»

21.01.2019

В России возбудили дела против Facebook и Twitter

Роскомнадзор уличил социальные сети Facebook и Twitter в нарушении российского закона о локализации баз данных. Как сообщил ТАСС пресс-секретарь ведомства Вадим Ампелонский, в отношении компаний заведены административные дела (InternetUA).

Ампелонский уточнил, что служба не получила содержательных ответов по этому вопросу от Twitter и Facebook. Он подтвердил, что 21 января 2019 года Роскомнадзор начнет административное производство в отношении компаний.

В формальных ответах компаний не содержалось никакой конкретной информации об исполнении российского закона, по которому персональные данные россиян должны храниться на территории России, утверждают в ведомстве.

В декабре 2018 года руководитель Роскомнадзора Александр Жаров сообщил, что ведомство направило Twitter и Facebook требования о

соблюдении этого закона. Ведомство ожидало получить юридически значимые ответы от компаний до 17 января 2019 года.

В противном случае в отношении компаний обещали возбудить административные дела. Им грозит штраф в размере пяти тысяч рублей. Позднее надзорная служба определит сроки, в которые социальные сети будут обязаны исполнить закон о локализации данных.

***

21.01.2019
Ирина Фоменко
Индия хочет, чтобы соцсети удаляли «незаконный» контент

Правительство Индии предложило новые правила, направленные на прекращение распространения фейковых новостей и дезинформации в социальных сетях – и местные группы активистов гражданских свобод не довольны.

Докладніше

***

21.01.2019
Входить в Интернет в России придется по паспорту

С каждым днем в России власти страны обращают все большее внимание на Интернет, который еще 5-10 лет назад совсем никак не контролировался. Теперь его пытаются всеми доступными средствами сделать «регулируемым», а для этого вводятся новые законы и требования к интернет-провайдерам.

Докладніше

***

22.01.2019
В мире все чаще практикуют отключение Интернета во время протестов

Вслед за массовыми протестами, которые начались в Зимбабве 14 января после резкого подорожания топлива, местные власти недавно полностью блокировали доступ в интернет в стране. Крупнейший провайдер Зимбабве – компания Econet Wireless – сообщил об отключении своих услуг по приказу главы государства.

Докладніше

***

22.01.2019
СБУ викрила російського пропагандиста, який провокував сепаратизм у Західній Україні

Чоловік адміністрував антиукраїнськими інтернет-групами та закликав до сепаратизму західні регіони України (Espreso.tv).

Про це повідомляє прес-служба СБУ у Facebook.

Російський журналіст з 2015 року перебував у складі закордонного антиукраїнського центру. На замовлення російських спецслужб він адміністрував антиукраїнськими інтернет-спільнотами.

Він робив публікації від імені вигаданих експертів, які створював негативний образ керівництва України й агітував за зміну конституційного ладу.

Чоловік також підбурював до сепаратизму західні регіони. Щоб налагодити «потрібні» зв'язки, він їздив до Чернівецької та Закарпатської областей. Там журналіст записував інтерв'ю із представниками румунської та угорської нацменшин, прихильниками неорусинства. Далі ці сюжети використовувались російською пропагандою для створення негативного медійного образу української влади.

***

22.01.2019

Роскомнадзор пошел в новую атаку на Telegram, заблокировав несколько тысяч прокси-серверов мессенджера

Заблокированный в России в апреле 2018 года мессенджер Telegram в последние месяцы был доступен большинству пользователей, многие из которых ранее настроили в приложении подключение через прокси-серверы для стабильной работы Telegram. Однако 21 января Роскомнадзор напомнил о себе и предпринял новую атаку на мессенджер.

Докладніше

***

23.01.2019

Начнет ли Россия войну с Facebook и Twitter?

В Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре) снова вспомнили о Facebook и Twitter, напомнив им, что они нарушают российский закон о персональных данных.

Докладніше

***

24.01.2019

СБУ задержала киевлянина за антиукраинскую агитацию

Сотрудники Службы безопасности Украины разоблачили жителя Киева, который администрировал антиукраинские сообщества в соцсетях. Его курировали российские спецслужбы, – передает пресс-служба СБУ (InternetUA).

«Он за денежное вознаграждение получал доступ к так называемым «рекламным кабинетам» аккаунтов украинских пользователей социальных сетей Facebook и Twitter. По замыслу заказчиков, таким образом злоумышленник должен был манипулировать сознанием украинских избирателей в интересах Кремля», – говорится в сообщении.

Отмечается, что сотрудники СБУ обнаружили еще более трехсот аккаунтов, которые в ходе президентской кампании планировали использовать для политической таргетированной рекламы.

«С их помощью организаторы планировали влиять на правосознание и личный выбор избирателей, а также распространять тенденциозную и фейковую информацию для дискредитации украинской власти и правоохранительных органов», – отмечают в СБУ.

Служба безопасности передала администрации социальных сетей Facebook и Twitter информацию о выявленных аккаунтах, которые могут использоваться в РФ в ходе гибридной агрессии против Украины.

***

24.01.2019

$350 млн і можливість відкритої війни: що РФ готує до виборів в Україні

Російська Федерація додатково виділила своїм спецслужбам $350 млн для реалізації підривної діяльності на виборах в Україні у 2019 році (Espreso.tv).

Про це заявив голова Служби зовнішньої розвідки Єгор Божок, передає «Укрінформ».

За його словами, РФ спрямовує на підривну роботу своїх спецслужб в Україні «колосальні бюджети».

«Ми отримали інформацію, що Кремль наказав на цей рік додатково виділити 350 мільйонів доларів своїм спецслужбам для роботи по втручанню у вибори в Україні», – сказав Божок.

Він сказав, що гроші будуть спрямовані на проплату фейкових новин і підкуп, організацію провокацій, протестів, внутрішньополітичного тиску на керівництво держави, а також для підготовки кібератак.

За даними розвідки, влада РФ розраховує, що будь-яке перезавантаження влади в Україні «потягне за собою певний параліч державного механізму», доки вибудується нова владна вертикаль.

«Ця пауза зачепить усі сфери життя, у тому числі й військової організації, що дасть Росії вікно можливостей у кілька місяців для того, щоб безболісно окупувати Україну, як вона намагалась це зробити в 2014 році. Для цього біля наших кордонів уже перебувають майже 50 тис. російських військових з усім

озброєнням і технікою. Ступінь їх готовності варіюється від 24 до 72 годин», – сказав голова Служби зовнішньої розвідки.

***

25.01.209

МІП і Facebook обговорили протидію втручанню у виборчі процеси

23 січня 2019 року керівництво Міністерства інформаційної політики України зустрілося з представниками компанії Facebook (Міністерство інформаційної політики).

Міністр інформаційної політики України Юрій Стець, заступник Міністра Дмитро Золотухін і державний секретар МІП Артем Біденко, а також керівник напрямку публічної політики Facebook у Центральній та Східній Європі Габріелла Чех і керівник напрямку публічної політики з питань виборів Facebook Аніка Геісел обговорили співпрацю з метою забезпечення захищеності виборчих процесів в Україні від ворожих впливів.

Заступник Міністра Дмитро Золотухін наголосив на важливості недопущення використання Facebook для здійснення інформаційних атак і впливів. «Ми вдячні Facebook за неймовірну роботу, яку компанія зробила, виявивши та видаливши велику кількість пов'язаних фейкових профілів, груп і сторінок. Для нас це важливо, оскільки одна з двох виявлених мереж ботів, що керувалися з Росії, використовувалися для інформаційних операцій в Україні», – розповів він.

Габріелла Чех зазначила, що Facebook серйозно ставиться до порушень стандартів спільноти та планує посилити заходи безпеки під час проведення виборів в Україні.

Аніка Геісел розповіла про одну із функцій, що вже стала доступна українським користувачам напередодні виборчих перегонів. Відтепер в інформації про популярну сторінку можна дізнатися, з якої країни походить її адміністратор і яку активну рекламу запущено від імені сторінки.

***

28.01.2019

YouTube станет «гораздо реже» рекомендовать к просмотру ролики, в которых пропагандируются теории заговоров

Команда разработчиков YouTube начала работу по борьбе с распространением дезинформации на площадке. В рамках эксперимента американским пользователем станут гораздо реже рекомендовать ролики с «пограничным контентом», содержание которых не противоречит правилам, однако находится на грани дозволенного (IGate).

По словам представителей сервиса, изменения политики рекомендаций затронут около 1 % видео, опубликованного на YouTube.

«Мы будем реже демонстрировать в разделе рекомендаций «пограничный контент», способный навредить пользователям. К примеру, заявления от приверженцев теории плоской Земли, рекламу чудодейственных препаратов от серьезных заболеваний или необъективную информацию о трагедии 11 сентября», – указывается в заявлении компании.

По мнению команды YouTube, изменения являют собой «компромисс между выполнением обязанностей перед посетителями ресурса и свободой слова». Особо подчеркивается, что изменения касаются только возможности попадания в рекомендованный список. На поисковую выдачу они не повлияют. Кроме того, если человек подписан на канал, публикующий дезинформирующие ролики, то его контент как и ранее будет рекомендоваться с той же частотой.

***

29.01.2019

Facebook запустит два центра для борьбы с предвыборными фейками в Европе и Азии

Компания Facebook объявила о запуске двух центров, сотрудники которых займутся борьбой с распространением дезинформации в ходе предвыборных кампаний в странах Европы и Азии. Сообщение об этом было опубликовано в блоге социальной сети.

Докладніше

***

29.01.2019

Спецслужби РФ намагалися завербувати українського військового за допомогою месенджера WhatsApp

Співробітники Головного управління військової контррозвідки СБУ викрили спроби російських спецслужб вербування військових-секретоносіїв Збройних Сил України для отримання інформації в оборонній сфері.

Докладніше

***

29.01.2019

Президентські вибори: Facebook заборонить рекламу, куплену за межами України

Facebook заборонить під час виборчої кампанії в Україні розміщувати рекламу, куплену за її межами задля того, аби запобігти поширенню неправдивих повідомлень (Espreso.tv).

Про це повідомляє Радіо Свобода.

Соціальна мережа заборонить розміщувати в українському сегменті виборчі оголошення, куплені за межами України під час президентської кампанії.

«Цей крок є частиною глобальної реакції соціальної мережі на поширення неправдивих повідомлень серед 2 мільярдів користувачів», – йдеться у повідомленні.

Зазначається, що Україна впродовж кількох років звертала увагу керівництва Facebook на кампанії дезінформації, підтримувані Москвою, включно з фейковими новинами, що мають на меті викликати недовіру до нинішнього прозахідного уряду, виправдати анексію Криму та підтримку Росією бойовиків на сході країни.

***

29.01.2019

В ЕС и США не одобрили план Facebook объединить WhatsApp, Instagram и Facebook Messenger

В конце минувшей недели газета The New York Times сообщила, что руководство соцсети Facebook планирует объединить принадлежащие компании сервисы Facebook Messenger, WhatsApp и Instagram. Хотя все детали плана и сроки его реализации пока не разглашаются, сообщение NYT вызвало беспокойство в ЕС и США (InternetUA).

По данным издания, план главы Facebook Марка Цукерберга предполагает, что все три сервиса продолжат функционировать в виде отдельных приложений, но их инфраструктура будет объединена, что позволит пользователям обмениваться сообщениями между ними. Также предполагается, что все сервисы получат поддержку сквозного шифрования.

Как пишет The Verge, Комиссия Ирландии по защите данных (в этой стране зарегистрирован европейский офис Facebook) потребовала от соцсети предоставить подробности о запланированном объединении сервисов.

Хотя этот проект Facebook находится на ранней стадии, в Комиссии отметили, что намерены заранее убедиться в соответствии этой идеи требования вступившего в силу в мае прошлого года Общего регламента о защите данных (GDPR).

В США намерения Facebook вызвали серьезную критику. Так, некоторые полагают, что регуляторы должны были запретить соцсети покупку WhatsApp и Instagram. «Представьте, как отличался бы мир, в котором Facebook конкурировала бы с Instagram и WhatsApp. Это подстегнуло бы подлинную конкуренцию, защиту конфиденциальности и принесло бы выгоды пользователям», – заявил конгрессмен Ро Кханна.

***

30.01.2019

Ирина Фоменко

Закон Японии теперь позволяет взламывать IoT-устройства граждан

Япония одобрила поправку к закону, которая позволяет чиновникам взламывать устройства Интернета вещей (IoT). Об этом сообщает IoT News.

Докладніше

Проблема захисту даних. DDOS та вірусні атаки

17.01.2019

Популярный файловый менеджер для Android позволяет красть чужие данные

Один из популярнейших мобильных файловых менеджеров ES File Explorer, известный как «ES Проводник», скрывает в своём коде опасную уязвимость. Её обнаружил французский исследователь в области безопасности Баптист Роберт. По его словам, через это приложение можно получить доступ к данным других пользователей (InternetUA).

ES File Explorer, помимо доступа к содержимому мобильного устройства, позволяет управлять данными на FTP, FTPS, SFTP и WebDAV-серверах, а также в облачных хранилищах. Кроме того, с его помощью можно копировать и вставлять файлы между устройствами по Bluetooth. Но обнаруженный экспертом открытый порт с помощью специального скрипта открывает доступ к изображениям, видео и данным на карте памяти другого устройства, находящегося в той же локальной сети Wi-Fi. Более того, злоумышленник даже может удалённо запустить вредоносное приложение на смартфоне жертвы.

Эксперт отправил отчёт разработчикам приложения, но они пока не дали своих комментариев. Некоторые считают, что в такой особенности файлового менеджера нет ничего страшного, ведь злоумышленнику нужно находиться в одной сети с жертвой. Вот только при количестве установок свыше 500 миллионов найти пользователя с ES File Explorer на смартфоне в любой открытой Wi-Fi-сети не должно составить труда.

***

17.01.2019

Wi-Fi можно использовать для шпионажа за людьми внутри помещения

Wi-Fi подходит для отслеживания перемещений. Чем больше хотспотов в здании или помещении, тем точнее будет результат наблюдения. Злоумышленнику достаточно будет погулять вокруг со смартфоном в руках.

Докладніше

***

21.01.2019

Facebook заплатит по полной за нарушение конфиденциальности личных данных

Компания снова попала на скандальный крючок. На этот раз ее подозревают в нарушении соглашения о защите конфиденциальности личных данных пользователей (Телекритика).

Напомним, в 2012 году Федеральная торговая комиссия (FTC) обязала заплатить Google $22,5 млн. Facebook «повезло» больше. Ожидается, что штраф за нарушение соглашения о защите конфиденциальности личных данных пользователей будет намного больше упомянутой суммы, которая побила рекорд когда-либо выплачиваемых FTC штрафов.

Проблема в том, что для крупных корпорацию даже такой большой штраф не имеет большого значения. «Руководители Facebook, похоже, давно подсчитали, что штраф, даже в $1 млрд, – это цена быстрого роста, и компания вполне может его себе позволить. Расчет окупился: Facebook не только превратил пользовательские данные в рекламную золотую жилу, но и использовал их, чтобы подавить конкурентов и сохранить монополию», – считает журналист Fortune Джефф Джон Робертс.

***

21.01.2019

До 200 браузерных расширений уязвимы для атак через веб-сайты

Прикладные программные интерфейсы (API) браузерных расширений могут использоваться для кражи конфиденциальных сведений об истории посещения веб-страниц, а также пользовательских закладок и даже файлов куки. С помощью последних, злоумышленник может взломать активную сессию авторизованного пользователя и получить доступ к его почтовым ящиками, профилям в соцсетях и к прочим учётным записям.

Докладніше

***

21.01.2019

База Whois важна для борьбы с пиратством

Американский реестр интернет-номеров (ARIN) обратился к правительству Канады с просьбой потребовать от интернет-провайдеров продолжать вести базу IP-адресов и номеров Whois. Это помогает идентифицировать нарушителей авторских прав.

Докладніше

***

22.01.2019

Шпионаж смартфонов Huawei за владельцами подтвердили на видео

21 января 2019 года, шпионаж смартфонов Huawei за своими владельцами подтвердили на видео, причем уже сейчас любой желающий может убедиться в этом самостоятельно. Пользователи с форума Reddit обнаружили, что если использовать на телефоне от данного производителя Twitter, который заблокирован в Китае как «враждебный сервис», то скачать из него изображения не получится.

Докладніше

***

22.01.2019

Миллиарды ноутбуков, смартфонов и консолей оказались подвержены взлому по Wi-Fi

Специалисты по безопасности компании Embedi обнаружили серьёзные уязвимости в нескольких контроллерах Wi-Fi, используемых в миллиардах популярных устройств. Потенциальными жертвами злоумышленников могут стать обладатели консолей Xbox One и PlayStation 4, а также некоторых моделей ноутбуков, смартфонов, маршрутизаторов и другого оборудования с доступом к сети.

Докладніше

***

22.01.2019

Соцсети – угроза приватности не только подписчиков, но и их друзей

Каждый раз, когда вы создаёте учётную запись в Facebook или в другой соцсети, вы предоставляете ей информацию не только о себе, но и о своих друзьях, утверждает математик Вермонтского университета Джеймс Бэгроу (James Bagrow). Он руководил совместным с Аделаидским университетом исследованием, итогам которого посвящена статья в выпуске журнала Nature Human Behavior (Компьютерное Обозрение).

Эта работа поднимает серьёзные вопросы приватности и показывает, что, по крайней мере в теории, человека можно с высокой точностью характеризовать – вплоть до политических и религиозных взглядов и кулинарных предпочтений – анализируя профили и действия его друзей. При этом человек может вообще никогда не пользоваться соцсетью или удалить свой эккаунт.

Авторы статьи собрали более тридцати миллионов публичных твитов от 13905 пользователей. Переработав эти данные, они показали, что сведений из сообщений от 8 или 9 контактов человека достаточно, чтобы предугадывать его следующие твиты, не глядя в его личную ленту.

Кроме того, онлайновые посты друзей обеспечивают примерно 95 % точность прогнозирования будущей деятельности человека, уже удалившего свою учётную запись или никогда её не имевшего.

«В соцсети нет укромного места, чтобы спрятаться», – утверждает соавтор статьи, Льюис Митчелл (Lewis Mitchell). Но скрыться нельзя и за её пределами. Решая, быть или не быть в Facebook, мы на самом деле ничего не меняем для своей онлайновой приватности – её контролируют люди вокруг нас.

***

22.01.2019

Троянец скрывается в программе для отслеживания курса криптовалют

Троянцы типа Downloader используются для загрузки других вредоносных программ. Trojan.DownLoad4.11892, обнаруженный недавно специалистами компании «Доктор Веб», – не исключение. При запуске он скачивает другого троянца с целью кражи персональных данных владельцев криптовалют (Компьютерное Обозрение).

Осенью 2018 г. в онлайн-сообществах, посвященных криптовалютам, появились сообщения с предложением установить программу для отслеживания изменения курса цифровых валют. Ее разработчики обещают бесплатный, надежный и сертифицированный виджет. На первый взгляд, приложение не вызывает подозрений: у него есть действительная цифровая подпись и оно показывает актуальную информацию о курсе криптовалют. Но за работоспособностью скрывается вредоносная функциональность.

При установке программа скачивает, компилирует и исполняет исходный код, загруженный с личного аккаунта разработчика на Github. После чего он загружает Trojan.PWS.Stealer.24943, известного также как AZORult. Этот троянец используется для кражи личных данных, включая пароли от кошельков криптовалют.

Преимущественно мошенники предлагают скачать вредоносную программу на русском, английском и польском языках. В русскоязычном сегменте Интернета троянца распространяют в группах майнеров криптовалют на vk.com. Также он все еще доступен на различных файлообменных сервисах и на Github.

***

24.01.2019

Больше половины пользователей Windows оказались под угрозой

Более половины программ, установленных на компьютерах на базе Windows, подвергают опасности пользователей из-за уязвимостей. Причина в устаревших версиях, выяснила компания антивирусной программы Avast на основе анализа 163 миллионов устройств (InternetUA).

Исследователи рассказали, что более 94 процентов юзеров пользуются устаревшей версией Skype, 85 процентов используют старую версию Mozilla Firefox, 77 процентов не обновили iTunes.

Специалисты компании предостерегли пользователей, заявив, что злоумышленники с помощью устаревших версий софта могут «скомпрометировать компьютер».

Отдельно производители антивируса отметили, что на старые версии Microsoft Office не выходит обновлений, что также может отрицательно повлиять на безопасность компьютера при возможной хакерской атаке. Специалисты посоветовали пользователям обновлять софт вовремя, чтобы избежать неприятных последствий.

***

27.01.2019

Кіберполіція: Росія планує кібератаки під час виборів в Україні

Хакери, які скоріш за все, співпрацюють з Росією, нарощують зусилля для зриву виборів Президента України за допомогою кібератак на сервери ЦВК та персональні комп'ютери працівників ЦВК. Про це заявив глава кіберполіції України Сергій Демидюк в інтерв'ю Reuters, передає УНН (InternetUA).

За словами Демидюка, кібер-зловмисники використовували заражені вірусом вітальні листівки, запрошення магазинів, пропозиції оновлення програмного забезпечення та інші шкідливі «фішингові» матеріали, призначені для крадіжки паролів і особистої інформації.

За десять тижнів до виборів хакери також почали купувати особисті дані співробітників ЦВК, сказав Демедюк, розплачуючись при цьому криптовалютою через Darknet, частини Інтернету, доступну тільки через певне програмне забезпечення і яка зазвичай використовується анонімно.

«Є постійні атаки – вони переходять від простих (програмних додатків) до додатків, які використовує той чи інший співробітник», – сказав він, пояснюючи, що ці атаки нагадують кібератаки на енергетичну, транспортну і банківську системи країни, які спостерігаються з 2014 року.

«Оплата відбувається в криптовалюті в більшості випадків ... і з тих же гаманців, які використовувалися для фінансування попередніх атак. Це говорить про те, що цим займаються ті ж хакерські організації, які знаходяться під контролем російських спецслужб», – сказав Демедюк.

На питання про зауваження Демедюка представник Кремля Дмитро Пєсков сказав, що «російські державні структури ніколи не втручалися і не втручаються у внутрішні справи інших країн».

***

28.01.2019

Владимир Кондрашов

Эксперт: база клиентов крупного сервиса онлайн-кредитов «ушла» к хакерам

База клиентов небанковского сервиса кредитования Moneyveo.UA по состоянию на 2017 год обнаружена в сети Интернет на «профильных» форумах так называемого «даркнета».

Докладніше

***

28.01.2019

Пользователи Instagram массово жалуются на невозможность восстановить аккаунт после взлома

Пользователи Instagram массово жалуются на проблемы с безопасностью на платформе – тысячи юзеров не могут восстановить свои аккаунты после того, как они были взломаны злоумышленниками.

Докладніше

***

29.01.2019

Facebook зарабатывала на детях, совершающих внутриигровые покупки без ведома родителей

Facebook зарабатывала тысячи долларов на пользователях соцсети – вернее, на их детях, которые без ведома родителей тратили деньги на покупки внутри игр и приложений, пишет Quartz со ссылкой на Reveal (InternetUA).

Издание основывается на обнародованных материалах группового иска против Facebook, согласно которым она использовала практику под названием «friendly fraud» (мошенничество первого лица, или «дружественное мошенничество») и даже призывала не препятствовать ей. Детей, совершающих крупные траты, называли «китами» – как в сленге игроков казино.

Как отмечается, иногда дети не знали, что растрачиваемые деньги «утекают» с карточек, привязанных к аккаунтам их родителей, или же что они тратят настоящие деньги. Родители же не имели понятия, что дети вообще могут получить доступ к карточкам без какой-либо авторизации. Судя по документам, Facebook об этом было известно, а её сотрудники предлагали способы остановить бесконтрольные расходы детей, однако компания не реализовала их.

Нажав иконку в углу экрана в Ninja Saga, ребёнок мог моментально приобрести магические способности за $20. За трёхмесячный период в 2010–2011 годах дети потратили на игры в соцсети $3,6 млн. По исследованию Facebook, средний возраст игрока, например, Angry Birds – всего 5 лет, хотя аккаунты в соцсети можно создавать с 13-ти. 93 процента возвратов средств в этой игре приходились на покупки «по незнанию».

Родители обращались в кредитные компании с просьбой помочь получить деньги назад, что соцсеть делала совсем неохотно. Процент возврата средств у Facebook вырос до 9 – обычно подозрения регуляторов вызывает уже 1 процент возвратов, а в среднем по компаниям он составляет 0,5 процента.

***

29.01.2019

Ольга Карпенко

Киберполиция закрыла украинский даркнет-ресурс xDedic. Он торговал взломанными серверами

xDedic – интернет-магазин, где продавали доступ к взломанным серверам. Его создали трое украинцев, они же и поддерживали работу известного в даркнете ресурса. Группа успела продать более 70000 паролей и логинов удаленного доступа к серверам из 170 стран мира (AIN.UA).

24 января 2019 года международная группа правоохранителей, куда входила и Киберполиция, провела обыски в девяти локациях Украины, изъяла компьютерное оборудование и задержала подозреваемых в управлении ресурсом. Деятельность магазина прекратили.

На чем зарабатывали

Хакеры взламывали доступ через протокол удаленного рабочего стола (RDP). Покупатели и продавцы торговали в этом магазине такими RDP-серверами, цена каждого взломанного сервера составляла от $6000 до $10000.

Большая операция

Над делом работали специалисты Генпрокуратуры, Нацполиции, Федерального подразделения по борьбе с компьютерной преступностью Бельгии, Федерального бюро расследований США, Службы внутренних доходов США в г. Тампа и другие. Американскую часть расследования проводила Прокуратура США Среднего округа штата Флорида.

Федеральная прокуратура Бельгии начала расследование о xDedic в июне 2016 года. Правоохранителям удалось установить, как выглядит инфраструктура xDedic, и получить цифровые копии ее самых важных серверов. Анализ этих серверов позволил идентифицировать администраторов из Украины. В ходе этого расследования бельгийские и украинские правоохранительные органы работали сообща. Позже над делом начали совместно работать бельгийские и американские следователи.

***

29.01.2019

Создатель интернета назвал главную опасность для всемирной сети

Американский ученый и разработчик Винтон Серф (Vinton Cerf) назвал незащищенные устройства интернета вещей главной опасностью для современной сети. Его слова приводит Business Insider (InternetUA).

Один из создателей сети обеспокоен тем, что число устройств, подключающихся к интернету, постоянно растет. Он уточнил, что проблема заключается в недостаточной безопасности таких гаджетов.

«Появляется лавина устройств, и они будут потенциально опасны», – заявил Серф, являющийся сейчас главным интернет-евангелистом Google. Ученый уточнил, что последствия сбоя в работе этих устройств могут быть непредсказуемыми.

В качестве опасного примера Серф привел взломанный автомобиль без водителя, который может попасть в аварию.

Разработчик заключил, что интернет имеет два врожденных недостатка: он не приспособлен для подключения миллиардов устройств, которые в конечном счете все-таки будут встроены в эту сеть, и отсутствие у него встроенных протоколов безопасности.

Из прогнозов исследовательской компании Gartner следует, что к 2021 году пользователи подключат к сети около 25 миллиардов устройств интернета вещей.

В октябре прошлого года сообщалось, что исследователь в области кибербезопасности обнаружил новый опасный вирус, похожий на известный ботнет Mirai. Агрессивное ПО активно захватывало устройства интернета вещей и подчиняло их хакерам.

***

29.01.2019

Google обеспечит европейским партиям киберзащиту перед выборами в Европарламент

Подразделение Google Jigsaw, занимающееся разработкой решений в области кибербезопасности, предложило европейским политическим партиям и организациям в преддверии выборов в Европарламент защитить их сети от DDoS-атак с помощью сервиса Project Shield. Об этом сообщила сегодня, 29 января, британская The Daily Telegraph (InternetUA).

Сервис был разработан Jigsaw в 2016 году, но до сих пор компания предоставляла его только американским информационным изданиям, журналистам, правозащитным организациям и группам наблюдателей на выборах. Именно по их сайтам чаще всего наносят удары хакеры в период подготовки к выборам, выводя их из строя с помощью DDoS-атак. Комментируя свое предложение в интервью порталу TechCrunch, глава пресс-службы Jigsaw Дэн Кизерлинг подчеркнул, что свои услуги всем политическим организациям Европы их компания предлагает бесплатно, в отличие от других провайдеров аналогичных сервисов.

***

29.01.2019

Один из департаментов Запорожской ОГА заявил о кибератаке – уничтожены важные документы

На Департамент капитального строительства Запорожской ОГА совершена кибератака, в результате которой были уничтожены файлы и информация, распорядителем которой являлся департамент (InternetUA).

Об этом чиновники сообщили ОО «Запорожский центр расследований» в ответ на запрос о предоставлении информации об освоении средств в 2018 году.

«25 января на Департамент была совершена кибератака, в результате чего была уничтожена значительная часть файлов и информации, роспорядителем которой является Департамент, что значительно затрудняет дальнейшую работу», – говорится в информации предоставленной директором департамента Сергеем Белевцовым.

***

29.01.2019

Новый троян крадет пароли под видом приложения Google Update

Специалисты компании Minerva Labs заметили вариант трояна AZORult, который маскируется под приложение Google Update и заменяет официальную программу вредоносной версией (InternetUA).

AZORult представляет собой инфостилер, который также может действовать как загрузчик для другого вредоносного ПО. Троян предназначен для кражи как можно большего объема конфиденциальной информации: от файлов, паролей, cookie-файлов и истории посещения в браузере до банковских учетных данных и криптовалютных кошельков пользователей.

Исследователи получили от одного из своих клиентов на первый взгляд легитимный исполняемый файл GoogleUpdate.exe, подписанный действительной цифровой подписью. Как оказалось при ближайшем рассмотрении, на самом деле файл был подписан сертификатом, выданным компании Singh Agile Content Design Limited вместо Google. Сертификат был выдан 19 ноября минувшего года и на протяжении прошедшего периода использовался для подписи более чем сотни исполняемых файлов, причем все они были замаскированы под Google Update.

В ходе анализа специалисты смогли идентифицировать вредонос в фальшивом файле Google Update как троян AZORult на основе нескольких признаков: отправка запроса HTTP POST к /index.php с домена в альтернативной зоне .bit и использование Mozilla/4.0 User-Agent.

Помимо основного функционала, новый вариант AZORult обладает дополнительной возможностью маскироваться под программу Google Updater (C:\Program Files\Google\Update\GoogleUpdate.exe). Таким образом вредонос может работать с привилегиями администратора и сохранять присутствие на

системе без необходимости модификации реестра Windows или добавления задач в планировщик.

***

30.01.2019

У Запоріжжі хакер із міжнародної банди викрадав дані іноземців для пограбування електронних рахунків

Служба безпеки Укриїни викрила у Запоріжжі хакера, який розповсюджував шкідливе програмне забезпечення (Espreso.tv).

Про це повідомила прес-служба СБУ у Facebook.

Чоловік розробляв та використовував хакерські програми для того, щоб зламати електронні платіжні системи, криптовалютні розрахунки та системи дистанційного обслуговування клієнтів банківських установ, переважно іноземного походження.

Він отримував дані користувачів та паролі завдяки використанню вірусу.

Через зараження вірусом гаджетів зловмисник хотів отримати несанкціонований доступ до електронних рахунків користувачів для привласнення коштів.

СБУ провела обшук у помешканні та виявила комп'ютерну техніку з встановленим шкідливим програмним забезпеченням, електронні накопичувачі інформації з даними понад тисячі користувачів, серед яких переважна більшість громадяни інших держав.

Спецслужби заблокували доступ до трьох віддалених серверів, за допомогою яких розповсюджувалось шкідливого програмного забезпечення.

Як повідомляє СБУ, чоловік є представником закритого міжнародного форуму хакерського направлення. Він просував свої розробки та обмінювався «досвідом» з учасниками міжнародного хакерського угруповання.

Правоохоронці відкрили кримінальне провадження, вилучили комп'ютерне обладнання та направили його на експертне дослідження.

***

30.01.2019

Facebook покупает данные за $20

Надежда Якимаха

Приложение Facebook Research имеет полный доступ к данным пользователей. За такую роскошь компания платит $20/мес каждому «подопытному» юзеру 13–35 лет.

Докладніше

ДОДАТКИ

Додаток 1

27.01.2019
Половина активных пользователей Facebook – боты

Аарон Гринспен называет себя создателем одного из прототипов самой большой соцсети мира – которым позже и воспользовался Марк Цукерберг. В 70-страничном отчете он утверждает, что сейчас Facebook – не лидер IT-отрасли, а колосс на глиняных ногах. И соцсеть ожидает судьба MySpace и AOL (InternetUA).

Гринспен называет себя автором идеи Facebook и даже пробовал судиться с Марком Цукербергом, но не преуспел. В преамбуле к своему отчету он признает, что воспринимает бизнес-империю Facebook предвзято. Но шокирующие выводы, тем не менее, могут оказаться правдой, предупреждает он. Потому с отчетом стоит ознакомиться всем.

Главная цифра, которую Гринспен подвергает сомнению – число активных пользователей Facebook, которые заходят в сеть ежемесячно – MAU. По собственной оценке соцсети, таких более 2 млрд человек.

Исследователь пишет, что даже после череды скандалов, сопровождавших FB на протяжении всего 2018 года, инвесторы плохо представляют ситуацию. Около половины активных аккаунтов – то есть миллиард – могут быть хитроумными ботами.

Гринспен утверждает, что в последнее время Facebook и сама начала путаться в различных метриках. Некоторые цифры противоречат друг другу, иные – попросту не логичны. По его версии, именно поэтому Марк Цукерберг значительно сократил перечень публикуемых данных в квартальных отчетах.

«Компания потеряла контроль над своим продуктом», – делает вывод он.

По мнению команды Plainsite, руководство Facebook не заинтересовано в очищении сети от ботов, так как они генерируют значительную часть ее доходов.

Для ботов это часть маскировки, а для Facebook – прибылей. Алгоритмы, чтобы сойти за живых пользователей, лайкают случайные страницы компаний, а также кликают на рекламные объявления. С учетом доли ботов, реклама на Facebook – это «деньги на ветер», подчеркивает Гринспен.

При этом часть ботов связана с правительствами ряда стран – разумеется, в отчете упоминается и Россия – и они разносят по сети ложные новости, дезинформацию, пропаганду, распространяют мошеннические ссылки.

Гринспен напоминает, что с 2012 года Цукерберг многократно подчеркивал, насколько для него важен поступательный рост соцсети. С учетом колоссального охвата сохранять прежние темы все сложнее. И сейчас менеджмент все больше озабочен тем, чтобы находить «мертвые души» вместо того, чтобы ориентироваться на потребности реальных пользователей.

Авторы отчета предупреждают: вероятность того, что Facebook выкинут на обочину ИТ-индустрии, как это произошло с AOL, CompuServe или MySpace, все больше. Если, конечно, компанию не разорят судебные иски.

После публикации отчета акции Facebook за считанные минуты рухнули на 2,4 %, однако затем стали потихоньку отыгрывать падение.

По времени публикация отчета на Plainsite совпала с колонкой «Факты о Facebook», которую от имени Марка Цукерберга опубликовали на сайте Wall Street Journal.

В ней основатель и глава соцсети защищает рекламную модель. Он объясняет, что таргетинг – давняя рекламная стратегия, просто интернет и соцсети позволяют делать это намного точнее, чем это было в эпохи телевидения или на уличных растяжках.

Марк жестко разделяет таргетинг рекламы и торговлю данными пользователей. Последним Facebook не занимается. Руководитель соцсети утверждает, что это было бы невыгодно: если бы конкуренты и вправду могли купить данные пользователей, FB потеряла бы свое конкурентное преимущество.

Теми же стратегическими соображениями он объясняет борьбу с кликбейтом и другими практиками «накачки» трафика. «Нет, [мы такого не делаем]», – отрезает он. Руководитель FB утверждает, что такой контент остается онлайн лишь потому, что ИИ-алгоритмы и люди-модераторы пока работают неидеально.

Цукерберг надеется, что благодаря подробным объяснениям бизнес-модель Facebook станет понятной для пользователей, и та часть, которая «склонна не доверять непонятному», изменит свою точку зрения.

На следующей неделе Facebook предстоит опубликовать очередной квартальный отчет. Он покажет, насколько ожидания Цукерберга обоснованны.

(вгору)

Додаток 2

22.01.2019

State of Social: на каких форматах сфокусируются маркетологи в 2019 году

Buffer выпустила результаты ежегодного исследования, опросив 1,842 специалистов по маркетингу. Так исследование обнаружило, что многие бренды используют формат Stories: 57 % считают этот формат «в какой-то степени эффективным» или «очень эффективным» в рамках своей стратегии. Хотя 62 % респондентов отметили, что еще не инвестировали в рекламу в Stories, 61 % планирует это сделать в 2019 году (Marketing Media Review).

Мессенджеры все еще недооценены. Несмотря на популярность таких платформ, как WhatsApp и Messenger, почти 71 % брендов не используют мессенджеры для маркетинга. 50 % маркетологов не планируют использовать мессенджеры в 2019 году.

Те, кто используют мессенджеры, отмечают, что процент открытий превышает 98 %, а кликабельности – 25 %.

Инфлюенсер-маркетинг – это эффективная стратегия для брендов, но здесь нужна ясность. 37 % респондентов отметили, что их компании инвестируют в маркетинг влияния. Среди них 68 % назвали этот маркетинг эффектным. 23 % брендов не уверены во влиянии influencer-маркетинга на их бренд. 88 % из тех, кто пользуется маркетингом влияния планируют продолжать использовать эту стратегию в 2019 году. Данные также показали, что большинство компаний приведены в замешательство правилами вокруг influencer-маркетинга, и только 6 % назвали эти руководства «ясными». Для 44,8 % они «неясны», а для 15,8 они «очень неясны».

Все больше брендов используют видеоконтент. Только 14,5 % компаний не публикуют видеоконтента, что меньше по сравнению с 25 % в 2018 году. 36 % размещают видеоконтент ежемесячно, а 24 % – еженедельно.

Facebook остается самым популярным каналом для брендов, которые делятся видеоконтентом (81 %), YouTube занимает второе место (62 %), а Instagram – третье (57 %). LinkedIn – на пятом месте (32 %). Однако за этой платформой следует следить в 2019 году, так как данные показывают, что видео в этой сети в 20 раз получают больше шеринга, чем другой контент.

У большинства брендов нет планов по использованию IGTV. Только 12,2 % респондентов использовали новый формат в 2018 году, а 72 % отметили, что не намерены создавать контент для IGTV в 2019 году.

Социальные медиа являются ключевой частью маркетинговых стратегий, однако почти 20 % не уверены, как измерять эффектность активностей в сетях.

Среди трудностей по созданию больше видеоконтента для сетей многие назвали отсутствие времени.

(вгору)

Додаток 3

24.01.2019

Покупатели скептически относятся к дополненной реальности, ботам и соцсетям

Согласно новому исследованию, проведенному Oracle NetSuite в партнерстве с Wakefield Research и The Retail Doctor, пользователи не хотят разговаривать с роботами при совершении покупок в магазине или через Интернет. Глобальное исследование 1200 потребителей и 400 руководителей предприятий розничной торговли в США, Великобритании и Австралии выявило огромную разницу между потребностями покупателей и тем, что розничные сети предлагают им в магазинах и онлайн, включая использование передовых технологий, таких как чат-боты, искусственный интеллект и виртуальная реальность (Компьютерное Обозрение).

Несмотря на значительные инвестиции в повышение качества обслуживания клиентов в Интернете и в магазинах, розничные магазины не

могут идти в ногу с быстро меняющимися ожиданиями покупателей. 73 % руководителей сетей розничной торговли считают, что за последние 5 лет общая обстановка в магазинах стала более привлекательной. Только 45 % потребителей согласны с ними, а 19 % заявили, что обстановка стала менее комфортной.

79 % руководителей считают, что чат-боты удовлетворяют потребности потребителей, но две трети клиентов (66 %) не согласны с ними и отмечают, что чат-боты в настоящее время больше вредят покупкам, чем помогают. Почти все (98 %) руководители считают, что взаимодействие с клиентами в социальных сетях важно для установления более прочных отношений с ними. Только 12 % потребителей считают, что это оказывает существенное влияние на то, как они относятся к бренду.

Несмотря на то, что почти половина потребителей (42 %) и почти две трети миллениалов (63 %) отмечают, что они готовы платить больше за улучшенную персонализацию, только 11 % руководителей полностью уверены, что их сотрудники имеют инструменты и информацию, необходимые для предоставления клиентам персонализированного опыта.

80 % потребителей считают, что им не предоставляется индивидуальный опыт покупок как в магазинах, так и в Интернете. Более половины (58 %) не удовлетворены тем, как магазины используют технологии для улучшения персонализации, и почти половина (45 %) сообщила о негативных эмоциях при получении персонализированных предложений в Интернете.

Исследование показало, что раскрученные технологии, такие как ИИ и VR, пока не являются панацеей от этих проблем. Почти все (90 %) руководители предприятий розничной торговли не уверены, что использование передовых технологий отвечает потребностям клиентов. 79 % считают, что использование ИИ и VR в магазинах увеличит продажи, но только 14 % покупателей отметили, что новые технологии окажут значительное влияние на их решения о покупке. Почти все (98 %) руководители думают, что ИИ и VR увеличат посещаемость их магазинов. С ними не согласны 48 % опрошенных покупаталей.

Несмотря на популярность онлайн-покупок, физические магазины никуда не денутся в ближайшее время. До тех пор, пока розничные продавцы обеспечивают простой покупательский опыт, люди будут продолжать делать покупки в магазинах. Почти все (97 %) потребители согласны с необходимостью идти в физический магазин для покупки товаров, и большинство (70 %) считают, что лучшие розничные магазины имеют функции, которые упрощают процесс совершения покупок.

Основными достижениями в области технологий, которые потребители хотят использовать при совершении покупок в магазине или через Интернет, являются киоски самообслуживания (38 %), примерка в виртуальной реальности (23 %) и мобильные платежи (15 %). Только 5 % выбрали общение с роботами и чат-ботами в качестве технологий, которые они больше всего хотят использовать.

(вгору)

Додаток 4

20.01.2019

Британские ученые выяснили, что гаджеты влияют на психическое состояние подростков не больше, чем картофель

Психологи из Оксфордского университета, воспользовавшись большим (более 355 тысяч участников) датасетом с информацией о жизни и здоровье подростков, родившихся в начале 2000-х годов в США и Великобритании, изучили, как использование гаджетов связано с психическим состоянием молодежи (InternetUA).

Важно отметить, что в качестве показателя психического здоровья были использованы данные о психическом самочувствии подростков (включая ответы на вопросы вроде «Считаете ли вы свою жизнь бессмысленной?»), попытках суицида и уровне одиночества, а в качестве статистического метода – анализ кривой спецификаций. Данный метод является разновидностью регрессионной модели и позволяет проверить на количественных данных все возможные валидные гипотезы, а не только те, которые поставлены исследователем. Другими словами, вместо того, чтобы определить зависимость лишь между использованием гаджетов и психическим состоянием, исследователи смогли проверить зависимость психического состояния от всех факторов, для которых было доступно достаточно информации.

В результате ученые действительно обнаружили статистически значимую негативную корреляцию между использованием гаджетов и неудовлетворительным психическим состоянием. Однако она была очень мала. Авторы подсчитали, что этот фактор может объяснить только около 0,4 % различий в психическом состоянии подростков: примерно такое же влияние на этот показатель у потребления молока и картофеля, а также ношения очков. Переменными, которые действительно негативно ассоциируются с психическим самочувствием подростков, оказались курение сигарет и марихуаны, драки и буллинг, а среди позитивных факторов ученые отметили достаточное количество сна, регулярный завтрак и потребление овощей и фруктов.

По итогам исследования авторы работы указывают на то, что использование гаджетов может быть не таким опасным, как временами утверждается. Вместе с тем, они подчеркивают, что их анализ выявил только корреляцию, и из полученных данных нельзя с уверенностью выделить информацию о каких-либо причинно-следственных связях: для этого, как минимум, необходимо проводить долгосрочные исследования.

(вгору)

Додаток 5

28.01.2019

Почему нельзя публиковать детские фото в Интернете

Многие считают, что соцсети – это своего рода семейный альбом, который можно показывать всем. Увы, последствия могут быть ужасающими (InternetUA).

«У моего сына нет друзей – что делать?», «Врачи советуют риталин – давать или инет?», «Порекомендуйте детского психолога в округе Ха-Шарон», «Моя красавица дочь со своим первым парнем» – это только часть тех публикаций, которые родители размещают в соцсетях. Наивность родителей и их желание поделиться со всем миром новостями из жизни своих детей на самом деле таят большую опасность. Когда дети вырастут, эти фотографии и посты могут сыграть в их жизни ужасную роль.

«Сегодня про любого кандидата на рабочее место можно узнать все, заглянув в соцсети. Работодатели больше не доверяют ни резюме, ни рекомендациям – они ищут имя прендендента в фейсбуке и инстаграме. То же самое происходит, когда мы ищем спутника жизни. Поэтому я хочу прокричать всем родителям: остановитесь! – говорит Това Бен-Ари, государственный инспектор министерства образования по исполнению закона о правах ученика. – Я считаю, родители перешли все границы конфиденциальности. Хотелось бы, чтобы они вообще не писали ничего о своих детях в соцсетях, а если да – то хотя бы посоветовавшись с ними насчет содержания. Надо понимать, что любой пост остается в сети долгие годы и потом может навредить ребенку».

Закрытые группы

«Когда родителям нужен совет или помощь, то вместо школьного консультанта они обращаются в соцсети, – сетует Нирит Цук, основатель и гендиректор родительского портала “Эсер плюс” и специалист по исследованию молодежной культуры. – Но люди ведь не рассказывают всем соседям о личных проблемах, не показывают незнакомцу в автобусе фотографии своего ребенка, так почему они считают нормальным выкладывать всю свою жизнь в сеть?» – задается вопросом Нирит.

Она говорит, что очень важно заботиться о неприкосновенности частной жизни своих детей и семьи, даже если речь идет о закрытых группах в фейсбуке. Ведь каждый участник группы может скопировать фото и разослать его потом куда угодно.

«Люди должны понимать, что содержание поста, включая фотографии, останется в сети навеки и будет доступно всем, кто ищет о вас информацию. Узнать место вашего проживания и ваши предпочтения тоже не составит большого труда».

По словам Нирит, каждый пользователь соцсети желает похвастать своей прекрасной жизнью, особыми ужинами, развлечениями или достижениями ребенка, гордясь им и не особо задумываясь о его праве на частную жизнь. Например, мать размещает в сети фотографии танцующей дочки и не думает, что этим ставит дочь в неловкое положение.

Другая тенденция – делиться своими чувствами и переживаниями. Мать, публикующая пост об одиночестве сына, возможно, беспокоится о благополучии ребенка, но совсем не думает о его чувствах в тот момент, когда он узнает о существовании этого поста.

«Кажется, люди забывают, что сеть – это не круг знакомых в чьей-то гостиной, а огромный резервуар, в котором информация хранится долгие годы. Посты о проблемах детей, их фотографии могут навредить ребенку – и вы даже не представляете, при каких обстоятельствах. Поэтому, – советует Нирит, – перед тем как нажать кнопку “Опубликовать”, родителям стоит задуматься и задать себе такие вопросы: Почему мне так важно разместить это фото в сети? Может ли оно как-то навредить моему ребенку в будущем? Хотел бы он сам выставить это фото на всеобщее обозрение?»

Родителям подростков еще до публикации следует спросить у ребенка разрешение опубликовать его фото – ведь даже будучи вашим ребенком, он имеет право на конфиденциальность согласно международному закону о правах ученика.

В Европейском союзе уже подняли вопрос об изменении понятия «частная жизнь» и пытаются защитить детей в сети. Дошло до того, что в некоторых европейских странах совершеннолетние могут через суд стереть из Сети информацию о себе или свои фотографии, опубликованные кем-то или их родителями.

Понятие частной жизни в наше время

Еще в 2010 году Марк Цукерберг заявил, что в Сети нет частной жизни, здесь все публично и доступно каждому. А как иначе? Каждый участник соцсетей сам выдает о себе информацию: имя, фамилию, дату рождения, фотографии и даже номер кредитки. В сети не счесть откровенных блогов и постов о личной жизни.

Однако специалисты возражают Цукербергу: конфиденциальность в сети есть, просто она видоизменилась по вине технологий.

По всему миру растет тенденция, запрещающая родителям публиковать в сети фотографии своих детей голышом, в купальниках или даже во время отучения от подгузника. Не секрет, как легко попадают такие фото в руки педофилов и сексуальных маньяков.

(вгору)

Додаток 6

22.01.2019

Система манипуляций Google и Facebook выходит из-под контроля

Гиганты ИТ-индустрии превращают действия человека в товар. Они незаметно контролируют каждый шаг пользователя и управляют его поведением. Система сбора информации и последующих манипуляций – это новый капитализм. И контролировать его развитие все труднее (InternetUA).

О феномене новых бизнес-моделей, построенных на основе слежки, рассказывает исследовательница Гарвардской школы бизнеса Шошанна Зубофф. В своей книге «Век надзор-капитализма» она описывает принципы, по которым работают современные ИТ-гиганты.

Как объясняет эксперт, люди изначально понимали условия сделки, на которую шли. Мы делимся с компаниями данными, а они бесплатно предоставляют нам услуги. Однако со временем ситуация изменилась. Компании стали считать бесплатными не только данные, но и самих людей, которые их генерируют. Наступила эпоха тотального мониторинга и контроля над поведением пользователя. «Человек стал источником сырого материала», – пишет Зубофф.

«Раньше мы искали в Google, а теперь Google ищет в нас. Раньше мы считали цифровые сервисы бесплатными, а теперь нас считают бесплатными», – цитирует исследовательницу Guardian.

Корпорации обогащаются за счет человека – они исследуют его, рассматривают под лупой, а затем тренируют алгоритмы на основе этих данных. В результате Google и Facebook создают инструменты для манипуляции и спекуляции под видом систем прогнозирования. Главным объектом торговли в условиях надзор-капитализма становится личный опыт человека, которым, как оказалось, можно оперировать на рынке.

Кто у руля

При этом большинство пользователей не представляет, насколько глубоко ИТ-гиганты исследуют их предпочтения и интересы. Каждый поисковый запрос, лайк, пост, геолокация, фото, видео и даже знак препинания «скармливается» алгоритмам на базе машинного обучения. Неудивительно, что даже невинный челлендж «Я 10 лет назад», который стал распространяться на Facebook и в Instagram, приняли за продуманный ход, запущенный социальными сетями для тренировки ИИ.

По мнению Зубофф, механизмы прогнозирования поведения пользователя – это не очередной виток развития бизнес-модели, а новый этап капиталистического уклада, который в конечном итоге подрывает демократию.

Общество в этих условиях делится на надзирателей и поднадзорных.

Подобная «асимметрия знаний» приводит к «асимметрии власти». И у людей не остается никаких рычагов контроля, поскольку надзор-капитализм никак не регулируется.

Ожидать, что корпорации займутся саморегулированием, не стоит. Сохранение существующей системы для них – залог выживания. «Требовать от надзор-капиталистов приватности – это то же самое, что просить Генри Форда вручную собирать каждый Ford T. Или как просить жирафа укоротить свою шею», – заключает Зубофф.

(вгору)

Додаток 7

30.01.2019

Еврокомиссия призвала Facebook и Twitter активизировать борьбу с дезинформацией

29 января Еврокомиссия сообщила, что получила первые отчеты от интернет-компаний, в том числе Google, Facebook и Twitter, о выполнении ими требований по борьбе с дезинформацией в сети, чиновники констатировали определенный прогресс в удалении фейковых аккаунтов, но ждут от компаний дополнительных мер (InternetUA).

В октябре 2018 года по предложению ЕК интернет-компании подписали кодекс практики борьбы с дезинформацией.

«Сегодня Google, Facebook, Twitter, Mozilla и ассоциации, представляющие рекламный сектор, представили свои первые доклады о мерах, которые они принимают для соблюдения кодекса практики против дезинформации. Хотя ЕК приветствует достигнутый прогресс, она также призывает стороны, подписавшие конвенцию, активизировать свои усилия в преддверии европейских выборов 2019 года», – говорится в сообщении ЕК.

Еврочиновники отмечают, что «был достигнут определенный прогресс, в частности, в удалении поддельных учетных записей и ограничении видимости сайтов, распространяющих дезинформацию».

«Однако необходимы дополнительные меры для обеспечения полной прозрачности политических объявлений к началу кампании по проведению выборов в ЕП во всех государствах-членах ЕС, для обеспечения надлежащего доступа к данным платформ в исследовательских целях и надлежащего сотрудничества между платформами и отдельными государствами-членами», – считают в ЕК.

По мнению вице-председателя ЕК по единому цифровому рынку Андруса Ансипа, компании теперь «должны убедиться, что эти инструменты доступны всем в ЕС, контролировать их эффективность и постоянно адаптироваться с учетом новых средств, используемых теми, кто распространяет дезинформацию».

Еврокомиссар по безопасности Джулиан Кинг заявил, что, «с учетом приближения европейских выборов, любой прогресс, достигнутый в борьбе с дезинформацией, приветствуется, но до мая нам нужно продвигаться дальше и быстрее».

Еврочиновники ожидают от компании Facebook «большей ясности относительно того, как социальная сеть будет использовать свои инструменты расширения прав и возможностей потребителей, а также активизировать сотрудничество с теми, кто проверяет факты, и исследовательским сообществом в ЕС». Компанию Google также призвали «поддерживать исследовательскую деятельность в большем масштабе».

«Twitter уделяет приоритетное внимание действиям против злоумышленников, закрывая поддельные или подозрительные учетные записи и автоматизированные боты. Тем не менее, необходима дополнительная

информация о том, как это ограничит постоянных поставщиков дезинформации от продвижения их твитов», – заявили в ЕК.

В январе 2019 года онлайн-платформы должны предоставить комиссии подробную информацию по проделанной работе. Этот первый ежемесячный отчет опубликуют в феврале, аналогичные отчеты будут предоставляться каждый месяц до мая, когда пройдут выборы в ЕП.

(вгору)

Додаток 8

21.01.2019
Ирина Фоменко
Индия хочет, чтобы соцсети удаляли «незаконный» контент

Правительство Индии предложило новые правила, направленные на прекращение распространения фейковых новостей и дезинформации в социальных сетях – и местные группы активистов гражданских свобод не довольны. Об этом сообщает The Verge (InternetUA).

В конце прошлого месяца Internet Freedom Foundation написали заявление, что новые правила будут оказывать «невыносимое давление на свободу слова в Интернете».

Если поправки примут, платформы, такие как Facebook и Twitter, будут обязаны подвергать цензуре контент, который правительство Индии считает неуместным – что, в свою очередь, повлияет на контент за пределами страны.

Кроме того, компании должны будут предъявлять пользовательские сообщения, если власти запрашивают информацию, а это негативно скажется на такие мессенджеры, как WhatsApp. Платформы также должны будут ежемесячно напоминать своим пользователям о политике конфиденциальности.

Платформы должны будут ввести новые инструменты для автоматической пометки контента, который правительство Индии признало незаконным. Согласно Wired, это будет включать «разжигание ненависти к определенным защищенным группам, клевету, жестокое обращение с детьми и изнасилования».

Эксперты опасаются, что новые требования могут подавить свободу слова и помочь обеспечить массовое наблюдение. Добавление пункта о расшифровке вызывает обеспокоенность у сторонников, так как правило может быть использовано для ознакомления с сообщениями граждан.

Согласно Bloomberg, прослеживаемость нарушит сквозное шифрование и потребует от платформ сохранять информацию в течение 180 дней на случай, если будет предложено расследование.

Генеральный директор Facebook Марк Цукерберг уже давно говорит, что его команда создает лучшие системы искусственного интеллекта для автоматической пометки контента, который нарушает правила платформы, еще до того, как он был опубликован. Тем не менее, незаконный контент каждый день попадает в новостные ленты пользователей.

(вгору)

Додаток 9

21.01.2019
Входить в Интернет в России придется по паспорту

С каждым днем в России власти страны обращают все большее внимание на Интернет, который еще 5-10 лет назад совсем никак не контролировался. Теперь его пытаются всеми доступными средствами сделать «регулируемым», а для этого вводятся новые законы и требования к интернет-провайдерам. Как стало известно 21 января, входить в Интернет на территории РФ придется по паспорту, а сообщил об этом министр культуры России Владимир Мединский, однако нужно сразу же заметить, что это его личное мнение (Украинский телекоммуникационный портал).

По мнению высокопоставленного чиновника, уже в скором будущем Россия и весь остальной мир придут к тому, чтобы позволять своим гражданам выходить в интернет только по паспорту, либо же при помощи других персональных идентификаторов, позволяющих быстро определить выполнение того или иного действия конкретным человеком, чтобы иметь возможность, при необходимости, привлечь его к ответу за совершенное правонарушение.

Министр уверен в том, что интернет в будущем по всему миру будет «жестко регулироваться», а случится это ради борьбы с нарушителями законодательства, которых с каждым днем в глобальной сети все больше и больше. В конце своего интервью чиновник заявил о том, что Министерство культуры не имеет права заниматься регулированием интернета в России или где-либо еще, поэтому все сказанное им – это лишь личное мнение, основанное на общей мировой ситуации. Очевидно, что министр культуры РФ считает блокировки веб-сайтов в интернете, которые распространяют запрещенную информацию, полностью неэффективными. Они не помогают полностью избавиться от проблемы, ведь люди, которые занимаются такими действиями, не несут никакой ответственности за свои деяния, что позволяем им совершать их снова и снова до тех пор, пока не надоест. Переход на принцип «интернет по паспорту» позволит штрафовать и, при необходимости, сажать в тюрьму людей, занимающихся противоправными действиями в интернет, например, распространением пиратских фильмов или же чем-то более плохим.

(вгору)

Додаток 10

22.01.2019
В мире все чаще практикуют отключение Интернета во время протестов

Вслед за массовыми протестами, которые начались в Зимбабве 14 января после резкого подорожания топлива, местные власти недавно полностью

блокировали доступ в интернет в стране. Крупнейший провайдер Зимбабве – компания Econet Wireless – сообщил об отключении своих услуг по приказу главы государства (InternetUA).

Заместитель министра информации Зимбабве Энерджи Мутоди (Energy Mutodi) сослался на необходимость данной меры для прекращения беспорядков, поскольку протестующие координировали свои действия онлайн.

Тем временем, в общественной организации NetBlocks, следящей за соблюдением прав в сфере цифровых технологий и регистрирующей ограничения доступа к интернет-сервисам, подсчитали, что трехдневное отключение от Глобальной сети могло обойтись и без того подорванной экономике Зимбабве в 17 миллионов долларов.

Движение за свободу интернета Keep It On в открытом обращении к министру информации Зимбабве Монике Муцвангве(Monica Mutsvangwa) написало:

«Отключение интернета препятствует свободному потоку информации и создает темную завесу, скрывающую нарушения прав человека от внимания общественности. Без цифровой связи журналисты и СМИ не могут контактировать с источниками, собирать информацию и передавать свои статьи. Технические средства, используемые для блокировки онлайн-доступа к информации, зачастую подрывают стабильность и отказоустойчивость интернета. Нельзя допустить, чтобы отключение интернета стало новым нормой».

Агентство CNN со ссылкой на данные правозащитной организации Access Now отмечает, что блокировка интернета во время протестов все чаще практикуется в мире, и с каждым годом число подобных случаев возрастает. В 2018-м задокументировано почти 190 отключений интернета против 108 в 2017 году и 75 в 2016-м.

Только за первые три недели 2019-го в пяти странах власти прибегали к частичному или полному отключению интернета – в Судане, Бангладеш, Конго, Габоне и Зимбабве, утверждают в Access Now.

В Судане в середине декабря вспыхнули массовые волнения в знак протеста против повышения цен на топливо и хлеб при дефиците всех основных потребительских товаров. Затем протестующие перешли к политическим лозунгам и потребовали отставки правительства и президента страны Омара аль-Башира. Чтобы остановить распространение выступлений, суданские власти распорядились ограничить доступ к основным соцсетям, в том числе Facebook и Twitter. По данным Access Now, блокировка длилась с 20 по 28 декабря, но и в январе сообщения о перебоях с интернетом и недоступности оппозиционных сайтов продолжали поступать.

Власти Бангладеш решили отключить мобильный интернет из-за парламентских выборов. За три дня до голосования, проходившего 30 декабря, Комиссия по регулированию электросвязи Бангладеш приказала операторам заблокировать Facebook и другие социальные платформы. Затем власти велели до конца выборов отключить скоростной мобильный интернет 3G и 4G,

мотивируя это необходимостью защиты избирательного процесса от саботажа и провокаций на политической почве. Кстати сказать, к таким мерам в стране прибегают не впервые. За несколько месяцев до этого правительство распорядилось замедлить скорость интернета во время студенческих выступлений. Также под предлогом борьбы с дезинформацией и фейковыми новостями применялась блокировка Skype и цензура крупных новостных сайтов.

В Конго интернет тоже был отключен из-за выборов. Вслед за голосованием 30 декабря, в ходе которого были отмечены различные нарушения, правительство велело заблокировать отправку SMS в стране и онлайн-доступ, заявив, что это было сделано во избежание злонамеренных действий, а не для противостояния публикации результатов выборов на избирательных участках. По данным Access Now, в январе ограничения все еще сохранялись.

7 января сбои с доступом в интернет зафиксированы и в Габоне во время попытки государственного переворота. Потери для экономики страны из-за 28-часового отсутствия связи оцениваются в 1 миллион долларов.

«Мы наблюдали резкий рост отключений интернета в 2018 году. И, судя по началу 2019 года, улучшения ситуации в обозримом будущем не предвидится», – заявила CNN активистка движения Keep It On Берхан Тай.

По информации правозащитников, чаще всего к блокировкам онлайн-сервисов и интернета в целом прибегают в Азии и Африке. Например, самое длительное отключение за последнее время произошло в Камеруне, где англоговорящие регионы страны провели 230 дней без доступа в Сеть с января 2017-го по март 2018 года.

Но тренд уже не ограничивается Азией и Африкой, а становится глобальным – за последние три года отключения интернета регистрировались в ряде стран Европы и Латинской Америки. Так, испанские власти прибегали к блокировкам во время протестов по поводу референдума о независимости 2017 года, а в России в 2018-м запретили Telegram, причем в тщетной погоне за мессенджером Роскомнадзор заблокировал миллионы IP-адресов крупнейших хостинг-провайдеров, что обернулось проблемами в работе других веб-ресурсов и сервисов.

По данным CNN, одно из первых массовых отключений интернета в политических целях произошло в Синьцзяне, регионе на северо-западе Китая. После того, как в июле 2009 года в региональной столице Урумчи вспыхнули беспорядки, доступ в интернет по всему Синьцзяну, наряду с услугами международной связи и отправки текстовых сообщений, были отключены на протяжении почти года.

Китайские власти оправдывали действия защитой безопасности, и теперь эту практику переняли другие. По данным Access Now, отключая интернет, в правительствах, как правило, называют три благие цели – обеспечение безопасности населения, недопущение распространения противозаконного контента и поддержание национальной безопасности.

Между тем, спецдокладчик ООН по вопросам свободы слова Дэвид Кайе (David Kaye) назвал всеобщее отключение доступа в Глобальную сеть «нарушением международного законодательства, которое ничем нельзя оправдать». Особенно во время выборов и других периодов повышенной напряженности «блокировки препятствуют не только доступу людей к информации, но и к базовым услугам», – подчеркнул Кайе, говоря о ситуации в Конго.

Одним из тех, кто пошел по стопам КНР, стал президент Уганды Йовери Мусевени (Yoweri Museveni). В 2016 году он назвал отключение интернета в стране «мерой безопасности для предотвращения распространения лжи, подстрекающей к насилию и оспаривающей законность результатов выборов».

Более того, власти Уганды решили улучшить опыт китайских коллег и летом 2018 года ввели налог на использование соцсетей и мессенджеров. Жители страны, желающие пользоваться Twitter, Facebook и WhatsApp, должны платить по 200 угандийских шиллингов в день или около 5 американских центов (чуть больше 3 российских рублей). Что интересно, перед этим местные чиновники побывали в Пекине для изучения опыта по контролю за социальными сетями.

Правозащитники финансируемой Вашингтоном организации Freedom House обеспокоены тем, что китайскую модель цензуры и слежки за онлайн-активностью жителей копируют другие государства, и что Пекин даже устраивает тренинги по вопросом интернет-политики и инструментам контроля для зарубежных делегаций.

Хотя активисты только догадываются о содержании подобных семинаров, они отмечают, что после того, как в апреле 2017 года такое обучение прошли вьетнамские чиновники, в 2018 году в стране был принят закон о кибербезопасности, копирующий аналогичное законодательство в КНР.

Также в докладе Freedom House сказано, что рост активности китайских компаний и должностных лиц в Африке предшествовал принятию ограничительных законов в области киберпреступлений и СМИ в Уганде и Танзании в течение прошлого года.

(вгору)

Додаток 11

22.01.2019

Роскомнадзор пошел в новую атаку на Telegram, заблокировав несколько тысяч прокси-серверов мессенджера

Заблокированный в России в апреле 2018 года мессенджер Telegram в последние месяцы был доступен большинству пользователей, многие из которых ранее настроили в приложении подключение через прокси-серверы для стабильной работы Telegram. Однако 21 января Роскомнадзор напомнил о себе и предпринял новую атаку на мессенджер (InternetUA).

21 и 22 января ведомство внесло в реестр запрещенных сайтов около трех тысяч новых IP-адресов. Об этом свидетельствует график пополнения реестра на сайте «Эшер II». Судя по жалобам пользователей на возникшие после этого пополнения реестра проблемы с Telegram, Роскомнадзор массово заблокировал адреса прокси-серверов, используемых для обхода блокировки мессенджера.

Источник «Ведомостей» в одном из операторов связи подтвердил, что Роскомнадзор активизировал блокировку Telegram. В свою очередь пресс-секретарь Роскомнадзора Вадим Ампелонский заявил, что служба не прекращала блокировку мессенджера.

Основатель и гендиректор компании Vee Security Александр Литреев подтвердил, что под новую волну блокировок попало большое число прокси-серверов. По его мнению, Роскомнадзор мог получить эти данные от операторов связи. Как подчеркнул Литреев, ничего нового в таком подходе к блокировкам нет, и пока действия Роскомнадзора не грозят полноценной блокировкой мессенджера в России.

В настоящее время под блокировкой из-за Telegram в России находится 3,7 млн IP-адресов, большая часть которых принадлежит облачному сервису компании Amazon. Побочным результатом блокировки стали сбои в работе сторонних сервисов и устройств «умного» дома, включая водонагреватели и лампочки.

(вгору)

Додаток 12

23.01.2019
Начнет ли Россия войну с Facebook и Twitter?

В Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре) снова вспомнили о Facebook и Twitter, напомнив им, что они нарушают российский закон о персональных данных (InternetUA).

Тот самый закон, согласно которому социальные сети обязаны хранить личные данные пользователей внутри России, и за несоблюдение, из-за которого в РФ была заблокирована соцсеть LinkedIn.

Так, что же, Россия окончательно решила выйти на тропу войны с Facebook и Twitter? И вообще, получится ли у Кремля заблокировать эти две соцсети? Давайте разберемся.

Прежде всего отмечу, что в нынешних условиях заблокировать доступ пользователей к чему бы то ни было – сайту, форуму, порталу, социальной сети – невозможно. Любой пользователь с достаточным желанием и базовыми навыками может обойти большую часть блокировок, затратив не так уж и много времени.

Вопрос в другом. Допустим, в России таки смогут провести тотальное блокирование этих социальных сетей, означает ли это, что работа соответствующей агентуры в них прекратится? Ведь, как известно, Facebook и

Twitter весьма активно используются для распространения вбросов, пропагандистских нарративов и т. д. Про то, как эти социальные сети использовались в ходе президентских выборов в США, вообще отдельная история.

Присутствие соответствующих специалистов и кибергрупп в них не уменьшится, уменьшится как раз присутствие простых пользователей, которые будут ограничены в доступе. С другой стороны, тех, которые будут иметь доступ в данные соцсетей в обход блокировки, т. е. в нарушение законодательства, будет легче отслеживать и наблюдать за их действиями.

А потому, цели блокировки Facebook и Twitter вполне ясны и довольно прозрачны, но, возвращаясь к озвученному выше, это реализовать Роскомнадзору вряд ли по силам. Facebook и Twitter это настолько глобальные и масштабные ресурсы, что даже не сама блокировка, а лишь попытка их заблокировать может обернуться серьезным ударом по репутации. Причем не репутации России как страны с некой условной «свободой», а как страны, обладающей техническими возможностями осуществлять подобные действия.

Например, как это было с блокировкой Telegram, когда в процессе блокирования социальной сети «ложились» сайты финансовых учреждений, сторонние ресурсы и даже выходили из строя кассовые аппараты в супермаркетах, хотя сама социальная сеть продолжала быть доступной.

Разумеется, в рамках глобальной замкнутой информационной системы РФ сделала многое: создала свои социальные сети, медиаплатформы, информационные площадки и даже открытые базы данных. Однако имея в наличии полное отражение мировых ресурсов, она до сих пор находится в зачаточном состоянии по реализации своей гипертрофированной мечты – объявления войны мировому интернету.

(вгору)

Додаток 13

29.01.2019

Facebook запустит два центра для борьбы с предвыборными фейками в Европе и Азии

Компания Facebook объявила о запуске двух центров, сотрудники которых займутся борьбой с распространением дезинформации в ходе предвыборных кампаний в странах Европы и Азии. Сообщение об этом было опубликовано в блоге социальной сети (InternetUA).

Как уточнили в Facebook, центры для оперативного реагирования на связанные с выборами фейки будут размещены в офисах компании в Дублине и Сингапуре.

«Это позволит нашим глобальным командам лучше работать в различных регионах в преддверии выборов и поспособствует укреплению координации и сокращению времени реагирования при взаимодействии сотрудников внутри страны и в Менло-Парке. Эти команды добавят новый уровень защиты от

фейковых новостей, оскорбительных высказываний и давления на избирателей», – говорится в сообщении.

Помимо этого, Facebook планирует использовать в странах, где будут проходить выборы, опробованную ранее в Нигерии практику запрета на размещение политической рекламы пользователями, которые находятся за пределами этой страны. Этот защитный механизм Facebook будет использовать в Украине и в ЕС для борьбы с иностранным влиянием на исход выборов.

Также соцсеть будет предоставлять пользователям дополнительную информацию о политических рекламных объявлениях и создаст архив таких объявлений за последние семь лет с возможностью поиска. Этот архив будет содержать как сами объявления, так и информацию о них, включая данные о расходах на их распространение и численности охваченной аудитории. В преддверии выборов такие архивы будут созданы в Индии, Израиле и в Украине, а до конца июня они станут доступны во всех странах.

Наконец, компания объявила о расширении программы, в рамках которой независимые организации занимаются проверкой достоверности материалов, ссылки на которые публикуют пользователи. В настоящее время программа действует на 16 языках, а теперь, помимо ссылок, эксперты смогут проверять также фотографии и видеозаписи.

«Всегда были люди, которые пытались подорвать демократию. Мы противостоим решительным противникам, которые пытаются действуют на многих фронтах, и мы признаем нашу ответственность. Мы никогда не остановим всех злодеев, но мы достигли реального прогресса и полны решимости продолжать совершенствоваться», – отмечается в сообщении.

(вгору)

Додаток 14

29.01.2019

Спецслужби РФ намагалися завербувати українського військового за допомогою месенджера WhatsApp

Співробітники Головного управління військової контррозвідки СБУ викрили спроби російських спецслужб вербування військових-секретоносіїв Збройних Сил України для отримання інформації в оборонній сфері (InternetUA).

Про це повідомили у прес-центрі СБУ, оприлюднивши відео з заявами українських бійців.

«Я військовослужбовець Збройних сил України, маю допуск до держтаємниці, 2018 року під час проходження військової служби у ЗСУ я за власною ініціативою звертався до посольства РФ з метою вирішення особистих побутових питань, не пов’язаних з моєю професійною діяльністю. Після мого візиту до дипустанови РФ, мені зателефонував співробітник консульського відділу та запропонував провести зустріч з метою вирішення моїх особистих питань. Після чого за допомогою месенджера WhatsApp мені надходило

декілька смс-повідомлень, які, як мені здалось, мали вербувальний характер. Від пропозиції провести зустріч і співпрацювати з представниками консульського відділу посольства РФ я категорично відмовився», – розповів один із українських військових.

У свою чергу, ще один військовий розповів, що протягом 2014-2018 років систематично їздив на територію окупованого Криму для відвідання родичів. Під час одного з таких візитів його затримали співробітники ФСБ РФ, які доправили українця до райвідділку для проведення допиту.

«Співробітників ФСБ цікавили питання щодо моїх функціональних обов'язків, персональні дані військовослужбовців, зокрема, керівного складу, обсяги інформації, до якої мене допущено, та порядок виїзду до тимчасово окупованих територій українськими військовослужбовцями. Після чого змушували мене надати згоду на конфіденційне співробітництво з метою збирання та передачі їм службової інформації. За виконання їхніх завдань мені обіцяли грошову винагороду», – розповів боєць.

Окрім цього він зазначив, що у разі відмови ФСБівці погрожували створити «суттєві проблеми» йому та його близьким і родичам.

Як зазначається, обидва офіцери інформації на шкоду інтересам держави не передавали.

Також у СБУ нагадали, що відповідно до ч. 2 ст. 111 КК України «звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їхніх представників жодних дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання», і закликали українців, яких намагалися вербувати російські спецслужби, невідкладно звертатись до правоохоронних органів України.

(вгору)

Додаток 15

30.01.2019
Ирина Фоменко
Закон Японии теперь позволяет взламывать IoT-устройства граждан

Япония одобрила поправку к закону, которая позволяет чиновникам взламывать устройства Интернета вещей (IoT). Об этом сообщает IoT News (InternetUA).

Поправка является частью исследования количества уязвимых устройств IoT, проведенного Национальным институтом информационных и коммуникационных технологий (NICT) под надзором Министерства внутренних дел и связи (MIC).

Япония проводит исследования с целью предотвратить использование устройств для кибератак на инфраструктуру в преддверии Олимпийских игр в Токио в 2020 году.

Еще в феврале прошлого года кибератака нанесла ущерб Олимпийским играм в Пхенчхане во время церемонии открытия. Вредоносное ПО Olympic Destroyer связывают с российскими злоумышленниками. Предполагается, что кибератака осуществлялась в ответ на запрет российским легкоатлетам участвовать в Олимпийских играх в Рио-2016.

Сотрудники NICT получат разрешение на попытку взлома IoT-устройств с использованием паролей по умолчанию и словарей паролей. Пользователи, которые оставляют пароли, установленные по умолчанию производителем устройства, часто подвергаются риску.

Когда будет обнаружено уязвимое устройство, отчет отправят как властям, так и интернет-провайдерам, при этом владельцу предложат защитить его.

Подход Японии является беспрецедентным, но активным способом решения проблемы безопасности IoT. В докладе, опубликованном MIC, подчеркивается, что две трети кибератак в 2016 году были направлены на устройства IoT.

Печально известный ботнет Mirai использовал более 100000 скомпрометированных устройств IoT, чтобы «зафлудить» DNS-провайдера Dyn рекордным объемом трафика – по сообщениям, в районе 1,2 Тбит/с – и нарушить работу популярных сервисов, включая Twitter, Spotify и PlayStation Network.

(вгору)

Додаток 16

17.01.2019

Wi-Fi можно использовать для шпионажа за людьми внутри помещения

Wi-Fi подходит для отслеживания перемещений. Чем больше хотспотов в здании или помещении, тем точнее будет результат наблюдения. Злоумышленнику достаточно будет погулять вокруг со смартфоном в руках (InternetUA).

Сквозь стены

Wi-Fi можно использовать для слежки за людьми «сквозь стены», причем для этого не требуется никаких особенных устройств, заявляют исследователи из Университета штата Калифорния в Санта-Барбаре.

Команда специалистов во главе с аспирантом Яньцзи Чжу (Yanzi Zhu) описала способ использования радиоволн с частотой 2,4-5 ГГц для отслеживания перемещений людей в помещениях, в которых находятся хотспоты Wi-Fi. Сами исследователи называют это «атакой», отмечая, что обнаруженный им способ слежки предоставляет практически беспрецедентные возможности для нарушения приватности.

Системы, позволяющие «смотреть сквозь стены» с помощью Wi-Fi, предлагались и ранее, однако у них было слишком много недостатков.

Ключевой – необходимость знать точное местоположение передатчика и быть подключенным к той же сети.

Новый способ этих недостатков лишен. Используя всего лишь обычный смартфон со встроенными средствами поиска беспроводных сетей (снифферами) любой желающий может «локализовать интересующего человека и следить за ним в его собственном доме или офисе, находясь при этом снаружи, и используя только отражения фоновых трансмиссий Wi-Fi», – пишут исследователи.

Прозрачный мир

Тут необходимо пояснить, о каких отражениях идет речь. Для сигналов Wi-Fi стены, двери, предметы мебели и люди почти прозрачны. «Почти» означает, что в сигнал все-таки вносятся определенные помехи и искажения. Если представить себе, что Wi-Fi – это излучение, видимое человеческому глазу (или камере), то получился бы очень странный ландшафт. С одной стороны, все полупрозрачное, с другой – отражений и преломлений будет столько, что разобрать что-либо окажется почти невозможным. Во всяком случае, в статике.

Однако любое движение заметить будет довольно просто: например, открывающаяся или закрывающаяся дверь наведет на все это пространство заметные искажения; человека обнаружить также будет довольно просто, поскольку люди отражают и преломляют Wi-Fi-излучение, в котором находятся сами.

При этом все-таки необходимо знать, где физически находится основной источник Wi-Fi-излучения (то есть, грубо говоря, ближайший роутер). Яньцзи и его коллеги нашли способ это делать: специальное приложение, использующее только Wi-Fi-антенну смартфона и встроенные акселерометры, позволяет измерять изменения в силе сигнала при движении условного «шпиона-недоброжелателя» вокруг здания или помещения, внутри которого находится искомый роутер. Последующий анализ изменений в силе сигнала позволяет вычислить примерное физическое месторасположение роутера, несмотря на все отражения и преломления.

Для достижения точности более 90 % исследователям понадобилось четыре раза пройтись по периметру нужного здания или помещения.

Ну, а чтобы точно установить местоположение роутера, понадобится план здания или помещения, которые, по крайней мере, в США, весьма легко добыть.

Дальше потенциальному соглядатаю останется только ждать, когда в интересующем его пространстве начнется движение с соответствующим наведением помех на радиоволны. Даже набор текста на компьютерной клавиатуре формирует достаточное количество искажений, чтобы их заметил Wi-Fi-приемник смартфона.

Исследователи применяли смартфоны Nexus 5 и Nexus 6 на базе Android. Им удалось проверить свой метод в 11 различных офисах и жилых помещениях, во многих из которых стояли несколько Wi-Fi-передатчиков.

Кстати, чем больше таких передатчиков, тем точнее результаты наружного наблюдения: если в обычной комнате располагаются два роутера или больше, точность отслеживания достигает 99 %.

Защита есть?

Что касается методов защиты, то их, как отметили исследователи, сразу несколько. Во-первых, геофенсинг, под которым здесь понимается географическое ограничение действия сигнала Wi-Fi – способ делать сигнал недоступным или почти недоступным за пределами данного здания или помещения. Реализовать его на практике сложно и неудобно для самих пользователей. Это потребует либо ослабить сигнал роутера, либо сделать его довольно узконаправленным, либо красить стены изолирующей краской (но тогда не пройдут и сотовые сигналы).

Второй метод – наведение шума в сигнал роутера, добавление фальшивых пакетов в трафик конечных устройств со случайной интенсивностью. Это сделает попытки вычислить точное местоположение точки доступа тщетными.

В целом, Яньцзи и его коллеги указывают, что само присутствие Wi-Fi-сигнала – это риск для приватности.

«В какой-то степени это правда, – считает Олег Галушкин, директор по информационной безопасности компании SEC Consult Services. – У всякого удобства есть цена, и возможность быть постоянно на связи, в свою очередь, означает несанкционированную вами возможность оказаться под чьим-то пристальным наблюдением. Является ли это поводом отказываться от технологий? Едва ли. Является ли это поводом изучать возможности защищать себя, свое личное пространство и свои данные? Вне всякого сомнения. Исследования Яньцзы и его коллег могут производить впечатление лишней сенсационности и алармизма, но на самом деле, практическая ценность подобных работ огромна».

(вгору)

Додаток 17

21.01.2019

До 200 браузерных расширений уязвимы для атак через веб-сайты

Прикладные программные интерфейсы (API) браузерных расширений могут использоваться для кражи конфиденциальных сведений об истории посещения веб-страниц, а также пользовательских закладок и даже файлов куки. С помощью последних, злоумышленник может взломать активную сессию авторизованного пользователя и получить доступ к его почтовым ящиками, профилям в соцсетях и к прочим учётным записям (Компьютерное Обозрение).

Более того, через уязвимые API можно организовать загрузку и сохранение на устройстве вредоносных файлов, запись в постоянную память

расширения той информации, которая в дальнейшем позволит отслеживать действия пользователя в Сети.

Эти типы атак проверил на 78 тыс. расширений Chrome, Firefox и Opera Дольер Сомэ (Dolière Francis Somé) из французского исследовательского института INRIA. С помощью разработанного им тестового кода, Сомэ смог выявить 197 расширений, у которых внутренние коммуникационные интерфейсы были открыты для веб-приложений. В нормальных условиях доступ к ним, а через них к пользовательским данным в браузере, может иметь (при наличии соответствующих разрешений) только собственный код расширения.

В выложенной им в открытом доступе статье Сомэ пишет, что к его удивлению лишь 15 (7,61 %) из 197 расширений можно отнести к категории средств разработки, которые, казалось бы, легче использовать для взлома.

Больше половины (55 %) уязвимых расширений были редко используемыми с числом загрузок менее 1000, однако свыше 15 % были установлены более 10 тыс. раз.

Сомэ ознакомил с результатами тестирования разработчиков браузеров ещё до публикации статьи. По его сведениям, Firefox уже удалила все проблемные расширения, Opera также устранила все кроме двух, позволяющих активировать загрузку. Команда Crome ведёт консультации с автором, решая, следует ли удалить расширения или ограничиться исправлением их кода.

Веб-приложение, созданное Сомэ, призвано упростить пользователям самостоятельную проверку наличия уязвимых API в файле manifest.json их браузерного расширения.

(вгору)

Додаток 18

21.01.2019

База Whois важна для борьбы с пиратством

Американский реестр интернет-номеров (ARIN) обратился к правительству Канады с просьбой потребовать от интернет-провайдеров продолжать вести базу IP-адресов и номеров Whois. Это помогает идентифицировать нарушителей авторских прав. База данных, которая уже существует, содержит получателей больших блоков IP-номеров (компании, университеты, госучреждения), а не физических лиц (Компьютерное Обозрение).

Одной из основных задач некоммерческой организации ARIN является распределение важнейших ресурсов интернета, включая адреса IPv4, адреса IPv6 и номера AS. Они не распределяются напрямую конечным пользователям, а отдаются крупным компаниям, включая Google и Amazon, интернет-регистраторам, а также интернет-провайдерам. До недавнего времени ARIN поддерживала базу данных Whois с помощью подхода «кнута и пряника». Компании регулярно возвращались, чтобы запросить новые IP-адреса (пряник),

и ARIN выделяли их только в том случае, если база данных Whois должным образом поддерживалась (кнут).

В письме, направленном правительству Канады в рамках пересмотра закона об авторском праве, ARIN подчеркивает, что база данных Whois является важным инструментом обеспечения прав интеллектуальной собственности.

«Когда в Интернете обнаруживаются материалы, нарушающие авторские права, или другой незаконный контент, Whois часто является первым пунктом исследования нарушителя, – говорит ARIN. – Правоохранительные органы и частные лица, чьи права нарушены, могут получить доступ к базе данных Whois либо в соответствии с политикой регистратора, либо по судебному решению».

Регистраторы не первый раз помогают бороться с пиратами. В 2015 г. ICANN предложил запретить «коммерческим» сайтам скрывать свои личные данные в Whois. Это поддерживалось группами правообладателей, включая MPAA, которые считают, что это поможет им привлекать к ответственности операторов нелегальных сайтов.

Напомним, что вопрос использования и модернизации базы Whois поднимается не первый год в контексте защиты персональных данных. Он является предметом дискуссий поборников конфиденциальности с одной стороны, а также всевозможных органов безопасности и структур защиты интересов правообладателей с другой.

(вгору)

Додаток 19

22.01.2019

Шпионаж смартфонов Huawei за владельцами подтвердили на видео

Вот уже как много лет компания Huawei занимается выпуском на рынок смартфонов, причем если раньше данный производитель старался выпускать только бюджетные модели, то теперь речь идет уже о премиальных аппаратах, стоимость некоторых из которых достигает $2000, пускай и продаются они лишь в Китае. Вот уже как больше года власти США обвиняют данного производителя в том, что его телефоны шпионят за своими владельцами, в результате чего бренду не позволяют начать официально продавать свою продукцию на американской территории (Украинский телекоммуникационный портал).

При этом правительство США не приводит никаких реальных доказательств своих слов, тогда как пользователи нашли их сами. Сегодня, 21 января 2019 года, шпионаж смартфонов Huawei за своими владельцами подтвердили на видео, причем уже сейчас любой желающий может убедиться в этом самостоятельно. Пользователи с форума Reddit обнаружили, что если использовать на телефоне от данного производителя Twitter, который

заблокирован в Китае как «враждебный сервис», то скачать из него изображения не получится.

В ходе эксперимента на телефоне Honor Note 10 для китайского региона удалось выяснить, что если скачать через приложение Twitter изображение на смартфон, оно автоматически удалится с него спустя несколько секунд. При этом на международной версии модели Huawei P20 Pro такого не наблюдается. Из этого следует, что китайские версии мобильных устройств данного производителя следят за своими владельцами. Они анализируют контент, который поступает на телефон, после чего цензурируют его.

И все это делается конечно же скрытно. Как считают пользователи с форума Reddit, подобные меры поиска запрещенного контента на смартфонах могут использоваться для скрытого шпионажа, ведь одно только руководство Huawei знает, по каким критериям осуществляется поиск фотографий, видеороликов, музыки и прочего контента, который автоматически удаляется со смартфона. Выходит, что гаджеты от данного производителя могут следить за самой разной активностью пользователя, вплоть до того, с кем и на какие темы он общается в мессенджерах.

(вгору)

Додаток 20

22.01.2019

Миллиарды ноутбуков, смартфонов и консолей оказались подвержены взлому по Wi-Fi

Специалисты по безопасности компании Embedi обнаружили серьёзные уязвимости в нескольких контроллерах Wi-Fi, используемых в миллиардах популярных устройств. Потенциальными жертвами злоумышленников могут стать обладатели консолей Xbox One и PlayStation 4, а также некоторых моделей ноутбуков, смартфонов, маршрутизаторов и другого оборудования с доступом к сети (InternetUA).

По словам представителей Embedi, злоумышленники могут взломать гаджеты с поддержкой Wi-Fi, чтобы выполнять произвольный код без каких-либо действий со стороны пользователя. Атака активируется каждый раз, когда уязвимое устройство выполняет поиск доступных сетей Wi-Fi, что зачастую происходит автоматически и на постоянной основе.

Уязвимость кроется в операционной системе реального времени ThreadX, которая используется в качестве встроенного программного обеспечения для многих контроллеров Wi-Fi. Экспертам Embedi удалось обнаружить четыре уязвимости, которые используют ошибку повреждения памяти, известную как «переполнение пула блоков». Она может быть вызвана во время сканирования доступных сетей без участия пользователя и позволяет загрузить вредоносный код на аппарат.

Одна из уязвимостей была обнаружена в широко используемом в технике контроллере Wi-Fi Marvell Avastar 88W8897. По словам представителей

Embedi, другие модели с прошивкой ThreadX также подвержены взлому аналогичным методом. Если верить официальному сайту ThreadX, по всему миру есть около 6 миллиардов устройств с этой прошивкой.

По умолчанию, уязвимые гаджеты настроены на сканирование новых сетей каждые пять минут, независимо от того, подключены ли они к Wi-Fi или нет. Следовательно, мошенники с лёгкостью могут внедрить свой код в аппарат ничего не подозревающего пользователя. Как только вредоносный код попадает на контроллер Wi-Fi, хакеры могут применить другие методы для отправки данных на устройство. Таким образом, злоумышленникам достаточно находиться в радиусе действия Wi-Fi жертвы, при этом им не нужно знать название или пароль сети.

Сотрудник Embedi Денис Селианин рассказал, что они передали сведения об уязвимостях Marvell ещё в начале мая 2018 года, но компания до сих пор не выпустила никаких исправлений.

(вгору)

Додаток 21

28.01.2019

Владимир Кондрашов

Эксперт: база клиентов крупного сервиса онлайн-кредитов «ушла» к хакерам

База клиентов небанковского сервиса кредитования Moneyveo.UA по состоянию на 2017 год обнаружена в сети Интернет на «профильных» форумах так называемого «даркнета» (InternetUA).

Базу данных компании, актуальную на 2017 год и содержащую 256625 записей о клиентах, включая их фамилии, дату рождения, телефон, e-mail, и паспортные данные, обнаружил в сети специалист по кибербезопасности Андрей Перевезий.

– Не думал, что меня можно чем-то шокировать. Moneyveo.UA, база Ваших клиентов тихонько гуляет по всемирной сети. База компании Moneyveo.UA по состоянию на 2017 год: 256625 записей – ФИО, дата рождения, телефон, e-mail, серия и номер паспорта, когда выдан, кем выдан. И эта вся прелесть в почти открытом доступе, – написал эксперт.

Как оказалось, в компании знают об утечке данных и по этому факту возбуждено уголовное дело.

– Источник данных установлен уже давно и нам известен, но, ссылаясь на тайну следствия, мы не могли делать никаких заявлений, – прокомментировал информацию Chief Information Officer (CIO) компании Moneyveo.UA Григорий Лисничий. – Установлены подозреваемые, которые уже задержаны. По всем упомянутым эпизодам ведется уголовное производство.

В подтверждение своих слов руководитель отдела ИБ компании продемонстрировал копию выписки из реестра досудебных расследований.

Компания по предоставлению небанковских кредитов, как следует из выписки из реестра досудебных расследований, 14 декабря прошлого года обратилась в полицию с заявлением о том, что неустановленное лицо 23 ноября 2018 совершило несанкционированный сбыт информации (базы данных клиентов) ООО «Манивео быстрая финансовая помощь».

В комментарии журналисту нашего издания Григорий Лисничий отметил, что сервис предпринял все необходимые меры по защите своих клиентов.

Согласно материалам дела, виновником утечки базы оказался сотрудник компании, который решил продать её конкурентам в Мексику. 28 сентября 2016 года в неустановленное следствием время сотрудник ООО «Манивео быстрая финансовая помощь» несанкционированно скопировал на мобильный телефон с электронно-вычислительной машины своих работодателей базу данных под названием «MoneyVeoMX». Уже дома злоумышленник скопировал указанную информацию на свой ноутбук, дав ей название «DB Mexico».

Сотрудник компании в Интернете обнаружил проект предприятия «МениМенМХ» по предоставлению денежных средств в Мексике, которому и предложил украденную ранее базу данных, договорившись о встрече. 6 февраля 2018, в неустановленное следствием время, подозреваемый встретился в Киеве в кафе с представителями упомянутой выше компании и продемонстрировал на своем ноутбуке базу данных. В этот же день и в этом же кафе сотрудника сервиса микрокредитования задержали правоохранители.

В пресс-службе Moneyveo.UA нам подтвердили, что обнаруженная экспертом информация о базе клиентов является копией тех данных, которые бывший сотрудник компании размещал на киберфорумах для рекламы предлагаемой «услуги»:

– В 2018 году службе информационной безопасности Moneyveo стало известно о попытке внутренней утечки информации, о которой компания сразу сообщила в правоохранительные органы. А именно – Moneyveo немедленно обратилась в киберполицию с соответствующим заявлением о преступлении по ст. 362 УК Украины (несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней), – сообщили в пресс-службе компании. – В рамках следствия сотрудники киберполиции изъяли все носители незаконно скопированной информации и сделали невозможным ее дальнейшее распространение.

В пресс-службе говорят, что ранее компания не делала никаких публичных заявлений в связи с тайной следствия, однако сейчас все подозреваемые задержаны и угрозы прямого распространения базы данных нет.

В Moneyveo подчеркнули, что постоянно совершенствуют все уровни защиты информации, которую пользователи предоставляют компании, а на предприятии установлена многоуровневая система доступа сотрудников к данным.

– С осени 2018 все новые сотрудники перед приемом на работу проходят проверку внутренней службы безопасности. А работники, имеющие доступ к данным пользователей, дополнительно тестируются на специальном устройстве – полиграфе, – рассказали в компании. – При разработке нашей системы скоринга и идентификации пользователей были учтены все требования законодательства Украины. Мы постоянно совершенствуем score-систему, предотвращая попытки мошенников получать кредиты в сервисе на чужие данные.

Также в компании уверяют, что регулярно проверяют систему доступа к данным сервиса и не допускают появления в ней уязвимостей.

– Сервис Moneyveo соответствует требованиям международного сертификата о защите карточных и персональных данных PCI DSS (Уровень 2). А в 2019 году мы планируем пройти сертификацию на уровень 1. Для резервных копий информации в сервисе используется система шифрования данных, – объясняют в пресс-службе. – Без согласия клиента мы не передаем его данные третьим лицам. Условия нашего кредитного договора содержат пункт о согласии на передачу данных бюро кредитных историй, факторинговым компаниям, правоохранительным органам.

Кроме того, для усиления контроля в августе 2018 Moneyveo внедрила Mobile Score – проверку надежности пользователей через обезличенные данные от провайдеров мобильной связи Kyivstar и Vodafone. А в октябре сервис заблокировал 99,99 % выдачу кредитов на банковские карточки, по которым невозможно определить владельцев. Также на сайте компании есть ликбез о защите данных пользователей.

(вгору)

Додаток 22

28.01.2019

Пользователи Instagram массово жалуются на невозможность восстановить аккаунт после взлома

Пользователи Instagram массово жалуются на проблемы с безопасностью на платформе – тысячи юзеров не могут восстановить свои аккаунты после того, как они были взломаны злоумышленниками. Более того, так как официальный процесс возвращения профиля слишком труден и громоздок, а администрация сервиса не справляется с нагрузкой, многие люди предпочитают обратиться к хакерам, чтобы побыстрее вернуть доступ к своим личным данным (InternetUA).

Украли средь бела дня

Так как аудитория Instagram растет с каждым днем и уже превышает миллиард человек, пользователи платформы все чаще становятся жертвами хакерских атак – злоумышленники взламывают аккаунты, меняют пароль и адрес электронной почты и становятся полноправными владельцами профиля.

Как оказалось, вернуть аккаунт обратно – задача не для слабонервных. По данным портала Mashable, за последние несколько месяцев около тысячи пользователей пожаловались на техническую поддержку Instagram.

По словам взломанных юзеров, процесс восстановления аккаунта очень трудный и медленный и вызывает не меньше стресса, чем сам взлом.

После того как пользователь заявляет о взломе профиля, ему приходит электронное письмо с просьбой записать на листе бумаги некий код и сделать с ним селфи либо предоставить администрации данные, которые были использованы при регистрации аккаунта. После этого техническая команда должна проверить подлинность информации, подтвердить личность пользователя и вернуть ему аккаунт.

При этом администрация Instagram не уточняет, что процесс восстановления профиля может занять недели и даже месяцы. Некоторые пользователи не выдерживают такого длительного ожидания и вообще отказываются от своих аккаунтов и использования Instagram.

«Взломали аккаунт? Можете с ним попрощаться», – пишет один из пострадавших пользователей на форуме.

Факт наличия проблемы признает и нынешний глава Instagram Адам Моссери.

«Это определенно та сфера, в которой нам следует приложить усилия. В настоящий момент мы работаем над тем, как облегчить жизнь людям, которые хотят вернуть свои аккаунты. Мы сообщим, как только появятся новости», – заявил Моссери в своем твиттере.

Пока же новости не появились, пользователи продолжают рассказывать о своем неудачном опыте восстановления Instagram-аккаунтов.

Стало только хуже

Фотограф Габриэль Тури обнаружила, что ее аккаунт был взломан в сентябре прошлого года. Она несколько раз пыталась вернуть его через техподдержку, но получала только уведомление о неправильном запросе – как оказалось, информация в профиле была полностью изменена злоумышленником.

Тогда Тури решилась на более радикальный шаг – она решила пожаловаться на собственный аккаунт «из-за нарушения авторских прав», чтобы его заблокировали. Фотограф надеялась, что в этом случае мошенник не получит доступа к ее личным данным.

Вскоре аккаунт был удален, но проблемы девушки на этом не закончились – теперь она не могла подключиться к своему второму аккаунту, привязанному к номеру телефона.

«Когда Instagram увидел мою жалобу, они удалили аккаунт, а заодно запретили мне пользоваться приложением, используя мой телефон», – рассказала Тури. Теперь она может заходить в Instagram только с ноутбука.

Другой пользователь по имени Клод рассказал, что потратил около месяца на восстановление своего аккаунта после того, как он был взломан, а электронная почта заменена на другую. По его словам, он тщательно выполнял

все инструкции техподдержки, но на последнем шаге бот предлагал отправить ему письмо с подтверждением сброса пароля на почту злоумышленника.

«Я снова обратился в Instagram, и они прислали мне точно такие же инструкции. Я объяснил, что я не могу отвечать с почты хакера, но в ответ я получил такое же автоматизированное сообщение... Если бы я смог поговорить с человеком, а не с роботом, этот процесс завершился бы гораздо раньше», – считает Клод.

Хакеры против хакеров

В Instagram-пространстве существуют не только рядовые пользователи, но и так называемые инфлюэнсеры – блогеры, которые воздействуют на аудиторию с помощью своего аккаунта. Количество их подписчиков может превышать сотни тысяч и даже миллионы человек, и поэтому их профили становятся желанной добычей хакеров.

Неудивительно, что после взлома популярные пользователи Instagram желают вернуть свои профили как можно скорее – для многих деятельность на платформе является крупным источником дохода, кто-то хранит конфиденциальную информацию в личных сообщениях, а кто-то просто не может нормально существовать без ежедневных публикаций.

Техподдержка Instagram не подразумевает ускоренного обслуживания для своих «звезд», поэтому им приходится ждать в общей очереди. По данным Motherboard, некоторые из взломанных блогеров настолько отчаялись, что прибегают к помощи других хакеров, которые за вознаграждение возвращают аккаунты гораздо быстрее, чем сам Instagram.

«Я потратил трое суток, чтобы связаться с техподдержкой Instagram, но так и не смог ничего от них добиться. Я звонил сотни раз и еще столько же писем отправил», – заявил один из пострадавших блогеров. Его «коллега» подтверждает, что Instagram не сделал ничего, чтобы ему помочь, кроме того, что отправил большое количество автоматизированных сообщений.

Обоим помог некий хакер, который вернул аккаунты, но не стал раскрывать подробностей операции. Он лишь заявил о том, что взломал устройства злоумышленников, похитивших аккаунты, чтобы добыть информацию о новых паролях.

(вгору)

Додаток 23

30.01.2019
Facebook покупает данные за $20
Надежда Якимаха

Приложение Facebook Research имеет полный доступ к данным пользователей. За такую роскошь компания платит $20/мес каждому «подопытному» юзеру 13–35 лет (Телекритика).

Издание TechCrunch сообщает, что Facebook платит пользователям $20 в месяц за установку на смартфон приложения Facebook Research с полным

доступом к личным данным. С 2016 года Facebook платит пользователям в возрасте от 13 до 35 лет до 20 долларов в месяц плюс реферальные сборы, чтобы они смогли продать свои конфиденциальные данные через приложение «Facebook Research» для Android (ранее и для iOS). Facebook даже просит пользователей делать скриншот страницы истории заказов Amazon. Эти данные могут помочь Facebook связать привычки просмотра и использования других приложений с предпочтениями и поведением при покупке. Полученная информация может быть использована для точного определения таргетинга рекламы и понимания того, как и какие продукты покупают пользователи.

Приложение управляется через службы бета-тестирования Applause, BetaBound и uTest, чтобы скрыть участие Facebook. Facebook платил пользователям за то, что они загружали VPN-приложение Facebook Research за пределами App Store.

Facebook начал распространять приложение Facebook Research VPN в 2016 году под названием Project Atlas. С середины 2018 года, когда усилилась негативная реакция на Onavo Protect, и Apple ввела новые правила, запрещающие Onavo, распространение приложения стало более активным. Ранее аналогичная программа называлась Project Kodiak. Facebook не хотел прекращать сбор данных об использовании смартфонов, поэтому программа исследований продолжалась, несмотря на то, что Apple запретила Onavo Protect.

«Если Facebook полностью использует уровень доступа, который ему предоставляют через установку приложения, он получат возможность непрерывно собирать данные следующих типов: личные сообщения в приложениях социальных сетей, чаты в приложениях для обмена мгновенными сообщениями, в том числе фотографии, видео, отправленные другим, электронные письма, веб-поиск, просмотр веб-страниц и даже текущую информацию о местонахождении, если у пользователя установлены приложения для отслеживания местоположения», – комментирует эксперт по безопасности Guardian Mobile Firewall Уилл Страфач.

То есть Facebook получает практически неограниченный доступ к устройству пользователя после установки приложения. У Apple уже был конфликт с компанией, когда та собирала данные через приложение Onavo Protec. Впоследствии его убрали из App Store. Сегодня приложение Facebook Research недоступно на Apple, как и Onavo Protec. Возможно, компания попросила Facebook прекратить распространение своего приложения. Тим Кук, генеральный директор корпорации Apple, неоднократно критиковал методы сбора данных Facebook, ведь они не подчиняются политике iOS по сбору дополнительной информации.

Facebook впервые занялся бизнесом по отслеживанию данных в 2014 году, когда приобрел Onavo примерно за 120 миллионов долларов. Приложение помогло пользователям отслеживать и минимизировать использование своего мобильного тарифного плана, а также предоставило Facebook глубокую аналитику о том, какие другие приложения они используют. Так, Facebook смог узнать, что WhatsApp отправлял в два с лишним раза больше сообщений в день,

чем Facebook Messenger. Onavo позволил Facebook заметить стремительный рост WhatsApp и оправдать уплату 19 миллиардов долларов за запуск чата в 2014 году.

Установить Facebook Research могут пользователи от 13 до 35 лет. Подростки делают это только с письменного согласия родителей. Если несовершеннолетний пользователь пытается зарегистрироваться, его просят получить разрешение его родителей с помощью формы, которая сообщает об участии Facebook и говорит: «Нет никаких известных рисков, связанных с проектом, однако вы признаете, что проект связан с отслеживанием личной информации через приложения вашего ребенка. Вы получите компенсацию за участие вашего ребенка».

Сайт The Applause обозначил, какие данные собирает приложение Facebook Research: «Устанавливая программное обеспечение, вы даете нашему клиенту разрешение на сбор данных с вашего телефона, что поможет понять, как вы используете интернет и функции в установленных вами приложениях. Это означает, что вы разрешаете нашему клиенту собирать информацию, например, о том, какие приложения находятся в вашем телефоне, как и когда вы их используете, данные о ваших действиях и контенте в этих приложениях, а также о том, как другие люди взаимодействуют с вами или вашим контентом в этих приложениях. Вы также позволяете нашему клиенту собирать информацию о вашей активности в интернете (включая посещаемые вами веб-сайты и данные, которыми обмениваются ваше устройство и веб-сайты) и об использовании вами других онлайн-сервисов. В некоторых случаях наш клиент будет собирать эту информацию даже в том случае, когда приложение использует шифрование или безопасный просмотр».

Страница регистрации BetaBound с URL-адресом, оканчивающимся на «Atlas», информирует, что «с помощью электронных подарочных карт за $20 мес. вы установите приложение на свой телефон и запустите его в работу в фоновом режиме». На этом сайте изначально не упоминается Facebook, но инструкция по установке Facebook Research раскрывает причастность компании. Заметим, похоже, Facebook намеренно избегала TestFlight, официальной системы бета-тестирования Apple, которая требует, чтобы Apple проверяла приложения. В руководстве пользователя показано, что «подопытные» загружают приложение с веб-сайта r.facebook-program.com и получают указание установить сертификат Enterprise Developer Certificate и VPN, а также «доверить» Facebook права root-доступа к данным, которые передает их телефон.

TechCrunch поручил Strafach проанализировать приложение Facebook Research и выяснить, куда оно отправляет данные. Данные перенаправляются на «vpn-sjc1.v.facebook-program.com», который связан с IP-адресом Onavo, а домен facebook-program.com зарегистрирован в Facebook, согласно MarkMonitor. Приложение могло обновляться без взаимодействия с App Store и было связано с адресом электронной почты PeopleJourney@fb.com. Также обнаружили, что корпоративный сертификат, впервые полученный в 2016 году,

указывает на то, что Facebook обновил его 27 июня 2018 года – через несколько недель после того, как Apple объявила о новых правилах, запрещающих подобное приложение Onavo Protect.

Facebook никогда публично не рекламировал Research VPN и использовал посредников, которые часто не раскрывали информацию об участии Facebook, пока пользователи не начинали процесс регистрации. Приложение не подчеркивает и не упоминает о полном объеме данных, которые Facebook может собирать через VPN.

Представители Facebook не отрицают информации о своем сервисе и уточняют, что не делятся этой информацией с другими компаниями.

(вгору)

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Терещенко** Ірина Юріївна

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
Сайт: http://nbuviap.gov.ua/
http://сіаз.укр/
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.