СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1.02–14.02)

2017 № 3

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1.02–14.02)
№ 3

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 2017

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

1.02.2017
Lego запустила детскую социальную сеть

Lego запустила социальную сеть «Lego Life» для детей возрастом младше 13 лет (mediabusiness).

Участники могут делиться собственным творчеством, публиковать фотографии и ролики, а также обсуждать постройки из конструктора. При этом общаться дети смогут только с помощью эмодзи.

В компании Lego решили, что детям не хватает собственной социальной сети, чтобы общаться с ровесниками и делиться фотографиями построек из конструктора. Поэтому вместе с благотворительной организацией «ЮНИСЕФ» Lego запустила детскую социальную сеть для детей младше 13 лет.

«Детям хочется делиться своими творениями из конструктора не только с семьей и друзьями, но у них не было никаких своих соцсетей для этого. С “Lego Life” они могут всего за пару минут показать свои постройки всему миру», – старший директор «Lego Life» Р. Лоу.

Чтобы присоединиться к сети, надо скачать приложение, которое доступно на iOS и Android. Пока что проект запущен в четырех странах: США, Великобритании, Германии и Франции. Приложение было разработано в первую очередь для платформы Apple и планшетов Amazon Kindle.

***

2.02.2017
Instagram позволит делиться несколькими фото в одном посте

Новую функцию заметили в последней версии приложения для Android. Вероятно, тестирование проходит для небольшого количества пользователей. Напомним, подобные фотоальбомы, под официальным названием «карусели», Instagram запустил в рекламных постах еще в 2015 г. Компания пока не дала комментариев относительно этой функции. Новшество позволит загружать до 10 фото из галереи, накладывать фильтры на каждое фото и загружать их в виде альбома в ленту. Фолловеры будут видеть альбом, просматривать фото и отмечать их лайками (Marketing Media Review).

***

2.02.2017
Twitter станет активнее бороться с оскорблениями

Twitter собирается добавить в сервис ряд улучшений, которые сделают сервис «более безопасным местом». В целой серии твитов вице-президент компании по разработке Э. Хо (Edward Ho) признал то, что все и так уже давно знали: Twitter проделала громадную работу в уменьшении случаев оскорбления пользовательской аудитории сайта. В течение недели пользователи начнут замечать признаки того, что компания пытается всё исправить. В частности, будут внесены исправления в систему блокировки пользователей, а недоброжелатели больше не смогут создавать новые аккаунты (ТОНЕТО).

Представитель Twitter также сообщил сайту VentureBeat следующее: «Мы подходим к безопасности со всей серьёзностью. Поэтому в ближайшие дни и недели мы внесём ряд изменений в продукт – некоторые из них станут заметны сразу же, а другие будут направлены на специфичные случаи. В процессе мы будем делиться с вами новой информацией и продолжим тестировать, учиться и перебирать эти изменения для оценки их эффективности. Вы можете ожидать существенного прогресса в этой сфере».

Борьба с оскорбительными и унизительными твитами в сервисе была объявлена высшим приоритетом для компании – особенно после того как генеральный директор Twitter Дж. Дорси (Jack Dorsey) в конце прошлого года попросил пользователей активно делиться своими мнениями по этому поводу. Дж. Дорси признал, что, «впереди много работы», отметив, что компания движется в нужном направлении не очень быстро. Теперь Э. Хо говорит, что Twitter хочет прогрессировать «в рамках дней и часов, а не недель и месяцев».

***

1.02.2017

Базиленко Анна

Facebook прибере зі стрічки новин публікації сторінок, які поширюють спам і накручують лайки

Facebook вкотре оновив алгоритм стрічки новин: тепер у ранжуванні будуть враховуватися актуальність і релевантність публікацій. Таке нововведення – черговий крок і боротьбі з фейковими новинами, йдеться в офіційному блозі компанії (Watcher).

Автентичність публікацій буде оцінюватися за кількома критеріями, включаючи категорію сторінки. Зокрема, чи були у неї порушення, пов’язані з розміщенням спаму або накруткою лайків. Також буде враховуватися поведінка користувачів: якщо вони приховують публікації сторінки, то її контент може вважатися нерелевантним.

На видимість контенту також впливатимуть Real-Time Signals: Facebook буде оцінювати залученість користувачів у взаємодію з публікаціями. Якщо публікації отримують багато коментарів і лайків, то алгоритм розцінюватиме це як ознаку важливості та актуальності. Відповідно, видимість такого контенту зросте.

У компанії зауважують, що оновлення не вплине на публічні сторінки, однак, за умови, що вони не користуються забороненими прийомами.

Як відомо, Facebook став першою соціальною мережею, яка відмовилась від простого хронологічного формату стрічки новин. Алгоритми соціальної мережі дозволяють відбирати найбільш цікаві для користувача матеріали і виводити їх «в топ». Таким чином, різко зростає популярність публікацій на персональних сторінках окремих користувачів, водночас як офіційні сторінки втрачають інтернет-аудиторію.

У липні 2016 р. Facebook оновив алгоритм стрічки новин: публікації членів сім'ї і друзів користувача почали показуватися частіше, аніж пости компаній та ЗМІ.

***

1.02.2017

Вышло большое обновление Viber для iOS

Мессенджер Viber анонсировал большое обновление клиента для мобильных устройств Apple. В числе нововведений программы заявлена поддержка исчезающих сообщений, отправка медиафайлов без сжатия, поддержка интерактивных уведомлений iOS 10 и короткие видео (InternetUA).

Функция «самоуничтожения» может быть активирована для любой фотографии или видео в Viber по нажатию соответствующей иконки. Включение опции запускает режим съемки фотографии или видеоролика, который автоматически исчезнет из ленты сообщений после просмотра. К «исчезающему» кадру можно добавить подпись. После подтверждения отправки, данные пересылаются собеседнику. Режим будет работать только для выбранной беседы, а не на всех пользователей в Viber, и может быть отключен в любой момент.

Второе нововведение мессенджера предусматривает пересылку контента без сжатия. В частности, это позволяет отправлять оригинальные фотографии и видео без потери качества. Функция опять же опциональная, пользователь может включить или отключить ее при отправке.

Также обновленный Viber получил поддержку интерактивных уведомлений iOS 10. Впервые уведомления, на которые можно отвечать не переходя в приложение появились в iOS 9. В десятой редакции ОС компания Apple реализовала еще более функциональные оповещения: теперь можно просматривать содержимое чата, не заходя в Viber.

Кроме того, обновленный Viber позволяет записывать короткие видеосообщения продолжительностью до 30 секунд. Записать и отправить такой ролик просто: функция встроена в окно чата. Режим включается однократным нажатием с удерживанием на кнопку отправки. При активации автоматически запускается фронтальная камера, а не основная, как у функции отправки видеофайла.

***

2.02.2017
Facebook начала тестировать онлайн-сервис знакомств

Социальная сеть Facebook выходит в сегмент онлайн знакомств. Компания приступила к тестированию нового сервиса под названием Discover People, сообщает Joinfo.ua. (Донбасс).

Пользоваться сервисом смогут те, кто заходит в соцсеть с мобильных приложений Facebook для Android и IOS. Discover People будет представлять собой отдельный раздел приложения, который поможет пользователям находить людей, которые имеют схожие интересы.

Цель этой функции – помочь пользователям сети в установлении новых деловых контактов, поиске друзей и даже романтических отношений.

На практике, услуга является своего рода каталогом профилей в Facebook. По данным компании, это облегчит общение людей со схожими интересами, не раскрывая деталей профилей пользователей, если они не хотят предоставления такой информации.

***

3.02.2017
Базиленко Анна
Штучний інтелект Facebook шукатиме фото за ключовими словами

Facebook дозволить шукати фото за ключовими словами, які описують контент зображення. Оновлення, яке компанія тестує у пошуковому функціоналі соцмережі, стало можливим завдяки напрацьованим алгоритмам «машинного зору». Нововведення тестується в США і є доступним у мобільній і веб-версії Facebook (Watcher).

Користувачі зможуть знаходити зображення не лише за тегами, а й за ключовими словами, що описують деталі фотографій.

Наприклад, можна задати пошук за допомогою фрази «картинки піци» або «фото помаранчевих сорочок» – і в результаті отримати вибірку фотографій друзів, які відповідають цьому опису. Такі публікації Facebook покаже в топі видачі, слідом за ними – варіанти зображень, релевантних запиту користувача.

Для оптимізації точності видачі Facebook також може здійснювати пошук по підписах до фото або коментарів.

Функція розпізнавання зображень Facebook працює на основі тієї ж технології, що впроваджена в iOS 10 або Google Photos.

За інформацією SocialMediaToday, у майбутньому соцмережа планує запустити «контекстний» пошук і по відео.

***

5.02.2017

С 1 марта старые версии Skype на Windows и Mac перестанут работать

Разработчики того или иного программного обеспечения то и дело прекращают поддержку старых версий своих приложений (iLenta.com).

Та же участь ожидает и пользователей старых версий Skype для операционных систем Windows или Mac. Их работа будет прекращена, начиная с 1 марта.

Такое заявление было опубликовано в официальном блоге компании Microsoft. Софтверный гигант поясняет это тем, что он старается предоставлять своим пользователям наилучший контент и опыт использования Skype.

Если не обновлять приложение, то такого опыта пользователи получить не смогут и их устройство может оказаться под угрозой взлома злоумышленниками.

С 1 марта те, кто использует старые версии Skype для Windows, (7.16 и ниже) или Mac (от 7.0 до 7.18), больше не смогут войти в систему. Им нужно обновить клиент приложения.

***

3.02.2017

Ежемесячная аудитория Facebook приближается к отметке в 2 миллиарда

Компания Facebook подвела итоги своей работы в последней четверти прошлого года и в целом за весь 2016 г. (IGate).

Доход и чистая прибыль соцсети растут. Так, за трехмесячный период выручка Facebook достигла отметки в 8,8 млрд долл., что сразу на 51 % больше результата последнего квартала 2015 г. В общем объеме доходов на рекламные поступления пришлось порядка 8,6 млрд долл.

Если же смотреть общие показатели за год, то стоит отметить, что выручка компании поднялась на 54 % – с 17,9 до 27,6 млрд долл. При этом на рекламу пришлось 26,9 млрд долл.

В Facebook отметили, что популярность соцсети продолжает расти. Размер ее месячной аудитории активных пользователей за последний год увеличился на 17 %, достигнув 1,86 млрд человек. Таким образом, в ближайшее время мы станем свидетелями преодоления грандиозной отметки в 2 млрд пользователей.

В компании обратили внимание и на рост ежедневной активной аудитории. Так, за 2016-ый она увеличилась более чем на 18 % и составила 1,23 млрд пользователей. Число активных мобильных пользователей соцсети достигло 1,15 млрд в сутки, что почти на 23 % больше в сравнении с 2015 г.

***

6.02.2017

Facebook работает над возможностью прокрутки контента при помощи наклона устройства

В последние дни января Facebook опубликовал патент, в котором описывается любопытная технология по управлению смартфоном 3D-жестами. Теперь же в прессе появилось информация об еще одном патенте, поданном еще в октябре 2016 г. и продленным в конце прошлой недели, что доказывает активность ведения работы над технологией. Этот патент описывает способ скроллирования изображения на мобильном устройстве путем его наклона. При этом жест наклона отрабатывает при наклоне во все стороны. В Facebook уточнили, что такая функция будет направлена на демонстрацию любого визуального контента, будь-то веб-страница, фотография, карта или еще что-нибудь (IGate).

Интенсивность прокрутки будет измерять наклоном, который будет фиксироваться встроенным гироскопом. Скроллинг содержимого начинается, когда гироскоп фиксирует минимальное значение наклона – прокрутка, соответственно, также будет медленной. Пользователь сможет проделать то же самое и традиционным способом – касаниями экрана.

Facebook указывает в патенте, что новый метод может использоваться и в играх. Вероятно, разработчики компании собираются предоставить людям возможность запускать игры в формате виртуальной реальности и на обычным мобильных устройствах в будущем.

***

7.02.2017

Google запускає сервіс, який перевірятиме фейки

Компанія Google оголосила про запуск проекту CrossCheck, який допоможе спільно перевіряти новини, що містять у собі недостовірну інформацію (Espreso.tv).

Про це повідомляє TechCrunch.

Метою CrossCheck є розвиток інструментів по боротьбі з верифікацією новин, які з’являються онлайн.

Медіа- і IT-компанії об’єднають свої зусилля, щоб усі чутки, інформаційні вкидання та фейкові публікації були своєчасно видалені з Інтернету.

Сервіс буде запущено 27 лютого 2017 р. у Франції і активно працюватиме під час президентських виборів у цій країні.

***

8.02.2017

Чат-бот исследовал предпочтения украинских пользователей Facebook

ENGINE Digital взяли чат-бота на работу как интерна с целью провести анкетирование, какой контент действительно цепляет пользователей, а какой – раздражает, на что подписчики готовы пойти ради бренда, а из-за чего – отписаться. Чуть менее половины опрошенных 236 респондентов ответили, что пользуются Facebook постоянно со всех гаджетов, 31 % отдает предпочтение смартфону или планшету, и только 22 % опрошенных «юзают» исключительно стационарный компьютер для чтения своей ленты. В пять раз больше пользователей в первую очередь обращают внимание на посты друзей, а не брендов. Но, все же, 14,9 % опрошенных замечают первыми публикации брендов, и только 7,8 % – тематических пабликов (Marketing Media Review).

Пользователи подпишутся на страничку бренда, если контент будет полезным и интересным – так ответили 58,4 % опрошенных. Еще 28,8 % готовы подружиться с брендом, если уже пользуются его продуктом. Известность бренда подкупает только 5,5 % респондентов, реальная возможность выиграть подарок – 4,5 %, навязчивая реклама – 1,8 %. И лишь 1 % опрошенных «френдит» бренды ради того, чтобы написать негативный отзыв.

Пропорционально разделились мнения юзеров касательно того, какие действия брендов в Facebook их раздражают. Постоянно просите шерить конкурсы или пишете на левые темы – вызываете гнев у 20,5 % пользователей на каждый пункт. Почти столько же ненависти (18,5 %) заработаете, если не отвечаете на сообщения. Несмешные шутки раздражают 15,1 % респондентов, однообразный контент – 13,2 %, плохое визуальное оформление – 12,7 %.

Кстати, с конкурсными механиками на Like & Share выводы неутешительны: больше половины опрошенных (57,1 %) не принимают в них участие, 37,2 % – только если подарок уж больно нужен. 5,6 % честно сознались: они призоловы.

Хорошие новости для брендов, которые используют live stream: 39,7 % пользователей утверждают, что смотрят их, но только если событие уникальное. Еще 6,9 % смотрят, потому что смотрят все подряд. 41,2 % людей реагируют лишь на лайвы друзей, а вот 12,3 % даже не знают, что это. Из другого хорошего: только 18,8 % пользователей ни разу не ходили на страничку бренда, чтобы просмотреть его старый контент. Остальные же делают это регулярно.

Относительно коммуникации с брендом: 53,9 % респондентов заявляют, что свое мнение о бренде напишут у себя на страничке и тегнут его. 25,5 % пользователей пойдут писать на страничку бренда. И только 20,4 % опрошенных скромно напишут ему в личку.

«89 % пользователей ответили, что им понравилось общение с ботом, почти половина хотела бы общаться с ним в будущем и треть – продолжили коммуникацию после окончания опроса. Это отличные показатели в пользу чат-ботов. Вкалывают роботы – счастлив человек», – отметил Д. Федотов, CEO & Co-Founder Unibot, компании-разработчика.

***

9.02.2017

Facebook запровадить функцію колективної допомоги у випадку стихійного лиха

Соціальна мережа Facebook розширює можливості сервісу Safety Check, який автоматично активується в разі кризових ситуацій. Тепер у ньому буде доступна опція Community Help (допомога спільноти), яка допоможе організувати взаємодопомогу під час стихійних лих (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє BBC.

Кожен користувач Facebook, який опинився в районі, в якому автоматично активується опція Safety Check (вона запускається в разі, якщо з одного місця надходить багато повідомлень про якесь лихо чи страшну подію), зможе запропонувати оточуючим чи замовити у них їжу, напої, дах над головою або можливість скористатися транспортним засобом.

Для зручності відповідна сторінка Facebook містить категорії допомоги. Там також містяться розділи «їжа для тварин», «дитячі речі», «одяг».

Крім того, Community Help допоможе в пошуку людей в зоні лиха і забезпечить з ними зв'язок.

На початку Community Help працюватиме в тестовому режимі лише в умовах природних катастроф і лише в США, Канаді, Австралії, Новій Зеландії, Індії та Саудівській Аравії.

Потім, за результатами тестового періоду, всі помічені недоліки будуть виправлені, і вона буде доступна для всіх країн і для всіх кризових ситуацій.

***

8.02.2017

Google, «ВКонтакте» и YouTube лидируют в рейтинге популярных сайтов в январе

2017 г. для рейтинга популярных сайтов начался без изменений в лидерах. Google.com+Google.com.ua, Vk.com, YouTube.com, Mail.ru и Yandex.ua – вот первая пятерка январского топа сайтов, по данным интернет-исследования KANTAR TNS CMeter. Закрытие сайтов Ex.ua и Fs.to позволило сайту My-hit.org подняться на 21-ю позицию. Интересно, что между двумя погодными ресурсами Sinoptik.ua и Gismeteo.ua разница в 6 пунктов и более 10 % охвата. ТОП-25 закрывает сайт по поиску работы Work.ua (Marketing Media Review).

***

8.02.2017

Twitter будет навсегда блокировать агрессивных пользователей

Сервис микроблогов Twitter расширяет кампанию против разжигания ненависти и агрессии в соцсети, сообщает «Русская служба BBC» (Телекритика).

Так, теперь компания будет устанавливать личность пользователей, чьи аккаунты были заблокированы за оскорбительное поведение, для того чтобы они не могли создать новые аккаунты, то есть были навсегда отлучены от Twitter.

Кроме того, соцсеть работает над созданием системы так называемого «безопасного поиска», которая будет исключать твиты с потенциально чувствительным содержанием. Твиты с потенциально оскорбительным содержанием удаляться не будут, однако система их исключит из результатов поиска по конкретному запросу.

Twitter также работает над исключением из поиска потенциально оскорбительных и «низкокачественных» обсуждений, которые мало связаны с заданной темой. Эти обсуждения не будут удаляться, но компания сделает их менее заметными для пользователей.

***

6.02.2017

В преддверии выборов Facebook вводит фильтр фейковых новостей во Франции

Социальная сеть Facebook объявила о сотрудничестве с восемью французскими медиакомпаниями, чтобы проверять и фильтровать фейковые публикации в преддверии президентских выборов по Франции. Об этом сообщает The Verge (InternetUA).

Эта кампания схожа по сути с введением фильтра недостоверной информации, запущенного в прошлом году в США и в январе в Германии. Пользователи могут заявить о публикации, которая им покажется фейковой, после чего она отправится на экспертизу до вынесения вердикта. В случае признания новости фейком она получит специальную отметку, которая будет видна всем, кто читает ленту.

***

7.02.2017

Украинская аудитория «Одноклассников» приблизилась к 10 миллионам

Во время практической конференции Digital Brand Coupage в Киеве, представители российской социальной сети «Одноклассники» рассказали, что каждый день в Украине этот сайт посещает пять с половиной миллионов пользователей. Основная аудитория – люди в возрасте от 26 до 35 лет.

Информация об этом появилась в блоге соцсети. Новость передает «Пресса Украины».

«Ежемесячное количество посетителей сети “Одноклассники” в Украине сосставляет 9,5 млн, ежедневное – 5,4 млн. В целом, “ОК” занимает второе место по веб-аудитории в стране, опережая Facebook, и первое по времени пребывания в сети», – говориться в сообщении.

По словам представителей этой соцсети, среди украинских пользователей больше всего людей в возрасте от 26 до 35 лет, что представляет 30 % от общего количества.

Кроме того, было отмечено и то, что 49 % всех посетителей сайта в Украине заходят в социальную сеть с мобильных устройств.

На конференции Digital Brand Coupage представители «ОК» объявили информацию, что отныне есть официальный представитель этой сети в Украине. Им стал К. Косоноцкий, который будет отвечать за развитие бизнеса проекта в государстве и работу с рекламными агентствами.

***

14.02.2017
В Twitch появились сообщества

В стриминговом сервисе Twitch появились сообщества – новый способ поиска контента и подбора целевой аудитории. Новый раздел, находящийся в стадии открытого бета-тестирования, помогает пользователям искать контент в таких категориях, как скоростное прохождение, ретро-игры, косплей, кулинария и другие (InternetUA).

Сообщества направлены на то, чтобы пользователи самостоятельно организовывались в группы по интересам и деятельности, через которые стримеры могут подбирать подходящую аудиторию, а также помогать зрителям находить контент, который может быть им наиболее интересен. Создавать сообщества могут любые зрители и стримеры.

«От наших стримеров и зрителей мы узнали, что они хотят иметь свободу в создании конкретных групп на основе таких тем, как скоростное прохождение, киберспорт, косплей и рисование, – заявила Ш. Раджу (Sheila Raju), менеджер по маркетингу Twitch. – С помощью сообществ мы даём нашим пользователям возможность создавать группы на свой выбор, а также предоставляем авторам очередной инструмент для расширения аудитории. Если у вас есть интерес, разделяемый другими, то сообщества – это то место, где такой коллектив может существовать».

Пользователям предоставляется целый набор инструментов для создания и управления сообществами. Руководители могут настраивать главную страницу, назначать модераторов, вводить определённые правила и предоставлять подписчикам доступ к актуальным трансляциям. Зрители и стримеры могут просматривать списки стримов в сообществах и подбирать те, которые наиболее соответствуют их тематике.

***

12.02.2017

В приложении Facebook появился раздел с погодой

Судя по всему, Facebook планирует добавить в свои мобильные приложения всё, чем только можно пользоваться на телефоне: игры, фильтры для фотографий и видеороликов, чаты, магазины, а теперь и прогноз погоды. В приложениях Facebook появился полноценный раздел с погодой, доступ к которому, как заявил представитель компании сайту TechCrunch, могут получить уже около 95 % пользователей по всему миру (ТОНЕТО).

Чтобы найти новый раздел, необходимо через главное меню нажать на кнопку «Увидеть больше» – под вкладками «Друзья», «События», «Группы» и так далее располагается кнопка «Погода». Там же можно найти некоторые экспериментальные функции компании – например, инструмент для поиска открытых точек доступа Wi-Fi. Есть и ещё один способ найти раздел с погодой: в самом верху новостной ленты может появиться приветствие от Facebook с прогнозом на день и ссылкой на раздел.

В нём присутствует базовый прогноз на пять дней, в котором говорится, будет ли погода солнечной или, например, дождливой. Там же указана температура на каждый час. Вся информация предоставляется погодным сервисом Weather.com и отображается благодаря её интерфейсу программирования приложений. По умолчанию погода показывается для текущего местоположения пользователя, но это всегда можно изменить через настройки приложения – как и сменить формат отображения температуры.

TechCrunch

Специализированные погодные приложения предлагают более подробные сведения и обычно позволяют просматривать информацию о погоде сразу в нескольких местах. Тем не менее, Facebook может стать достойной альтернативой таким сервисам – особенно для тех, кто испытывает недостаток свободной памяти на смартфоне.

***

13.02.2017

Базиленко Анна

Кожен п’ятий українець дізнається про стан справ в країні з соцмереж

«Детектор Медіа» оприлюднила результати дослідження впливу російської пропаганди на суспільну думку в Україні. В опитуванні взяли участь 2040 респондентів зі 110 населених пунктів (лише на територіях, що контролюються урядом України) (Watcher).

Так, згідно з результатами дослідження, українці продовжують дізнаватись інформацію про стан справ у країні переважно з загальнонаціональних телеканалів – 87,1 % опитаних. 40,7 % – отримують інформацію з онлайн-ЗМІ. Загальнонаціональні газети та радіо суттєво відстають – 17 та 16,5 % відповідно.

Водночас з російських телеканалів отримують інформацію 7,9 % українців. Водночас майже половина опитаних (47,7 %) отримують інформацію про події в Україні з неофіційних джерел – від родичів, друзів, сусідів, колег по роботі.

Як з'ясувала «Детектор Медіа», українському телебаченню найбільше довіряють як джерелу інформації про збройне протистояння на Донбасі, довіра до російських телеканалів майже на нулі.

40,4 % опитаних українців довіряють загальнонаціональним телеканалам. На Сході довіра до центральних телеканалів значно нижча – 22,2 %. На другому місці, зі значним відривом, за довірою – родичі, друзі, сусіди, колеги по роботі (18,8 %), на Сході ця цифра становить 13,4 %. На третьому – інтернет-ЗМІ – 17,5 % (на Сході – 14,2 %). Іншим видам ЗМІ довіряють вкрай мало: радіо – 5,3 % (Схід – 0,5 %), газети – 3,8 % (Схід – 1,4 %), соцмережі – 7,1 % (Схід – 1,9 %).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

2.02.2017

Дмитрий Демченко

Сервис такси Lyft впервые обошел Uber по числу скачиваний из-за протеста против Трампа

Приложение для заказа такси Lyft впервые обошло по числу скачиваний в США своего конкурента – Uber. Это произошло в результате кампании #DeleteUber, во время которой пользователи начали удалять свои аккаунты в сервисе. Об этом сообщает The Verge, ссылаясь на данные аналитической фирмы App Annie (AIN.UA).

28 января в Международном аэропорту имени Дж. Кеннеди проходили протесты против задержания беженцев. В это время сервис Uber отключил дополнительные коэффициенты на стоимость поездки в районе аэропорта.

Как отмечает издание Vox, много людей расценили этот шаг как попытку компании помешать протестам. В результате пользователи стали публиковать скриншоты, на которых они удаляют приложение, сопровождая их хэштегом #DeleteUber.

Представитель исследовательской фирмы App Annie рассказал The Verge, что в воскресение количество скачиваний приложения Lyft увеличилось вдвое по сравнению со средним показателем за последние две недели. Издание TechCrunch отмечает, к концу недели приложение поднялось с 39 на 7 место в категории бесплатных для iPhone. Издание Financial Times также приводит

данные аналитической фирмы Mobile Action, согласно которым по количеству скачиваний Lyft обогнал конкурента в понедельник.

Uber была одной из первых компаний, которая отреагировала на действия Д. Трампа, пообещав выдать компенсации пострадавшим водителям. Генеральный директор Т. Каланик, который является советником президента, пообещал поднять вопрос миграционной политики. Financial Times отмечает, что это не остановило пользователей поддерживать кампанию #DeleteUber.

В свою очередь, Lyft пожертвовал 1 млн долл. Американскому союзу защиты гражданских свобод и раскритиковал иммиграционный указ Д. Трампа. «Мы выступаем против подобных действий и не будем молчать, если что-то угрожает ценностям нашей компании», – заявили основатели сервиса.

***

2.02.2017

22 віджимання: Нацгвардійці у зоні АТО приєдналися до флешмобу

Бійці Слобожанської бригади (Харків), що виконує завдання у зоні проведення АТО, долучилися до флешмобу 22 Pushup Challenge (Espreso.tv).

До віджимання в рамках флешмобу приєдналися й бійці, які безпосередньо несуть службу на блокпостах і взводних опорних пунктах.

Естафету військовослужбовці 5-ї бригади передали своїм побратимам 3-ї оперативної бригади, яка також виконує бойові завдання на Донеччині.

***

8.02.2017

У крымских татар появилась собственная социальная сеть

Для общения крымских татар, оставшихся на оккупированном полуострове, с крымскими татарами, которые находятся на материке, создали специальную социальную сеть (Гордон).

У крымских татар появилась своя социальная сеть, задача которой – создать важную «в условиях роста дистанции между материком и Крымом» платформу для общения, обмена и реагирования, сообщила в Facebook первый заместитель министра информационной политики Украины Э. Джапарова.

Соцсеть находится по адресу: qirim.online.

«Часто слышу, что крымские татары в Крыму и на материке “говорят на разных языках”. Причин тому много, в том числе кампания российской пропаганды по дискредитации Украины и украинцев», – написала она.

Э. Джапарова сообщила, что сама она уже зарегистрировалась на «крымскотатарском Facebook».

На входе в крымскотатарскую соцсеть говорится, что Qırım.Online является «единственным в мире крымскотатарским сообществом,

объединившем в себе социальную сеть, новостной сайт, площадку для блогов и многое другое».

***

9.02.2017
Вчені розповіли про свою роботу за допомогою флешмобу

Вчені з усіх куточків світу публікують у Twitter фотографії з роботи, щоб розповісти про свою професію (Espreso.tv).

Вчені пишуть своє ім'я, додають фотографії на своєму робочому місці, описують свою професію і відзначають твіти хештегом.

Як виявилося, вчені – це не кабінетні працівники. Їм часто доводиться їздити в експедиції, працювати в полях. Наприклад, пірнати з аквалангом, вивчаючи життя океану, забиратися в найвіддаленіші ділянки планети, досліджуючи формування ландшафту, проводити археологічні розкопки для вивчення минулого, йти в дикі джунглі, спостерігаючи за тваринним світом.

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

2.02.2017
Количество пользователей Facebook в мире достигло 1,9 млрд

Количество пользователей социальной сети Facebook в мире достигло почти 1,9 млрд человек. Об этом на своей странице в соцсети написал основатель компании М. Цукерберг. Из них 1,2 млрд пользователей составляют активную ежедневную аудиторию. Количество бизнес-аккаунтов в сети составляет более 65 млн. По словам М. Цукерберга в дальнейшем компания планирует фокусироваться на видеосервисах (РБК-Україна).

***

1.02.2017
Facebook работает над созданием приложения для ТВ-приставок

Как отмечает Wall Street Journal, социальная сеть работает над приложением, где будут собраны все ТВ-программы и пользователи смогут перенести видеоконтент из сети на экраны телевизоров. WSJ отметили, что так как приложение на стадии разработки, компания не дает никаких подробных комментариев. Известно, что на данный момент Facebook ведет переговоры с различными медиа-холдингами, чтобы договориться о долгосрочных лицензиях: от сериалов до спортивно-развлекательных мероприятий. Компания

планирует занять большую часть рынка ТВ-рекламы и повысить доход за счет размещения рекламы в приложении. По информации издания, компания уже давно вынашивала идеи ТВ-приложения для потокового видео, но только летом прошлого года разработчики Facebook начали работу над ним (Marketing Media Review).

***

2.02.2017
Річний прибуток Facebook зріс більше ніж удвічі

Компанія Facebook відзвітувала про фінансові показники за минулий квартал і весь 2016 р.

Про це йдеться в звіті компанії (ESPRESO.TV).

Виручка Facebook за підсумками IV кварталу 2016 р. становила 8,81 млрд дол., що на 51 % більше порівняно з тим самим кварталом 2015 р. При цьому чистий прибуток компанії становить 3,57 млрд дол., що на 128 % більше, ніж прибуток Facebook у IV кварталі 2015 р.

За підсумками 2016 р. виручка компанії становить 27,64 млрд дол., а чистий прибуток – 10,22 млрд дол. Таким чином, порівняно з 2015 р., чистий прибуток Facebook збільшився на 177 %.

Крім того, середня кількість користувачів, які щодня заходили у соцмережу в грудні, становить 1,23 млрд осіб. Зростання порівняно з попереднім роком становить 18 %.

***

1.02.2017
Ольга Карпенко
В MailChimp добавили работу с рекламными кампаниями в Facebook

Популярный сервис управления почтовыми рассылками MailChimp на днях объявил об интеграции с рекламными кампаниями Facebook. Теперь пользователи сервиса смогут создавать такие кампании и управлять ими, не выходя из MailChimp. Можно таргетировать Facebook-кампании по существующей рассылке или по аудитории, схожей с базой рассылки, или же просто выбрать определенную аудиторию сети (AIN.UA).

В компании уверяют, что такой инструмент у разработчиков попросили сами пользователи. Сервис не зарабатывает на посредничестве: все платежи за такие кампании отправляются прямиком в Facebook.

«Бизнесы держат данные о пользователях, фото продуктов в MailChimp, так что это удачное место, чтобы начать рекламную кампанию для поиска новых клиентов. А поскольку пользователи могут синхронизировать данные своего бизнеса с MailChimp, мы можем рассказать им о ROI и о продажах, которые принесло рекламное объявление», – говорит Дж. Форман, вице-президент по продукту компании.

Пользователи сервиса считают, что решение – не особо революционное, но удобное. «Таргетировать свои рекламные активности на списки рассылки, если у вас есть email и/или мобильный телефон пользователя, бизнес-кабинет Facebook позволяет уже давно. Для этого вам нужно было выгрузить список из своей системы рассылок или CRM и загрузить его в рекламный кабинет Facebook – и вы получите все те же возможности, которые анонсировал MailChimp», – говорит Д. Маслов, директор по развитию бизнеса агентства Dievo.

По его словам, MailChimp просто упростил эту опцию, сделав ее доступной для большего числа клиентов. «Безусловно, это весьма удобно – запускать рассылки и рекламные кампании в одном окне и смотреть сводную аналитику по ним. Уверен, что у малого и среднего бизнеса это решение будет пользоваться большим спросом», – говорит он.

В. Галика из Engine Digital рассказывает, что его команда уже успела «пощупать» новую функцию. «Это очень удобно тем пользователям, для которых email-маркетинг является основным каналом, а Facebook – дополнительным. Ведь в кабинете MailChimp для Facebook-кампаний доступны все те же инструменты для кастомизации, что используются для рассылок. Удобна интеграция с покупками и сбор аналитики – статистики по Facebook и реакции на рассылки – в одном месте», – считает он.

Выходя за рамки email-маркетинга, компания заявляет о намерении стать «универсальной маркетинговой платформой» и говорит о том, что вскорости предложит пользователям и другие маркетинговые каналы. Так что MailChimp, похоже, придется менять название.

***

7.02.2017

Акционерам Facebook предложили сменить Цукерберга независимым человеком

Часть акционеров компании всемирной соцсети Facebook выступает за то, чтобы основатель компании М. Цукербега был устранен от управления компанией. Эту инициативу поддерживают инвесторы из правозащитной организации SumOfUs («Пресса Украины»).

Группа инвесторов интернет-сообщества SumOfUs убеждена, что для руководства компании следует избрать «независимого» человека.

«Марк Цукерберг – основатель Facebook. По нашему мнению, независимый человек лучше справится с ролью руководителя компании и сможет обеспечить нужный контроль за работниками организации, улучшить корпоративное управление и утвердить более четкий план относительно работы акционеров», – отметил один из инвесторов.

Кроме того, по словам членов SumOfUs, вступление в совет директоров независимого человека будет способствовать повышению стоимости акционерного капитала.

«Такой шаг возобновит необходимый баланс власти между CEO и советом директоров. Это также приведет к установлению эффективного руководства компании», – отметили инвесторы.

Следует подчеркнуть, члены SumOfUs обеспокоенности тем, что стоимость акций может существенно снизиться из-за того, что М. Цукерберг много рабочего времени находится вне стен компании Facebook.

Однако, невзирая на эти волнения, в прошлом году чистая прибыль компании выросла на 177 %.

***

8.02.2017

Реклама в мобильной сети Facebook оказалась эффективнее, чем в Google

Впервые Facebook обогнал Adwords на Android, согласно аналитической компании Singular, которая проранжировала рекламные сети для iOS и Android в зависимости от показателя ROI, отмечает adindex.ru. Топ самых эффективных сетей во второй половине 2016 г. возглавил мобильный Facebook, показав более высокий ROI по сравнению с Google. В Mobile ROI Index используются показатели конверсии и данные о расходах, собранные анонимно из 1500 приложений и 1000 рекламных сетей. Исследование ставит своей целью обеспечить максимальную прозрачность рынка мобильной рекламы и выделить рекламные сети, продвижение с помощью которых приносит больше доходов при минимальных затратах (Marketing Media Review).

Система AdWords – третья по величине рекламная сеть по размеру расходов на рекламу на iOS, однако она недостаточно эффективна по сравнению с 18-ю другими сетями, в том числе такими небольшими, как Fyber, Mobvista и CrossInstall, говорится в исследовании. При этом стоимость размещения рекламы в AdWords сопоставима с ценами в других ведущих сетях. Кроме того, хотя пользователи на Android в 1,65 раз «дешевле», чем пользователи на iOS, реклама на устройствах Apple показывает в 1,3 большую рентабельность. Это значит, что за каждый доллар, потраченный на «покупку» пользователя iOS, маркетолог получит в 1,3 раза больше прибыли, чем с Android-пользователя, отмечают в Singular.

В топ пять самых эффективных рекламных сетей для iOS также вошли AdColony, Vungle, Unity Ads и AppLovin, для Android – AppLovin, AdColony и AdAction. Самым быстрорастущими сетями названы Fyber, Motive Interactive и Mobvista.

***

10.02.2017

«ВКонтакте» начинает работу с благотворительными организациями

Руководство популярной социальной сети «ВКонтакте» объявил об открытии нового направления в работе, которое поможет продвигать благотворительность среди пользователей. Информация об этом была предоставлена сотрудниками пресс-службы ресурса (Grifonsoft.ru).

В сообщении говорится, что это направление также необходимо для объединения представителей некоммерческого сервиса на полях «ВКонтакте». Уточняется, что все желающие представители благотворительных организация смогут принять участие в этой программе. Другие для них подготовят лекции и тестовые задания.

Для волонтеров компания «ВКонтакте» создала карту благотворительных фондов, с которыми соцсеть взаимодействует на постоянной основе.

***

13.02.2017

Facebook предоставил новые варианты для покупки видеорекламы

Социальная сеть предложит рекламодателям три новых варианта покупки видеорекламы в самой соцсети, Instagram и Audience Network: completed view buying (покупка полного просмотра), two-second buying (покупка двухсекундного просмотра) и sound-on buying (покупка со звуковым сопровождением), отмечает adindex.ru. Что касается покупки полного просмотра, то рекламодатели будут платить только за те ролики, которые были полностью просмотрены, в течение любого времени до десяти секунд. Покупка двухсекундного просмотра подразумевает оплату только в случае, когда на экране видны по крайней мере 50 % пикселей видеорекламы на протяжении двух последовательных секунд и более. Покупка со звуковым сопровождением означает, что рекламодатели смогут оговаривать возможность оплаты за просмотры видеорекламы с включенным звуком. Также в следующем месяце Facebook предоставит рекламодателям больше данных по просмотрам (impression level data), сообщили в соцсети. С сентября 2016 г. соцсеть несколько раз признавалась в том, что в метриках компании присутствовали ошибки. На ошибочные показатели опирались рекламодатели при планировании или оценке своих кампаній (Marketing Media Review).

***

10.02.2017

Социальные сети оказывают влияние на 46 % потребителей

В ходе исследования Science of Social Video было обнаружено, что пользователи тратят шесть часов в неделю на просмотр видеоконтента в социальных сетях. 67 % респондентов из 5500 опрошенных отметили, что это количество времени выросло за последний год. Исследование также проанализировало, как видео в сетях влияет на покупательские решения. 46 %

отметили, что совершили покупку под влиянием видео от бренда в сетях, а 32 % респондентов только подумали о покупке (Marketing Media Review).

***

8.02.2017

В Украине появился официальный представитель соцсети «Одноклассники»

К. Косоноцкий, ранее руководивший отделом таргетированной рекламы в социальных сетях в украинском sales house T-Sell, будет отвечать за развитие бизнеса проекта, работу с рекламными агентствами, прямыми рекламодателями и партнерами в Украине, а также представлять интересы социальной сети в стране, отмечает sostav.ua. «Украина – вторая страна по количеству пользователей в “Одноклассниках”. Мы планируем динамично развивать присутствие в Украине и давать больше информации о работе социальной сети как для пользователей, представителей бизнеса, так и для рекламодателей», – говорит С. Боярский, менеджер по развитию бизнеса проекта Одноклассники (Marketing Media Review).

***

10.02.2017

Facebook запустит собственное телешоу

М. Цукерберг сообщил, что компания начнет эксперимент по производству коротких эпизодических видео (Экономические известия).

Социальная сеть Facebook начнет производство видеоконтента для пользователей и запустит собственное телешоу.

Для работы над проектом шоу руководство Facebook наняло М. Лефевр. Ранее она курировала на MTV работу с программами, которые снимали по собственным сценариям. В проекте Facebook она займется работой над сценариями для видеороликов. М. Лефевр будет работать вместе с основателем проекта CollegeHumor.

***

8.02.2017

Евгения Чирок

YouTube позволит блогерам зарабатывать на видео со смартфонов

Представители видеохостинга YouTube заявили о возможности зарабатывать на видеотрансляциях со смартфона. Эта услуга будет доступна для блогеров с десятью тысячами подписчиков (HiTech-News.ru).

На YouTube проявилась информация о том, что видеохостинг в ближайшее время запустит новую функцию Super Chat. Она будет включать в себя платные видеотрансляции ведущих блогеров, чьи подписки превышают

более десяти тысяч. В ленте они будут отображаться определенным цветом, что отличит их от бесплатных роликов. Таким образом, блогеры смогут зарабатывать на отснятых видео.

Опубликован список из 20 стран, в которых будет протестирован Super Chat – России в нем нет. Пока также не известна стоимость за видеоролик.

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

13.02.2017

Батьків попереджають про нелюдів, які через соцмережі втягують дітей у смертельні ігри

Українців попереджають про небезпеку. Так, у соціальних мережах у групах закликають дітей до вчинення самогубства. Суїцидальні спільноти називаються «Море китів», «Тихий дім», «Розбуди мене о 04:20», «F57». Назви груп можуть містити назви з інших слів або «набір букв», тому вартує звернути увагу на аватарки груп із китами, порізаними руками, свастикою, депресивними підлітками. При виявленні таких груп варто негайно повідомляти до кіберполіції, наголошує координатор групи «Варта 1» О. Чобіт (InternetUA).

У таких групах діє долучення до гри по заявці або напису спеціальних слів на сторінках (тоді куратори самі додаються до дитини).

Куратору, особі, яка вестиме дитину до самогубства дитина має скинути повне ПІБ та номер мобільного телефону. Опісля, дитині даються завдання, їх є від 13 до 50. Спочатку йде перевірка на фейковість – дитина надсилає своє селфі з певним написом на аркуші куратору. Опісля вже завдання, які несуть загрозу дитині, наприклад поріз руки (може бути одиночний поріз або поріз у вигляді кита). Усі завдання потрібно виконувати строго у вказаний час і надсилати фото чи відеозвіт.

На своїй сторінці дитина у статусі прописує зворотній відлік, наприклад 5/50. Також, змінюється тематика публікацій, постять про смерть і китів. У друзях дитини з’являються невідомі люди, котрі мають у даних похідні від слова кит або аватарки з зображенням китів.

Фінальним завдання є самогубство. У приватних повідомленнях дитину перевіряють на готовність вчинити самогубство. Після підтвердження, створюють аудіозапис з скаргами дитини на життя і переконують, що єдиний

вихід з ситуації – самогубство. Тоді, дитині вказують, як саме вчинити самогубство та учасники групи знімають момент загибелі на відео, щоб розмістити підтвердження смерті у соціальних мережах.

При відмові дитині погрожують у соціальних мережах смертю батьків і вбивством самої дитини. Також погрожують за допомогою телефону, який завчасно питають при вступі у групу. Тому, зверніть увагу з ким спілкується дитина по телефону та зміни у розмовах, наприклад дитина виходить з кімнати, щоб поспілкуватися по телефону.

Вступаючи у гру, дитина дуже змінює свою поведінку:

1. Безпричинна зміна поведінки. Був спокійним – став нервовим або навпаки стають надто ввічливими.

2. Порушення сну: сонливість або безсоння, так як завдання часто видаються дитині вночі.

3. Дитина стає замкнутою, куратори груп забороняють комусь розповідати про гру та налаштовують дитину проти батьків.

4. Зневажливе ставлення до своєї зовнішності у підлітків, які раніше не були в цьому помічені: перестають вмиватися, чистити зуби, одягаються неохайно.

5. Дії, які можна трактувати, як прощання: спроби закінчити всі справи, раздарювання улюблених речей друзям.

При виявленні таких груп громадян просять негайно повідомляти до кіберполіції (https://www.cybercrime.gov.ua – цілодобово), телефон гарячої лінії (044) 374-37-21 (з 8:45 до 19:30 в робочі дні) або звертатися до адміністрації соцмережі, у якій було виявлено группу.

Кіберполіція виявила одну з таких групп – https://vk.com/blueskitea. До неї входили 209 користувачів з України. При цьому слід наголосити, що такі групи щодня блокуються адміністрацією соціальних мереж за зверненнями правоохоронних органів або їх користувачів. Аналізуючи діяльність зазначених груп, кіберполіція встановила постійних учасників таких спільнот, які реєструються з території України.

У зв’язку з цим кіберполіція звертається до батьків та всіх не байдужих із проханням бути пильними, при можливості – перевірити облікові записи ваших дітей, чи не зареєстровані вони під зазначеними у списку іменами. При виявлені додаткових облікових записів Департамент кіберполіції інформуватиме шляхом оновлення цього списку.

***

7.02.2017

Як соцмережі насправді впливають на самооцінку

Психологи розповіли, як через соцмережі можна визначити, яке у користувачів психічне та фізичне здоров’я (Радіо24).

Відповідно до досліджень, соціальні мережі негативно впливають на моральний стан людей, особливо під час депресії та стресів. Спеціалісти

відзначають, що довге перебування у віртуальному світі може не просто знизити самооцінку, а й призвести до психічних розладів.

Виявилося, що серед 5 тисяч осіб віком у середньому у 48 років, користувачі із поганим фізичним здоров'ям частіше ставили «Подобається». А от люди із погіршеним психічним здоров'ям частіше оновлювали статуси, фото, стіну на сторінці.

До слова, фахівців здивувало те, що користувачі, які ділилися історіями свого кохання, мали міцніші стосунки. А от тривалі почуття були у тих, хто приховував свій сімейний стан.

***

14.02.2017
Facebook став машиною часу

Під час експерименту психологи з Кентського університету Великобританії з'ясували, що користувачі Facebook страждають порушенням сприйняття часу (Факти). Про це повідомляє Science Daily.

Учасникам експерименту були показані п'ять зображень, які асоціювалися з Facebook, і п'ять картинок з нейтральними інтернет-асоціаціями.

Також їм запропонували оцінити час, витрачений на їх перегляд.

Виявилося, що більшість людей неправильно його оцінили.

Варто зазначити, що контрольні зображення не викликали спотворення сприйняття часу.

Нагадаємо, є безліч причин відмовитися від використання соціальних мереж.

Маніпулятивні технології

1.02.2017
Олег Прошкин
Россия искусно использует социальные сети, чтобы разделять Запад

«Россия искусно использует социальные сети, чтобы разделять Запад и увеличить влияние Москвы в Европе, США и в последнее время в Азии, – сообщает К. Заппоне в The Age. – Использование социальных сетей как платформы для разделения демократий работает отчасти потому, что эта стратегия базируется на основательном слепом пятне открытых сообществ: происхождении и громкости голосов, принимающих участие в сетевой дискуссии» (24news.com.ua).

«Западные страны, изобретатели интернета и социальных сетей, таких как Facebook и Twitter, склонны воспринимать дискуссию в социальных сетях как открытое отражение взглядов общества, – говорится в статье. – Сама эта

открытость означает, что в дебаты могут вмешиваться голоса извне – не с целью расширить дискуссию, а чтобы кооптировать аргументы и с их помощью вывести заключения, подрывающие западные общества и правительства».

«Пропаганда может кристаллизоваться до хэштегов, и смыслы могут искажаться с целью затуманить понимание предмета или испортить репутацию идей, партий или деятелей, – указывает автор. – В этом мире противоположность свободной торговли – не протекционизм, а "антиглобализм". Либералы – "неолибералы". Голосование за Трампа позволит "избежать войны с Россией". Хиллари становится "Killary" (от английского "kill" – убивать. – Прим. ред.). Эта пропаганда склоняется к крайностям, стремясь разъесть более широкую центральную область согласия, необходимого для функционирования либеральных демократий, где бы они ни находились, включая Азиатско-Тихоокеанский регион».

«Скорость распространения и проникающая способность пропаганды в социальных сетях может доводить пользователей до эффекта 360 градусов, когда воспринимаемое ими кажется не связным идеологическим посланием, а естественным и нарастающим консенсусом толпы», – полагает К. Заппоне.

«В социальных сетях используются боты (сокращение от "роботы") – программки для автоматизации размещения публикаций или ответов на сообщения. В последние годы в ходе политических кампаний применялись боты, но не всегда это приводило к желаемому эффекту, – говорится в статье. – Влияние взаимодействия между ботами и людьми не всегда ясно, по словам [директора по исследованиям проекта «Пропаганда» Оксфордского института интернета] С. Вули. Однако понятно, что боты могут применяться для превращения ключевых слов в тренды. Это огромная задняя дверь, сквозь которую в западные СМИ могут прийти внешние силы. В Facebook, Google и Twitter алгоритмы формирования трендов довольно сильно зависят от чисел, утверждает С. Вули, «и боты массово разгоняют эти алгоритмы».

«В то же время фокус российской пропаганды сместился, по сравнению с советскими временами, когда она превозносила материальный успех коммунизма и критиковала западный декаданс», – говорится в статье. Сегодняшняя российская пропаганда «очень адаптивна и не сводится ни к какой идеологической системе», как выразилась старший редактор журнала Intersection Project О. Ирисова в интервью Fairfax Media. Это справедливо для всего множества голосов, которые разносят эту пропаганду, в том числе поддерживаемых государством телевещателей, вроде Sputnik и RT, гордящихся тем, что они предлагают «альтернативы» традиционным СМИ. Это существенное изменение, по сравнению с холодной войной».

«Если во время холодной войны было более-менее ясно, какие сюжеты будет продвигать советская пропаганда, заряженная коммунистической идеологией (капитализм против коммунизма как альтернативной модели развития; истории о том, как плохо живется людям в капиталистических странах и как хорошо советское государство заботится о своем народе), нынешняя кремлевская пропаганда может продвигать почти любой сюжет,

способный подорвать веру людей в либеральный образ жизни», – сказала О. Ирисова.

По ее словам, «для левых у Кремля одно послание, для правых – другое».

«Почему Россия делает это? Потому что при президенте В. Путине эта страна начала пытаться вернуть себе былую славу, которую, по ощущению многих ее граждан, у нее отобрали после развала Советского Союза, – утверждает К. Заппоне. – Эта кибервойна использует сильные стороны российского общества – уверенное владение компьютером и иностранными языками, процветающая интернет-культура и знание Запада».

«Сколько бы мы ни говорили о “фальшивых новостях”, в случае России наибольший риск проистекает из того, что точнее можно назвать “полуфальшивыми новостями”», – указывает автор.

«Важно понимать, что полностью выдуманные истории встречаются довольно редко, – сказала О. Ирисова. – Большинство прокремлевских СМИ берут настоящие новости или события, однако с помощью эмоционального стиля и подходящих к случаю «экспертов» искажают их так, чтобы Запад или либералы выглядели «плохими парнями».

***

7.02.2017

«Чорний список» пропагандистських ЗМІ РФ оприлюднили у Естонії

Центру Propastop, який підпорядковується Центру кіберзахисту Естонії, опублікував перелік російських ЗМІ, які займаються путінською пропагандою та становлять загрозу національній безпеці Естонії (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це інформує MediaSapiens.

У «чорному списку» опинились 28 сайтів серед яких Sputnik, Russia Today, інформаційне агентство ТАСС, «Российская газета», сайт телерадіокомпанії «Звезда», сайт «Вести.ру», сайт телеканалу «НТВ», сайт «Ридус», Lenta.ru та ін.

Разом з тим Propastop закликає естонських підприємців не співпрацювати із тими ЗМІ, які потрапили до оприлюдненого списку.

***

7.02.2017

У США створять центр для ведення інформаційної війни проти Росії, – ЗМІ

Центр стежитиме за пропагандистськими кампаніями за кордоном, аналізуватиме їх та протистоятиме фейкам (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

Про це повідомляє The Daily Beast.

Видання повідомляє, що відкриття центру очікується вже в цьому році. На його роботу буде виділено 160 млн дол.

Зазначається, що на думку ініціаторів, створення міжвідомчого Центру глобальної взаємодії (GEC) для боротьби з пропагандою і фейковими новинами, сенаторів Р. Портман та К. Мерфі, орган допоможе захистити інтереси США та союзників.

«Ця установа допоможе захистити наші інтереси й інтереси наших союзників ... за рахунок прямої протидії неправді та недостовірності в ЗМІ», – зазначив сенатор Р. Портман. Американські ЗМІ зазначаються, що Центр стежитиме за пропагандистськими кампаніями за кордоном, аналізуватиме та протистоятиме їм.

Центр також виділятиме гранти для зарубіжних журналістів, приватних компаній і громадських організацій, таких як Bellingcat або StopFake.org, які надають достовірну інформацію, а також протидіють неправдивій російській пропаганді в Україні.

***

14.02.2017
Георгій Почепцов
Пропаганда и социальные сети

Социальные сети изменили многие параметры человеческой жизни, что с неизбежностью должно было отразиться и на пропаганде. Новые технологи каждый раз существенно влияют на социосистемы. Например, СССР не смог бы сделать свою индустриализацию, не опираясь на новые медиа типа радио и кино, поскольку без них он не справился бы с созданием массовой рабочей профессии (PRportal).

Кстати, Англия времени промышленной революции привлекла к этой трансформации крестьянина в рабочего и другие средства. Это был чай, который помог новому рабочему не засыпать у станка, а также джин, который снимал напряжение в послерабочее время.

Кино же помогло становлению диктаторов XX века – Гитлера и Сталина. Это было воздействие нового типа, которое помогло создать культ личности в считанные сроки, на что в прошлом уходили столетия воспитания поклонения к первым лцам.

Сегодня социальные сети стали формировать новых лидеров, примером чего стали выборы Д. Трампа. Социальные медиа создают иллюзию доступности говорения для всех. Хотя разнообразия мнений как раз услышать нельзя, поскольку алгоритмы Facebook создают эхо-камеры, где потребитель получает сообщения от близких ему по взглядам людей.

В этом плане феномен комментариев также ничего не меняет. Высказавшему какое-то мнение начинают возражать в комментариях люди с

совершенно противоположными взглядами, но, как известно, в результате таких жарких дискуссий люди только укрепляются в своем мнении, ни в коем случае не меняя его.

Много также писалось о роли фейков в этой кампании, вносящих сумятицу в массовое сознание. Вот целый набор статей из Newsweek, за ними стоят тексты ученых, на которые они опираются, по поводу роли фейковых новостей в современных информационных потоках [см. тут, тут и тут]. Кстати, сегодня считается, что Ф. Кастро подняли на роль латиноамериканского Робин Гуда именно фейковые новости.

Правда, постизбирательные исследования утверждают, что фейки все же не повлияли на результат. С другой стороны, Pew Research Center акцентирует, что двое из трех граждан США (64 %) считают, что сфабрикованные новости привносили путаницу в понимание текущих вопросов и событий.

Это принципиально новая сфера, которая проявила себя в рамках выборов 2016 г. в Америке в достаточно большом объеме. Исследователи отмечают следующее: «Во время президентских выборов 2016 г. фокус сместился в сторону социальных медиа. Социальные медиаплатформы типа Facebook имеют принципиально иную структуру, чем любая медиатехнология прошлого. Контент может попадать пользователям без существенного фильтра третьего участника, без проверки фактов, без редакторской оценки, а индивидуальный пользователь без истории или репутации может в некоторых случаях достигать такого же количества читателей как Fox News, CNN или New York Times».

Почти каждая европейская страна создала сегодня структуры, призванные бороться с фейковым потоком, в первую очередь из России. Швеция, например, доказала связь между информационными вбросами и активными мероприятиями России. То есть все эти действия носят не случайный, а вполне системный характер. Они изучили метанарративы, продемонстрировали, как внимание к Украине упало, когда появилась Сирия.

Исследователи также пишут: «Как и советская пропаганда, сегодняшняя российская публичная дипломатия может быть совершенно непоследовательной. Запад подается как слабый, в то же время представляя из себя угрозу существования России. Европа обладает ксенофобией к беженцам, но глупо разрешает им искать убежище. Но сутью является отнюдь не дать целевым аудиториям последовательный альтернативный нарратив. Такой инструментарий, как “Спутник”, может также служить цели распространять путаницу и поощрять разобщенность. Более того, “Спутник” на шведском опирается за некоторыми исключениями на переписывании уже существующих новостных историй из признанных медиаисточников. Возникает парадокс между обычными обвинениями западных медиа в предвзятости и антироссийскости в своей ориентации с реальным использованием тех же западных медиа как источника публикаций “Спутника”».

Интересно под этим углом зрения посмотреть на Украину, которая постоянно подвергается «обстрелу» фейковой информации со стороны России,

что позволило заполнять доказательством «фейковости» целые сайты, например, наиболее известный StopFake (www.stopfake.org). StopFake печатает статьи о распознании фейков.

Социологи создали индекс результативности российской пропаганды, который задается как распространенность поддержки главных тезисов российской пропаганды населением. Здесь можно увидеть, что наибольшее воздействие российской пропаганды наблюдается в Харьковской, Одесской областях и на Донбассе, наименьшее – на западе и в центре Украины. Интересно, что эти данные коррелируют с расекреченными сегодня данными ЦРУ от 1957 г. по степени недовольства режимом регионов Украины. Крым и Донбасс называются максимально лояльными советской власти. Справедливости ради следует отметить, что и Россия также отслеживает искажения в украинской пропаганде. В результате российское население четко удерживает свои стереотипы по отношению к Украине, что можно увидеть в дискуссии Д. Быкова и А. Мироновой. Все это, видимо, и позволяет А. Невзорову говорить, что реальная поддержка В. Путина, вероятно, даже не 86 %, а все 96 %.

Перед нами определенное упрощение ситуации коммуникации, как с точки зрения передаваемого контента, так и с точки зрения массового сознания, которое благодаря социальным медиа стала откатываться назад. Следует вспомнить также феномен развлекательности, который охватил не только массовую культуру, но и новостные потоки. Инфотейнтмент становится определяющим качеством этого потока. Третьим фактором, формирующим сегодняшний информационный поток, стало преобладание визуальности, которое постепенно трансформирует культуру чтения, когда два тома «Войны и мира» становятся недоступными даже для специалистов. Все это проявляется еще сильнее, когда в дело вступают дезинформационные, а не только информационные цели. Специалисты ЕС приходят к выводу, что дезинформационная кампания является невоенным средством достижения политических целей (см. тут и тут). Цель такой дезинформационной кампании они видят в ослаблении и дестабилизации Запада со стороны России.

Причем к этим рассуждением следует добавить еще один фактор. Если победа, как и атака, с помощью военных методов видна сразу, то в информационной сфере результаты могут проявляться гораздо позже. Именно поэтому и возникают термины типа стратегических коммуникаций или операций влияния, призванные подчеркнуть отдаленный тип последствий.

***

9.02.2017

В Facebook массово появились однотипные посты в защиту министра Кутового

В социальной сети Facebook в последнее время было размещено сразу несколько однотипных сообщений с поддержкой действий министра Аграрной

политики и продовольствия Т. Кутового, пишет Комсомольская правда в Украине (Mignews.com.ua).

Посты вышли у так называемых ЛОМов – лидеров мнений, ранее не замеченных в интересе к аграрному рынку.

В написанных как под копирку сообщениях отмечается, что глава МинАПК Т. Кутовой, якобы, начал полномасштабные реформы, способные остановить коррупцию в спиртовой отрасли и обезопасить простых потребителей от суррогатного спирта.

Блогеры уверяют своих читателей, что новое руководство государственной компании «Укрспирт», находящейся в ведении МинАПК, закрывает нелегальные каналы распространения спирта и разрушает многолетние теневые схемы.

Также читателей призывают поддержать борьбу министра с некими неназванными «нечистым на руку олигархами», которые, якобы, всячески противятся реформам министерства.

Такие посты появились у провластных блогеров М. Олешко, Я. Матюшина, паблике «Я-Патриот» и даже региональном паблике «Жить в Харькове», что может свидетельствовать о проплаченной информационной компании, заказчиком которой может быть сам министр или кто-то из руководства концерна «Укрспирт».

Во всех случаях пользователям Facebook предлагается ознакомиться с сюжетом, который вышел на «5 канале» в формате независимого расследования ситуации в спиртовой отрасли, снятым в рамках проекта «Стоп Коррупции».

Координатором проекта «Стоп коррупции» является журналист Р. Бочкала, который ранее был замечен в публичной поддержке бизнесмена Л. Парцхаладзе. В частности, он фактически обеспечивал Л. Парцхаладзе информационную поддержку во время работы последнего на посту заместителя главы Киевской ОГА, а также сотрудничал с ним в рамках других проектов.

Нынешний глава АПК Т. Кутовой считается человеком, близким к Парцхаладзе. С 2004 по 2009 г. он работал финансовым директором принадлежащей последнему компании ЗАО «Инвестиционная компания XXI век».

Подобный конфликт интересов ставит под сомнение объективность материала «5 канала», который теперь продвигается в Facebook с помощью известных блогеров.

Спецслужби і технології «соціального контролю»

1.02.2017

Свободівці викрили фейкові сторінки у соцмережі, «підконтрольній ФСБ»

У мерії Конотопа стурбовані великою кількістю фейкових сторінок, які створюють на ім’я відомих посадових осіб. Чиновники запевняють, що повідомлення, які розсилають ці фейки, та їх пости, що розміщують у популярних пабліках, покликані на те, щоб підірвати репутацію посадовців (Сумські Дебати).

У «Типовому мері Конотопа» «ВКонтакте» та у Facebook пишуть:

«Офіційно:

Міський голова Конотопа А. Семеніхін, голова фракції ВО “Свобода” в Сумській облраді М. Биркун, керуючий справами виконкому Конотопської міськради В. Яроцький не мають сторінок у соцмережі, яка контролюється ФСБ РФ, “ВКонтакте”. Усі дописи, які робляться від імені вищезгаданих посадовців у цій соцмережі є фейковими».

***

1.02.2017

WikiLeaks нагадав про тисячі документів, пов’язаних з Фійоном і Марін Ле Пен

Електронний ресурс WikiLeaks нагадав про те, що має тисячі документів, пов’язаних із кандидатами в президенти Франції Ф. Фійоном і М. Ле Пен. Про це йдеться у Twitter WikiLeaks (LB.ua).

Згідно з цими повідомленнями, близько 3,5 тис. документів стосуються Ф. Фійона, ще близько тисячі – М. Ле Пен.

Зазначимо, що документи щодо Ле Пен датуються 2011–2013 рр., стосовно Ф. Фійона – 2005–2011 рр.

29 січня французьке видання Mediapart опублікувало матеріал, що компрометує Ф. Фійона, – у ньому йшлося, що кандидат у президенти міг бути причетним до розкрадання бюджетних грошей під час роботи в Сенаті.

За день до цього французькі ЗМІ опублікували інформацію про те, що Фійон під час роботи в Сенаті також найняв як асистента свою дружину Пенелопу. Вона провела на цій посаді вісім років і отримала загалом 500 тис. євро. Однак, за даними ЗМІ, на роботі Пенелопа Ф. Фійон не з’являлася. Після публікації цієї інформації понад 100 тис. французів підписали петицію із закликом до дружини Фіойна повернути отримані гроші в бюджет. Напередодні в парламенті Франції почалися обшуки у справі дружини Фійона.

***

5.02.2017

У США агент Секретної служби попадає під слідство через антипатії до Трампа

Високопоставлений агент Секретної служби США К. О’Грейді, яка донедавна очолювала округ у Денвері, відсторонена від виконання обов’язків за пост про Д. Трампа у Facebook (LB.ua).

Про це повідомляє телеканал CBS News.

«Спеціальний агент Секретної служби, яка відповідає за округ у Денвері, відсторонена від виконання обов'язків, проти неї порушено слідство через повідомлення у соціальних медіа, де вона зазначила, що не піде під кулі за президента Д. Трампа», – йдеться у повідомленні.

За повідомленнями місцевих ЗМІ, К. О'Грейді була відсторонена зі збереженням оплати.

Агент зробила це повідомлення ще у жовтні, до того, як було оголошено переможця виборів президента США. У своєму пості на Facebook О'Грейді висловила своє ставлення до кандидата у президенти від Республіканської партії і заявила про підтримку іншого кандидата – Г. Клінтон.

Як уточнює телеканал, К. О'Грейді – голова офісу у Денвері, але може не зберегти цю посаду після того, як розслідування щодо її запису завершиться.

***

5.02.2017

Суд обязал Google передавать властям США письма с иностранных серверов

Американский суд обязал компанию Google предоставлять властям США электронные письма ее клиентов, которые хранятся на зарубежных серверах. Об этом 4 февраля сообщает Reuters (InternetUA).

Как отмечается, судья штата Филадельфия Т. Рутер принял это решение, чтобы агенты Федерального бюро расследований (ФБР) могли проводить внутри США следствия, связанные с мошенничеством.

«Получение сведений с многочисленных серверов Google за рубежом может восприниматься как вторжение в частную жизнь, однако на самом деле фактическое нарушение неприкосновенности происходит только в случае раскрытия информации в Соединенных Штатах», – говорится в постановлении судьи.

В Google заявили, что намерены обжаловать решение судьи.

22 декабря 2016 г. сотрудник Google подал иск к корпорации, поскольку считает незаконной слежку за работниками. По его мнению, политика конфиденциальности компании не соответствует трудовому законодательству штата Калифорния. В иске сказано, что в Google существует шпионская программа, которая якобы предназначена для предотвращения передачи потенциально компрометирующих данных в прессу и государственным органам.

***

7.02.2017

Китай еще больше ужесточит контроль за Интернетом

Китайские власти займутся ужесточением контроля Интернета, создав новую Комиссию по координации онлайн-сервисов и компьютерного оборудования. Об этом сообщает Reuters (InternetUA).

В ноябре 2016 г. Китай принял неоднозначный закон о кибербезопасности с целью противодействия террористам и хакерам, который затронул правозащитные организации и иностранные компании. Теперь власти планируют ввести новый орган, который будет изучать угрозы для информационной безопасности страны и своевременно сообщать о них правительству.

***

9.02.2017

Amnesty: влада Казахстану «придушує» свободу слова у соцмережах

Влада Казахстану використовує «дедалі більш витончені й агресивні методи, щоб викорінити» інакомислення в Інтернеті і соціальних медіа.

Про це заявляє правозахисна організація Amnesty International.

Зокрема, у доповіді правозахисники стверджують, що влада Казахстану використовує недавно ухвалені закони для обмеження або блокування доступу до різних сайтів.

Як заявляють правозахисники, уряд президента Н. Назарбаєва також використовує судові рішення у кримінальних й адміністративних справах, щоб переслідувати людей «за реалізацію права на свободу слова і мирні збори».

У доповіді наводяться справи правозахисників М. Бокаєва і Т. Аяна, затриманих у травні 2016 р. після публікації інформації про антиурядові протести проти змін до Земельного кодексу Казахстану.

Обидва були засуджені до п’яти років тюремного ув’язнення кожен після того, як суд визнав їх винними в розпалюванні соціальної ворожнечі, поширенні завідомо неправдивої інформації, а також порушенні закону, що регулює суспільні збори.

Amnesty International визнало правозахисників в’язнями сумління.

***

13.02.2017

СБУ сообщила об активной борьбе с сепаратистами в соцсетях

Сотрудники Службы безопасности Украины продолжают бороться с антиукраинской пропагандой в Интернете. За последнее время было открыто 30 уголовных дела против администраторов сепаратистских сообществ в социальных сетях. Кроме того, 17 правонарушителям сообщили о подозрении в запрещенной деятельности, а также было направлено в суд 13 обвинительных приговоров.

Об этом сообщили в пресс-центре СБУ. Новость передает «Пресса Украины».

На сегодня в социальных сетях есть очень много сообществ и сайтов, в которых сепаратисты распространяют призывы о массовых беспорядках среди украинского народа, о свержении конституционного строя и других преступных действиях.

Служба безопасности Украины направила все силы для эффективной борьбы с правонарушителями. В частности, судами разных инстанций было вынесено приговоры 13 лицам за противоправные действия в Интернете.

«Администраторы призывали подписчиков сообществ к насильственному изменению и свержению конституционного строя Украины, а также к увлечению государственной власти», – говорится в сообщении.

Как отметили в СБУ, уголовную ответственность будут нести также люди, которые создавали террористические группы или организации и посягали на неприкосновенность и территориальную целостность государства.

***

1.02.2017

СБУ затримала у Дніпрі адміністратора сепаратистських груп у соцмережах

Мешканця Дніпра, який вів активну антиукраїнську пропаганду в соціальних мережах, затримала Служба безпеки України (Дніпроград).

У 2014 р. 27-річний працівник філії російської ІТ-компанії через Інтернет познайомився з терористами «ДНР/ЛНР», які воюють проти України на Сході держави.

Виконуючи завдання бойовиків, зловмисник створив та адміністрував групи у соціальних мереж, де розповсюджував матеріали спрямовані на дискредитацію державної влади в Україні, розпалювання міжнаціональної ворожнечі, входження південно-східних областей України до складу Росії.

Також поплічник терористів збирав і передавав подільникам дані про суспільно-політичну та соціальну ситуацію в Дніпропетровській області.

Під час обшуку співробітники спецслужби вилучили у затриманого комп’ютерну техніку із доказами протиправної діяльності.

Відкрито кримінальне провадження за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України.

Тривають слідчі дії.

***

2.02.2017

У Львові жінка через соцмережі допомагала сепаратистам

Співробітники Служби безпеки України викрили у Львові адміністратора проросійських спільнот у соцмережах (Західна інформаційна корпорація).

Про це повідомляє прес-центр СБУ.

Зловмисниця створила фейкові акаунти та адмініструвала групи антиукраїнської спрямованості, де розповсюджувались матеріали, що дискредитують Українську державу, пропагують створення т. зв. «Новоросії».

Крім того, жінка організовувала збір фінансової допомоги бойовикам т. зв. «ДНР/ЛНР».

Також поплічниця сепаратистів збирала та передавала російським модераторам дані про суспільно-політичну та соціальну ситуацію на Львівщині, займалася блокуванням проукраїнських спільнот і користувачів у російських соцмережах.

Під час обшуків співробітники спецслужби вилучили комп'ютерну техніку із доказами її протиправної діяльності.

Відкрито кримінальне провадження за ч. 1 ст. 110 (посягання на територіальну цілісність і недоторканість України) Кримінального кодексу України. Тривають оперативно-слідчі дії.

***

6.02.2017
Базиленко Анна
В Ужгороді затримали адміна сепаратистських груп у «ВКонтакте»

Служба безпеки України викрила в Ужгороді адміністратора проросійських груп у соцмережі «ВКонтакте». Зловмисник створив фейкові акаунти в соцмережі та адміністрував спільноти, де поширював антиукраїнські матеріали, дискредитував владу та пропагував військову агресію РФ на Сході України (Watcher).

Під час обшуку оперативники вилучили у затриманого комп'ютерну техніку. Відкрито кримінальне провадження за ч. 2 ст. 109 (розповсюдження матеріалів із закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади) Кримінального кодексу України. Досудове розслідування триває.

***

6.02.2017
Двое жителей Славянска проведут пять лет в тюрьме за антиукраинские призывы в соцсетях

Молодые люди 1993 и 1994 г. р. вели в социальной сети «Вконтакте» несколько групп антиукраинского характера (InternetUA).

Во время судебных слушаний было установлено, что в феврале 2014 г. жители Славянского района создали группы в социальной сети. Здесь, поддерживая террористов, молодые люди размещали посты антиукраинского характера и агитировали к изменению территориальной целостности Украины.

В апреле 2015 г. сотрудниками Службы безопасности Украины преступная деятельность злоумышленников была приостановлена.

По ходатайству прокуратуры фигуранты дела были арестованы.

Несмотря на то, что своей вины молодые люди в суде не признали, государственным обвинением, которое поддерживала прокуратура Донецкой области, полностью доказана их вина в совершенном преступлении.

Благодаря принципиальной позиции прокуратуры, оба сторонника «русского мира» приговорены к пяти годам лишения свободы.

***

7.02.2017

До трьох років позбавлення волі загрожує чоловіку, котрий через соцмережі закликав до захоплення Закарпатської ОДА

Процесуальним прокурором повідомлено підозру у вчиненні громадянином публічних закликів до захоплення державної влади, тобто злочину, передбаченого ч. 2 ст.109 КК України (PMG.ua).

Ідеться про коментарі у соціальній мережі Facebook громадянина, який поширював заклики про необхідність блокування та пікетування адміністративної будівлі Закарпатської обласної державної адміністрації, а також розміщував у окремих групах соцмережі такі публічні заклики про необхідність збройного блокування та пікетування адміністративної будівлі Закарпатської ОДА, – стверджує прес-служба прокуратури Закарпаття.

Згідно з висновком лінгвістичного дослідження, у матеріалах, опублікованих 31.01.2017 користувачем Facebook, які надані на дослідження, простежується чітка позиція автора у тому, що тільки масове застосування зброї є запорукою наведення порядку.

Сприйняття змісту аналізованого тексту як такого, що містить заклики до агресивних дій із застосуванням зброї з метою позбавлення службових осіб, державних діячів можливості виконувати свої повноваження, що є одним із способів насильницького захоплення державної влади, є одним із можливих варіантів суб'єктивного сприйняття вказаного тексту реципієнтом.

Це є злочин проти основ національної безпеки України і санкція статті передбачає покарання у вигляді обмеження волі на строк до трьох років або позбавленням волі на той самий строк з конфіскацією майна або без такої.

Проблема захисту даних. DDOS та вірусні атаки

1.02.2017

Сенсоры Oculus Rift можно использовать для слежки за пользователями

Исследователь из Калифорнийского университета в Д. Оливер Крейлос (Oliver Kreylos) пришел к выводу, что сенсоры Oculus Rift мало чем отличаются от веб-камер и намеренно вводят компьютер в заблуждение (InternetUA).

Специалист рассказал изданию UploadVR, что в последнее время занимался изучением сенсоров Oculus Rift. Как известно, сенсоры призваны отслеживать положение Rift и контроллеров Touch в пространстве, ориентируясь на незаметные человеческому глазу инфракрасные светодиоды, которые наличествуют и на контроллерах и на самом VR-шлеме. Исследователь объясняет, что при этом сенсор, по сути, является камерой, с которой при желании можно извлечь изображение.

«Oculus решили скрыть тот факт, что сенсоры Rift – это простенькие веб-камеры. Обычно, когда вы подключаете к USB-порту компьютера веб-камеру, она анонсирует себя как устройство USB video class (uvc), и ПК загружает стандартные драйверы для uvc-камеры, после чего та работает как plug&play устройство.

Камера Rift – это все еще uvc-камера, но идентификатор, который она отправляет ПК, это не video class, а vendor-specific class. Поэтому она не определяется как камера, даже если подключить ее к компьютеру без установки ПО Oculus.

Чтобы все заработало, мне пришлось пропатчить в Linux uvc-драйвер камеры. Когда драйвер видит USB-вендора и ID продукта, совпадающие с Rift, он игнорирует тип класса и воспринимает устройство как uvc-камеру. Так как устройство, по сути, камерой и является, с этого момента оно работает», – рассказывает специалист.

Также исследователь пишет, что Oculus эффективно обманывает компьютер относительно видеоформата, так, вместо реального 1280×960 Y8, сенсоры якобы предлагают лишь 640×960 YUYV.

Несмотря на обнаруженные факты, Крейлос успокаивает публику и говорит, что Facebook, которой принадлежит Oculus, не пытается шпионить за пользователями. На самом деле, исследователь лично убедился в том, что драйвер Oculus не запоминает и не хранит данные, полученные с камеры-сенсора. Эти данные немедленно уничтожаются, после того как из них извлекается информация о расположении (x, y) инфракрасных диодов. Подтвердили выводы исследователя и сами представили Oculus, к которым журналисты обратились за комментарием:

«Кадры, захватываемые сенсором, обрабатываются таким образом, чтобы отделить инфракрасные сигналы от фона, а затем кадры немедленно уничтожаются. Сенсор не подключен к Интернету напрямую, и мы не храним захваченные им кадры, так что никто не сможет получить доступ к этой информации на наших серверах».

Однако Крейлос убежден, что здесь производитель вступает на опасную территорию. Если сенсор способен работать как камера, и при желании с него можно извлечь изображение, этой особенностью могут воспользоваться хакеры, проделав с сенсором все то же самое, что обычно делают с веб-

камерами пользователей на скомпрометированных компьютерах. В теории изображения так же могут передаваться и на серверы Facebook, если компания этого захочет. Впрочем, такой исход видится исследователю маловероятным, так как финансовая выгода для компании будет невелика, а вот проблем подобное поведение вызовет много.

***

1.02.2017

В маршрутизаторах Netgear обнаружена очередная уязвимость

Исследователь компании Trustwave С. Кенин (Simon Kenin) сообщил об уязвимости в маршрутизаторах Netgear, позволяющей злоумышленникам взломать сотни тысяч устройств. С ее помощью атакующий с доступом к web-интерфейсу маршрутизатора может получить пароль администратора в открытом виде. Проблема затрагивает 31 модель устройств Netgear и 2 модели Lenovo (InternetUA).

Уязвимость позволяет осуществить CSRF-атаку и получить полный контроль над маршрутизатором. Жертва может посетить вредоносную web-страницу, позволяющую хакеру с помощью JavaScript получить контроль над устройством, отключить его, изменить настройки DNS таким образом, чтобы в браузерах открывались сайты с вредоносным ПО, и т. д. Если настройки устройства позволяют получать доступ к его панели управления через интернет, злоумышленник может проэксплуатировать уязвимость (CVE-2017-5521) удаленно.

Как обнаружил С. Кенин, вызвав сообщение об ошибке, можно получить код, позволяющий при использовании его с инструментом для восстановления пароля узнать учетные данные администратора. Во многих случаях код даже не требовался, достаточно было ввести произвольный набор цифр. Если коротко, то уязвимость позволяет атакующему с локальным или удаленным доступом к панели управления получить пароль администратора и захватить контроль над устройством.

В настоящее время производитель выпустил обновление, исправляющее уязвимость в некоторых версиях прошивки.

***

1.02.2017

Компания ESET хочет предупредить о фишинговой атаке владельцев электронных счетов PayPal

Компания ESET хочет предупредить о новой фишинговой атаке, которая нацелена на владельцев электронных счетов PayPal. Прежде всего, мошенники присылают фишинговое письмо, имитирующее официальное обращение сервиса (HiTech-News.ru).

Пользователю говорят, что с его учётной записью возникли проблемы из-за подозрительной активности, потому администрация просит подтвердить свою личность для того, чтобы получить доступ к аккаунту. Если обратить внимание на грамматические ошибки, то можно угадать, что пользователь не является носителем английского, однако очень малое количество людей акцентируют внимание на особенностях написания слов в этом сообщении.

После нажатия кнопки «Вход в систему» пользователь попадает не на сайт PayPal, а на другую площадку. На ней пользователю предлагается ввести персональные данные, чтобы вновь пользоваться доступом к аккаунту. Эксперты компании ESET рекомендуют не отвечать на спам и подозрительные ссылки. Для того, чтобы защититься, нужно использовать сложные пароли и двухфакторную аутентификацию.

***

1.02.2017
Предложены радикальные альтернативы паролям

Две компании Nuance Communications и SecureAuth – предлагают радикальные замены паролям в качестве средства доступа к устройствам и сетевым ресурсам. Nuance предлагает авторизацию по голосу, а SecureAuth – по поведению пользователя (InternetUA).

Имитаторы не пройдут

Nuance Communication предлагает голосовую авторизацию в качестве альтернативы паролям. Nuance Communications совершенствует свою технологию распознавания речи более 15 лет, и, по утверждению разработчиков, сегодня она достаточно надежна, чтобы даже самые искусные имитаторы не могли ее обмануть.

Как говорит директор по продуктовой стратегии Nuance Б. Беранек (Brett Beranek), их технология анализирует сто разных характеристик голоса каждого человека. На то, как звучит голос, влияет множество факторов, в том числе форма гортани и носовой полости, отсутствие отдельных зубов и так далее. Вдобавок, у каждого своя уникальная манера говорить.

Технология Nuance анализирует все эти характеристики, благодаря чему успешно различает голоса разных людей. Мало того, она может отличить голос живого человека от аудиозаписи или голосового синтезатора.

«В большинстве случаев мы можем с гарантией различить голоса идентичных близнецов», – заявил Б. Беранек.

Он также отметил, что у клиентов, которые начали использовать решение Nuance, резко сократилось количество мошеннических инцидентов после отказа от более традиционных паролей и прочих средств авторизации.

Замечено нестандартное поведение

Другая «беспарольная» технология, предлагаемая компанией SecureAuth, выглядит еще более продвинутой.

Решение SecureAuth требует авторизации по отпечатку пальца (многие смартфоны сегодня оборудованы соответствующими сканерами), однако даже если авторизация была пройдена, система внимательно наблюдает за особенностями поведения пользователя. Например, она может среагировать на «нетипичные» нажатия клавиш, движения курсора мыши, а также на необычное географическое расположение точки входа пользователя и время логина. Система также отслеживает аппаратные характеристики устройства, с которого пользователь залогинился.

Если ряд признаков свидетельствует о том, что в систему залогинился посторонний (даже несмотря на биометрический сканер), ему будет немедленно заблокирован доступ.

Пароль? – Нет пароля. – Проходите.

Эксперты давно говорят, что пароли – это вчерашний день: их эффективность и сама по себе довольно относительна, и вдобавок самым популярным в мире паролем остается комбинация 123456. То есть сами пользователи часто ставят себя в очень рискованное положение просто потому, что им недосуг задать какой-то более труднозапоминаемый пароль.

«Безусловно, биометрические средства авторизации – куда надежнее, чем пароли и идентификационные номера», – говорит Д. Гвоздев, генеральный директор компании “Монитор безопасности”. – «Авторизация по голосу, отпечаткам пальцев и другим уникальным признакам заметно снижает возможности несанкционированного доступа, – при условии, что средства авторизации работают надлежащим образом. А это не всегда так. Пароли, по-видимому, еще какое-то время сохранят свой статус основного средства авторизации: альтернативные технологии либо дороги, либо обладают какими-то иными недостатками, препятствующими их широкому распространению. Да и сами пользователи неохотно принимают новые технологии, которые требуют от них чего-то больше, чем просто ввод пароля».

Д. Гвоздев также отметил, что обеспечить высокий уровень надежности защиты можно и с помощью традиционных методов, если использовать их в комбинации: «Многофакторная авторизация в любом случае эффективнее однофакторной, даже и самой что ни на есть продвинутой».

***

1.02.2017

Как Google немного следит за вами

Уже давно ни для кого не секрет, что компания Google довольно тщательно следит за своими пользователям и даже подслушивает их. Они не только записывают разговоры и хранят эти данные на своих серверах, а слушают вас через микрофон когда телефон просто лежит рядом. В компании объясняют подслушивание необходимостью сбора и анализа информации, которая в последствии поможет алгоритму подобрать для вас рекламу соответственно интересам (InternetUA).

В целом, ничего страшного в этом нет, если бы эти данные иногда не воровались хакерами разных мастей. Кроме того, случись у вас какой-либо конфликт или просто недопонимание с властями, ваши разговоры компания обязана будет передать в соответствующие органы. Ну и наконец, «подогнанная» под интересы пользователей реклама часто совершенно не попадает под эти самые интересы.

Самое забавное то, что компания и не скрывает все эти данные.

Здесь (https://myactivity.google.com/myactivity?restrict=vaa) хранятся все данные с микрофона вашего телефона. Если тут пока ничего нет, значит, вы ещё не пользовались голосовым помощником, т. е. никогда не говорили: «ОК, Google». А вот полное досье (https://myactivity.google.com/myactivity), которое на вас собрал Google, основываясь на том, что вы делаете в Интернете. Там же есть все, что вы искали в Google, что читали, смотрели и прочее. Кстати, довольно удобное, если нужно что-то еще раз посмотреть. Там же все это можно удалить.

***

1.02.2017
Вредоносная программа крадёт данные и биткоины

Было обнаружено новое вредоносное приложение, нацеленное на клиентов банков. Оно крадёт пароли и биткоины из кошельков пользователей. Открытие сделала занимающаяся информационной безопасностью компания Cyren и она описывает его как масштабную кампанию по распространения вредоносного кода. В данном случае речь идет о кейлоггере, который распространяется в виде вложений в электронных письмах. Отправителями этих писем якобы являются банки (InternetUA).

Письма рассылаются ботами из США и Сингапура, выдавая себя за письма от банков вроде Emirates. В письме обычно указываются финансовые сведения, такие как уведомления о сетевом платеже, тогда как во вложении указываются коды SWIFT для идентификации банков и финансовых институтов для передачи денежных средств. В результате письмо выглядит подлинным.

Вложения могут выглядеть как файлы формата PDF, на самом же деле это исполняемые файлы. При запуске файл удаляет себя и создаёт новый файл под названием filename.vbs в автозагрузке. Программа начинает собирать пароли и другую конфиденциальную информацию, в том числе из браузеров, FTP и почтовых клиентов, где таких сведений больше всего. Собираются пароли и имена пользователей, история браузера, куки и т. д. Если на компьютере есть криптографические кошельки, программа заглядывает в них. Она умеет красть множество валют, включая Bitcoin, Litecoin и Namecoin.

Поскольку это кейлоггер, весь набираемый на клавиатуре текст перехватывается, как и перемещение мыши. Пользователям следует с

осторожностью относиться к получаемым письмам, особенно относительно платежей, которых они не ждали.

***

1.02.2017

Большая часть интернет-трафика в прошлом году была сгенерирована ботами

Интернет захвачен ботами (IGate).

В 2016 г. более 51 % всего трафика в сети было сгенерировано ботами. К такому выводу пришли исследователи компании Imperva Incapsula, специализирующейся на сетевой-безопасности.

В своем докладе аналитики отметили, что из 16,7 млрд визитов на 100 тыс. случайно выбранных доменов в период с 9 августа по 6 ноября прошлого года на ботов пришлось 51,8 % трафика, тогда как на людей – 48,2 %. При этом в 2015 г. уровень человеческого трафик превышал автоматизированный – 53 % на 47 %.

Imperva Incapsula разделяет ботов на «хороших» и «плохих», на них пришлось 22,9 и 28,9 % трафика соответственно. Под «плохими», компания подразумевает ботов, используемых, например, для DDos-атак или рассылки спама. «Хорошие» же боты используются для сбора, обработки и анализа информации.

На долю «плохих» ботов обычно приходится порядка 30 % интернет-трафика ежегодно, отмечают в компании. Таким образом можно утверждать, что каждый третий посетитель сайта – вредоносный бот. Самыми активными из них являются так называемые имитаторы, способные маскироваться под настоящих пользователей и обходить систему защиты.

За прошлый год специалистам Imperva Incapsula удалось отследить 504 уникальных полезных бота, 278 из которых генерировали не менее тысячи посещений в сутки.

***

1.02.2017

5 деталей о себе, которыми нельзя делиться на Facebook

Ваша личная информация чрезвычайно ценна для Facebook. Чем больше сайт знает о вас, тем больше денег компании заплатят рекламодатели, в чью целевую аудиторию вы попали. Но кое-каких подробностей о вас на Facebook быть не должно, иначе однажды вы можете сильно пожалеть об этом. Ранее мы писали о пяти роковых ошибках в вашем поведении на Facebook, а сегодня рассмотрим подборку фактов о себе, которым в личном профиле делать нечего. По крайней мере, так считают в USA Today. Сами по себе эти факты не опасны, но все вместе они могут сослужить добрую службу мошенникам, которые так и рыщут по соцсетям в поисках легкой наживы (From-UA. Новости Украины).

Домашний адрес

Любой человек, который хочет вас ограбить, воспользуется этой информацией. Если вы однажды поддались соблазну и все-таки вписали свой адрес в Facebook, зайдите в свой профиль, нажмите кнопку «редактировать» в разделе «Контактная и основная информация» и удалите свой адрес.

Еще одно место, где неожиданно может всплыть ваш домашний адрес, это – мероприятия, которые вы создаете. Например, если вы публикуете сведения о вечеринке, Facebook может автоматически добавить на страницу ваш адрес, чтобы люди знали, куда идти. Если в настройках мероприятию присвоен статус «Публичное», то любой человек сможет узнать, где вы живете. Или, допустим, ваши друзья захотят пригласить своих друзей – таким образом, круг осведомленных лиц расширится.

Лучше удалите мероприятие, если это произойдет. Пускай люди спрашивают адрес в личной переписке. А чтобы убедиться, что инцидент не повторится, проверьте свою хронику на наличие старых мероприятий, в которых мог остаться ваш адрес.

Что угодно о работе

Постарайтесь не публиковать на Facebook информацию, которая указывает, где вы работаете. Когда кто-то из ваших коллег захочет найти вас на Facebook, он может наткнуться на нечто такое, что ему не понравится. Точно так же, когда хакер захочет проникнуть в систему вашей компании, он сначала соберет доступную в сети информацию о сотрудниках. И есть немало душераздирающих применений вашей социальной информации для получения несанкционированного доступа.

Удалите всю информацию о работе и будьте очень избирательны в отношении коллег, с которыми вы дружите в Facebook. Когда придет время менять работу, едва ли вы захотите продолжать общаться с большинством из них. А если все-таки захотите, старайтесь не публиковать ничего плохого о вашем прежнем месте работы.

Статус отношений

Писать семейный статус в Facebook – значит привлекать излишнее внимание. Количество лайков которое соберет ваша смена статуса с «в отношениях» на «без отношений», вас поразит. Нужна ли вам эта неловкость? Кроме того, смены статусов привлекают кибersталкеров. Вы и сами, наверное, не раз получали уведомление, что ваш друг «развелся» или теперь у вашей подруги с ее новым бойфрендом «все сложно».

Проще всего удалить семейный статус совсем и уведомлять людей об изменениях в личной жизни каким-нибудь другим способом.

Платежная информация

Facebook бесплатный, но иногда он запрашивает номер кредитной карты. Ваша финансовая информация позволяет вам покупать открытки и прочие продукты, доступные прямо на сайте. Как удобно!

Лучший способ слить злоумышленникам данные своей кредитной карты – это забыть выйти из профиля на рабочем или любом публичном компьютере.

Посторонний человек, а иногда друг или член семьи может очень быстро потратить ваши деньги до того, как вы спохватитесь и заблокируете счет. Вы же не хотите, чтобы это случилось с вами?

И вообще, где гарантии, что когда-нибудь Facebook не взломают? Лучше для вас, чтобы данные ваших счетов попадали в онлайн как можно реже.

Номер телефона

А это уже не так просто, потому что некоторые действительно полезные функции Facebook в области безопасности требуют как раз номер вашего телефона. Кроме того, если вы пользуетесь приложением Facebook на вашем телефоне, соцсеть все равно знает ваш номер.

С другой стороны, некоторые люди зачем-то указывают свой номер в профиле. Но иногда даже те, кому вы меньше всего хотели бы его раскрывать, могут увидеть заветные цифры. Если вы однажды так же погорячились и добавили номер телефона в свою анкету, зайдите в раздел «Контактная и основная информация» и напротив своего номера в ниспадающем меню выберите, кто будет видеть эту информацию – «Только я». Затем сохраните изменения.

Так же, как и в случае со своим домашним адресом, пройдитесь по всем мероприятиям, которые вы создавали. И боже вас упаси публиковать одно из этих сообщений «Я потерял свой телефон, вот мой новый номер: XXX-XXX-XXXX.» Люди, которым нужно с вами срочно связаться, могут написать вам личное сообщение, раз уж на то пошло.

***

2.02.2017

Программа, способная разгадать графический ключ на смартфоне

Сегодня сканером отпечатков пальцев оснащены практически все современные смартфоны, даже недорогие. До появления этих сканеров пользователи Android доверяли безопасность графическому ключу на экране блокировки (Украинский телекоммуникационный портал).

Многие продолжают использовать его на планшетах по привычке или на устройствах, не оснащенных дактилоскопическим сканером. Есть весомый повод окончательно перейти к использованию более современной и безопасной технологии.

По данным PhysOrg, появилось программное обеспечение, которое позволяет обойти защиту графическим ключом. На это требуется не более пяти попыток.

Программное обеспечение было создано на основе исследований Ланкастерского Университета, Китайского Северо-Западного Университета и Университета Бат.

Оно анализирует движение человеческих рук во время разблокировки смартфона. Анализ можно проводить с помощью камеры смартфона,

направленной на пользователя устройства практически с любого ракурса и на расстоянии до 2,5 м.

Полученное изображение обрабатывается с помощью алгоритма, который выдает несколько возможных вариантов графического ключа, используемого владельцем смартфона.

Любопытно то, что чем сложнее графический ключ, тем проще для алгоритма его разгадать, так как пользователь будет совершать больше движений, что дает больше данных для анализа.

Из 120 графических ключей, установленных разными пользователями, таким образом удалось разгадать 95 %, сделав не больше пяти попыток.

Лучший способ защититься от такого взлома – это прикрывать свою руку во время разблокировки устройства либо выбрать другой способ защиты персональных данных.

***

7.02.2017

«Доктор Веб» обнаружил Windows-троянца, заражающего Linux-устройства

Linux.Mirai – самый распространенный на сегодняшний день троянец для операционных систем семейства Linux (ITnews).

Первая версия этой вредоносной программы была добавлена в вирусные базы Dr.Web под именем Linux.DDoS.87 еще в мае 2016 г. С тех пор она приобрела большую популярность у вирусописателей, поскольку ее исходные коды были опубликованы в свободном доступе. А в феврале текущего года специалисты компании «Доктор Веб» исследовали троянца для ОС Windows, способствующего распространению Linux.Mirai.

Новая вредоносная программа получила наименование Trojan.Mirai.1. При запуске троянец соединяется со своим управляющим сервером, скачивает оттуда конфигурационный файл и извлекает из него список IP-адресов. Затем Trojan.Mirai.1 запускает сканер, который обращается к сетевым узлам по адресам из конфигурационного файла и пытается авторизоваться на них с заданным в том же файле сочетанием логина и пароля. Сканер Trojan.Mirai.1 умеет опрашивать несколько TCP-портов одновременно.

Если троянцу удается соединиться с атакуемым узлом по любому из доступных протоколов, он выполняет указанную в конфигурации последовательность команд. Исключение составляют лишь соединения по протоколу RDP – в этом случае никакие инструкции не выполняются. Помимо этого, при подключении по протоколу Telnet к устройству под управлением Linux он загружает на скомпрометированное устройство бинарный файл, который в свою очередь скачивает и запускает вредоносную программу Linux.Mirai.

Кроме того, Trojan.Mirai.1 может выполнять на удаленной машине команды, использующие технологию межпроцессного взаимодействия (inter-

process communication, IPC). Троянец умеет запускать новые процессы и создавать различные файлы – например, пакетные файлы Windows с тем или иным набором инструкций. Если на атакованном удаленном компьютере работает система управления реляционными базами данных Microsoft SQL Server, Trojan.Mirai.1 создает в ней пользователя Mssqla с паролем Bus3456#qwein и привилегиями sysadmin. От имени этого пользователя при помощи службы SQL server job event автоматически выполняются различные вредоносные задачи. Таким способом троянец, например, запускает по расписанию исполняемые файлы с правами администратора, удаляет файлы или помещает какие-либо ярлыки в системную папку автозагрузки (либо создает соответствующие записи в системном реестре Windows). Подключившись к удаленному MySQL-серверу, троянец с аналогичными целями создает пользователя СУБД MySQL с именем phpminds и паролем phpgod.

***

7.02.2017

Троянец-шифровальщик парализовал работу целого города

Администрация округа Ликинг в штате Огайо вынуждена была отключить свои серверы и системы телефонной связи, чтобы остановить распространение троянца-шифровальщика (InternetUA).

Кто-то открыл не то письмо

Стало известно, что более тысячи компьютеров в США, относящихся к сетям администрации одного из американских округов, оказались заражены. Все системы были отключены, чтобы заблокировать дальнейшее распространение зловреда, предотвратить потерю данных и сохранить улики для расследования.

Все приемные и административные учреждения работают, но работа с ними возможна только при личном визите.

Размер требуемого выкупа представители администрации не называют; они также отказываются комментировать вероятность выплаты. По словам члена окружной комиссии Ликинга Т. Бабба (Tim Bubb), сейчас ведутся консультации с экспертами по кибербезопасности и правоохранительными органами.

Ручной режим

Отключение телефонных линий и сетевых коммуникаций означает, что все службы округа, в чьей работе задействованы информационные технологии, перешли на «ручной режим». Это касается даже центра помощи 911: телефоны и рации спасателей работают, но доступа к компьютерам нет. По крайней мере, вызовы полиции, пожарных и скорой помощи по-прежнему принимаются, но, как выразился директор центра спасения Ш. Грейди (Sean Grady), работа службы в том, что касается скорости обработки вызовов, отброшена на четверть века назад.

***

6.02.2017

Microsoft: Windows 10 останавливает приложения-вымогатели

Когда сторонние антивирусы не справляются с блокировкой приложений-вымогателей, на помощь приходит операционная система Windows 10, утверждает компания Microsoft. Именно угрозы со стороны вымогателей разработчики называют главной мотивацией для перехода организаций на Windows 10. Система обладает встроенной защитой Windows Defender Advanced Threat Protection (ATP), которая способна блокировать вымогатели (InternetUA).

Microsoft провела исследование с участием семейства Cerber, которое в период между 16 декабря и 15 января доминировало среди нацеленных на корпоративные сети вымогателей. Исследование показало, что кампания по распространению вымогателей способна продолжаться много дней и даже недель, используя похожие файлы и методы. Если организации смогут быстро провести расследование первого случая заражения, они имеют шанс эффективно противостоять нашествию вымогателей, утверждает член исследовательской команды ATP Т. Близард. ATP может обнаруживать автоматический запуск Cerber и выполняемые перед шифрованием файлов действия. Пользователи получают уведомления, которые позволяют им быстро отреагировать.

Поскольку разные вымогатели использует похожие методы, это исследование относятся и к другим семействам. В последнее время Microsoft активно агитирует предприятия переходить на Windows 10 и утверждает, что безопасность Windows 7 не соответствует современным требованиям. Windows 10 Defender ATP получит новые возможности в обновлении Creators Update, в том числе возможность обнаружения вредоносного кода в оперативной памяти, эксплоитов на уровне ядра и инструменты изолирования заражённых систем.

***

6.02.2017

Киберзлодеи. От сбора денег на сепаров до путан по предоплате

Ежегодно в Украине совершается несколько тысяч киберпреступлений.

Интернетизация всего, от микроволновки до ошейников домашних питомцев, – это не только удобно, но еще и опасно. «ДС» выяснила, чего стоит бояться любителям гаджетов. О киберпреступлениях рассказал бывший руководитель технического подразделения департамента киберполиции Е. Чумаченко, который сегодня работает в частной Лаборатории компьютерной криминалистики и принимает участие в документированни следов киберпреступлений (Украинские реалии).

Немного киберцифр

Киберпреступления в Украине регулируются 12 статьями УК – от нарушения авторских прав и неприкосновенности частной жизни до распространения порнографии и создания вредоносных программ или техсредств. Также наказывают за распространение нелегальных веществ через Интернет и нарушение работы транспортных средств или промышленной безопасности (пример – атаки на несколько украинских предприятий облэнерго). За 2016 г. было совершено более 7 тыс. киберпреступлений. Из них около 10 инцидентов связаны с системными атаками на инженерную инфраструктуру предприятий и организаций. По данным департамента киберполиции МВД, за прошлый год полиция получила около 10 тыс. заявлений о киберпреступлениях. Самое популярное (60 % всех инцидентов) – продажа несуществующего товара в Сети (например, детских товаров или телефонов). Точной статистики киберпреступлений нет – для ее получения приходится отфильтровывать среди традиционных криминальных нарушений, совершенных с привлечением компьютерной техники.

ТОП-10 ПОПУЛЯРНЫХ КИБЕРПРЕСТУПЛЕНИЙ

Онлайн-мошенничество с применением электронных торговых площадок – продажа с полной или частичной предоплатой несуществующих товаров и услуг.

Кардерство – вид мошенничества, связанный с противозаконным использованием банковских продуктов (может быть усложнено применением фишинга или вредоносного программного обеспечения).

Мошенничество с использованием телефонных линий и SMS повышенной тарификации – используется с целью незаконного извлечения и «отмывания» финансовых средств пострадавших.

Нарушение Конвенции Совета Европы Medicrime – распространение наркотиков, психотропных веществ, прекурсоров и нелегальных медицинских препаратов через интернет.

Терминация и оригинация телефонного трафика – мошенничество при помощи распределенных аппаратно-программных комплексов с метаданными телефонных соединений, в результате чего оператор недополучает прибыль на огромные суммы.

Нарушения авторского и смежных прав. Истории с закрытием сервисов FS и EX – лишь вершины этого айсберга.

Применение фишинга – пересылка сообщений с тематической ссылкой точной копии страницы ресурса с авторизационными полями «логин», «пароль» (позволяет получить личные данные).

Применение вредоносного программного обеспечения – пересылка сообщений, содержащих ссылку, при переходе на которую скачивается исполняемый файл, замаскированный под легальное приложение или документ.

DoS-атаки – происходят как с целью получения прибыли, так и по политическим или личным мотивам.

Дефейс – изменение внешнего вида публичного сайта, совершается с целью демонстрации политических, религиозных и иных идеологических

требований, удовлетворения личной неприязни, дискредитации владельца веб-сайта.

Махинации с картами лояльности, обмен сепаров и реестры

Независимо от сложности киберпреступлений ущерб от них может составлять от 10–20 грн до 1 млн долл., которые исчезают со счетов крупных компаний. Причем зачастую мошенники придумывают хитроумные способы «сравнительно честного отъема денег у населения». Е. Чумаченко рассказал нам о самых интересных случаях из своего опыта.

Наркотики для подростков

Достаточно необычный пример, связанный с наркоторговлей, – распространение информации о контактных онлайн-данных наркоторговцев на стенах локаций в онлайн-играх для подростков. Сами данные при этом видны только при освещении стены виртуальным инфракрасным фонариком.

Предоплата без секса

Разнообразным бывает и мошенничество с предоплатой. Чаще всего продают несуществующие популярные бытовые товары или технику несуществующей компании. Одним из самых оригинальных было предложение услуг проституток с серьезными скидками по предоплате на телефонный номер в ближайшем таксомате. Известны также частные случаи подмены платежных реквизитов на некоторых атакованных веб-ресурсах, в результате чего деньги поступали на счета мошенников. А при использовании телефонных линий и SMS повышенной тарификации достаточно оказалось платной телефонной связи с Коста-Рикой для оказания услуг секса по телефону. Кстати, этот вариант может быть многоканальным. Для нанесения ущерба достаточно, будучи в роуминге, потерять контроль над телефоном с корпоративной контрактной связью. Известный ущерб в 600 тыс. грн был нанесен буквально за 10 часов крупной медицинской корпорации. У сотрудницы просто украли телефон во время экскурсии в музее.

Золотая буква

Одним из самых знаковых кейсов на памяти Е. Чумаченко стала пересылка огромной суммы денег мошенникам. К сотрудникам Лаборатории обратился некий А, собственник небольшой юридической компании, которая осуществляла управление делами другой офшорной компании в интересах клиента Б. Ежедневной многолетней работой А было получение рутинных указаний делового характера по почте от Б и передача их исполнителям (К). Однажды А получил указание разбить сумму в несколько сотен тысяч долларов на ряд более мелких и отправить их по указанным реквизитам. А чуть позже Б предъявил требование о возврате переведенной суммы. Как оказалось, на самом деле письмо было не от Б – имя почтового ящика отличалось всего лишь на одну букву. Отличались от обычных и реквизиты счетов, куда были переведены деньги. Добиться возврата проведенных платежей А так и не удалось.

Ложь во благо

Еще одним интересным случаем социальной инженерии стали украинские волонтеры, которые собирали денежные средства для наших

воинов в группах сепаратистской направленности – давали собственные платежные реквизиты в сочетании с «героической» символикой и риторикой в стиле самопровозглашенных «ДНР» и «ЛНР».

Взлом реестра

Нотариусу или его помощнику приходит письмо с каким-нибудь «приказом Минюста» и настоятельной просьбой включить макрос «для правильного отображения документа». Не подозревающий ничего нотариус запускает скачанный файл и тем самым дает нападающему удаленный доступ к файловой системе своего компьютера. После этого нападающий получает доступ во внешний реестр Минюста и делает, например, перерегистрацию права собственности с одного субъекта на другого. Наибольший известный ущерб от таких действий – около 1 млн долл.

Фейковые карты

Своеобразным ноу-хау стало сочетание в одном из кейсов гибрида трех видов безопасности: сетевой, финансовой (1С аудит) и классической внутренней. Жертвой мошенников стало крупное предприятие с сетью собственных магазинов и ритейлом в крупных торговых сетях. Выяснилось, что безопасность Сети была на очень низком уровне – легкие пароли и устаревшая версия 1С, в которую мог внести изменения любой кассир. В результате был выявлен сговор бывшего бухгалтера и кассира с пятилетним стажем, которые оплачивали реальные товары несуществующими деньгами с помощью карт лояльности, заведенных на «произвольных» пользователей, а выручку от настоящих клиентов без таких карт присваивали.

Как раскрывают цифровые преступления

Опасаться, что киберагенты постоянно роются в чужих переписках, просматривают закрытые банковские данные либо прослушивают разговоры, не стоит. Борцы с киберпреступлениями заверяют, что не так часто используют личные данные для расследования – для вскрытия переписки требуется разрешение суда. Чаще всего информацию ищут на основе открытых источников и анализируют данные с помощью электронных экспертных систем.

Работа частных исследователей идет параллельно с работой киберполиции. На госслужбу не так-то просто набрать людей. Ведь зарплата IT-специалиста, нужного для работы такого уровня, на рынке может составить 3–5 тыс долл. Тогда как год назад инспектор киберполиции с двухлетним стажем работы получал около 7 тыс. грн (до переаттестации – порядка 4 тыс.). Начальник техподразделения департамента киберполиции получал после переаттестации 15,5 тыс. грн (до – чуть больше 8 тыс.). В настоящий момент в департаменте заняты менее 300 сотрудников при штате в 410 (370 оперативников и 40 агентов).

Спрятаться от киберзлодея

Рядовым гражданам советуют время от времени перепроверять принадлежность своего имущества в реестре Минюста, применять антивирусы и регулярно менять пароли. Известным личностям стоит использовать пароли

высокой сложности при хранении сетевой информации. А богачам – по минимуму использовать онлайн-сервисы, заботиться о конфиденциальности электронной переписки, проверять реестры, использовать биометрические данные для контроля доступа и даже создавать радиопомехи, чтобы дроны не могли снять данные территории частных объектов. Бизнесменам нужно периодически проверять свои офисы на предмет сетевой, экономической и внутренней информации. Всем пользователям рекомендуют использовать двухфакторную идентификацию, шифрование почты, шифрование канала интернет-связи VPN, а также быть внимательнее при получении ссылок и файлов по Сети.

Все научно-технические прорывы последних лет позволяют предположить, что нас ждет рост преступлений, связанных с инфраструктурой «интернета вещей». В список потенциально уязвимых попадают системы «умный дом», телефоны с NFC-чипами, банковские карточки с технологией PAY PASS, браслеты и гаджеты, которые считывают биометрию хозяина, применение медицинской микроробототехники, документы, которые содержат в чипах личные данные, роботизированные такси и аэротакси.

Реагировать на цифровой мир придется и правительствам: не за горами, по словам Е. Чумаченко, развитие невоенных и гибридных конфликтов за передел сфер влияния в области поисковых систем, систем Big Data, средств «малой войны», социальной инженерии, электронных СМИ и социальных сетей. Не стоит сбрасывать со счетов и опасность взлома систем выборов – хакеры могут нанести вреда не меньше, чем «карусели» и мертвые души. «Теоретически никакая компьютерная или сетевая система не может быть на 100 % безопасной», – отмечает Е. Чумаченко и приводит пример 22 мая 2014 г., когда хакеры попытались вывести из строя сайт ЦИК и систему «Выборы» серией направленных атак. Часть из них, по данным СБУ, предпринималась из РФ. После этого электронную защиту ЦИК усилили, но гарантировать, что она выдержит любую атаку, нельзя.

Первой страной в мире, которая решила заняться «цифровым» вопросом, стала Дания: там в начале года создали должность цифрового посла, в задачи которого входит налаживание отношений с цифровыми корпорациями, оказывающими влияние на мир подобно государствам. «Европейское государство осознало, скажем так, состояние некоторого цифрового неравенства, при котором его граждане пользуются технологиями, которые лежат вне его сферы влияния. То есть технологии на них влияют, а они без цифрового посла – нет», – говорит Е. Чумаченко. По его словам, транснациональность совершения киберпреступлений обрекает страны на сотрудничество. Если преступление, связанное с банковскими картами, начинается на территории одной страны, дампы карт заливаются на пластик в другой стране, а обналичивают их дропы (подставные лица) на территории третьей страны, то без быстрого обмена полицейской информацией и исполнения решений суда на территории других стран сделать что-либо очень сложно.

***

5.02.2017

Как защитить квантовые сети от хакерских атак

Американские ученые из университета Оттавы разработали методику, способную защитить квантовой сети от хакерских атак извне (Украинский телекоммуникационный портал).

Теперь все компьютерные данные будут в безопасности, поскольку специалисты исключают возможность взлома в случае использования специального аппарата.

Современные защиты в виде нулей и единиц не относятся к разряду надежных, об этом свидетельствует ситуация, которая произошла в прошлом году в США о время выборов президента страны.

Для решения возникшей проблемы специалистам пришлось погрузиться в мир квантовых вычислений, в котором бит данных, может перебывать одновременно как в состоянии нуля, так и единицы.

При этом в подобном случае защитить информацию от внешних посягательств становится в разы сложнее.

Тем не менее, команда ученых-исследователей под руководством профессора-физики Э. Карими нашла выход из ситуации, сконструировав уникальный в своем роде квантовый аппарат клонирования, который перехватывает спецсообщение на полпути.

В ходе эксперимента специалисты придумали, как можно обезопасить сети от попыток взлома, поскольку им удалось воссоздать полностью идентичные настоящим фатоны, которые задействованы в передачи информации, точнее кубитов.

Кроме того, удалось выяснить, что способ передачи данных, который ранее считался неподвластным взлому, не оказался таковым на самом деле, однако ученые усовершенствовали его по всем направлениям.

***

7.02.2017

76 популярных приложений с 18 млн загрузок в App Store позволяют перехватывать данные пользователей

Специалист по информационной безопасности изучил особенности работы приложений в App Store и обнаружил, что некоторые из них лишь имитируют защиту. По данным экспертов Sudo Security Group, десятки программ, шифрующих информацию пользователей, делают это ненадлежащим образом (InternetUA).

Как сообщает Securitylab, глава Sudo Security Group У. Страфач обнаружил 76 приложений для iPhone, iPod touch и iPad, которые уязвимы к атакам, позволяющим перехватить данные.

У. Страфач утверждает, что из-за ошибок в связанном с передачей данных коде программы могут принимать недействительные сертификаты TLS. Протокол TLS используется для защиты информации, передаваемой приложением через интернет-соединение. Без него хакер может прослушивать трафик и перехватывать любые интересующие его данные, например, логины и пароли.

«Подобные атаки может осуществить кто угодно, находящийся в зоне действия сети Wi-Fi, пока вы пользуетесь вашим устройством. Атаки возможны в общественных местах или даже у вас дома, если атакующему удастся подобраться достаточно близко», – заявили в Sudo Security Group.

У. Страфач обнаружил проблему в 76 iOS-приложениях, просканировав их с помощью разработанного компанией сервиса verify.ly. Исследователь протестировал уязвимые программы на iPhone, работающем под управлением iOS 10. Используя прокси-сервер, эксперт успешно внедрил в соединение недействительный сертификат TLS.

Эксперт утверждает, что 43 из 76 мобильных разработок представляют высокий и средний уровень риска, поскольку злоумышленник может перехватить передаваемые ими логины, пароли и токены. Остальные 33 приложения несут меньшую угрозу, поскольку позволяют перехватывать лишь электронные адреса.

В общей сложности 76 исследуемых приложений были загружены из магазина Apptopia 18 млн раз. У. Страфач не раскрывает названия программ, однако уже уведомил их создателей о проблеме.

***

8.02.2017

У Google фільтруватимуть спам і небезпечні додатки

У середньому тільки 0,1 % вхідних листів у Gmail є спамом. Так, згідно з повідомленням в блозі Google Україна, фільтри в Gmail перевіряють тисячі сигналів: звідки ці повідомлення надіслані, кому вони адресовані, що міститься в повідомленні, і як часто ця людина писала користувачу в минулому (ІНФОРМАЦІЙНА АГЕНЦІЯ «ВГОЛОС»).

У компанії додають, що фішингові шахрайства часто починаються саме з оманливих спам-листів, передає Watcher.

Аби цьому запобігти до моніторингу підключається веб-фільтр Safe Browser, який рекомендує користувачу не відвідувати даний сайт, оскільки, скоріше за все, він містить шкідливі програми та фішинг-атаки.

Safe Browser дозволяє визначити небезпечний контент та убезпечити пристрої від вірусних атак, пояснюють у Google.

«Ми навчаємо Safe Browser просто її (небезпеку) блокувати та оновлюємо систему, позначаючи це як risk rule. У нас є можливість підключити додаткові точки та використовувати інформацію для вдосконалення виявлення шкідливого контенту. Усе це разом допомагає нам показувати червоні

попередження користувачам та захистити 2 млрд пристроїв», – запевняють у компанії.

Схожий за принципом роботи аналізатор Android-додатків сканує програми в Google Play та в інших магазинах. Щодня сканер додатків перевіряє понад 6 млрд програм на 400 млн пристроїв. Коли він знаходить потенційно небезпечні програми, то знищує та видаляє їх з Android-пристрою.

Нагадаємо, у компанії повідомили про те, що у 2016 р. Google заблокував сотні фейкових новинарних сайтів і відключив понад мільярд «поганих» рекламних оголошень.

Такі дії пояснюють реалізацією оновленої політики компанії щодо сайтів, які своїм змістом вводять в оману користувачів.

***

9.02.2017

Опасный «невидимый» вирус поражает банки по всему миру

Инженеры компании «Лаборатория Касперского», разрабатывающей программы для компьютеров, обнаружили новый вирус, заразивший их систему безопасности. Попадая в систему, он остается в оперативной памяти, после чего его очень сложно удалить (Grifonsoft).

Инженеры компании «Лаборатория Касперского» выяснили, что вредоносная программа, названная Duqu 2.0, является дочерней вируса Stuxnet, по версии некоторых специалистов, созданного хакерами США и Израиля, чтобы атаковать ядерную программу Ирана. Теперь эксперты утверждают, что троян распространяется по всему миру.

Вирус очень сложно найти, так как он вписывается в оперативную память системы и может находиться там долгое время. На данный момент Duqu 2.0 уже распространился в более 140 банковских организациях по всему миру, с помощью его киберпреступники совершают финансовые операции, незаконным образом переводя деньги на банковские карточки, а затем снимая их с банкоматов. По данным работников «Лаборатории Касперского» вирус уже найден во Франции, США, Великобритании и Кении.

***

8.02.2017

В «анонимной» истории 70 % информации выдают пользователя

Это удалось установить, сравнив информацию в соцсетях и историю посещения веб-страниц (Экономические известия).

Специалисты смогли идентифицировать порядка 70 % информации из анонимной истории пользователей, информирует news.eizvestia.com.

Для этого они сравнили посты в Twitter с историей посещения сайтов в зашифрованном режиме.

Авторами исследования стали представители Стэнфордского и Пристонского университетов. Сообщается, что принимающие участие в исследовании юзеры использовали расширение Chrome, сохраняющее историю просмотра.

Далее исследователи задействовали собственный протокол сокращения ссылок, и выявили ссылки типа t.co. Проанализировав их, ученые установили, что до 81 % информации после прохождения через программу деанонимизации можно восстановить и получить очень конкретные данные.

При этом точная идентификация пользователя была возможна в 72 % случаев.

В итоге оказалось, что рекламодатели, а также брокеры, могут успешно проводить подобный анализ благодаря отслеживанию файлов cookie, получая в итоге необходимые данные о пользователе.

Специалисты утверждают, что отчасти ограничить подобные попытки поможет использование протокола HTTPS соединения и услуги VPN. Однако в первом случае не маскируется базовый URL сайта, а во втором – не создаются преграды для отслеживания cookie.

***

9.02.2017

Новый вирус превращает Android-устройства в «кирпичи»

Специалисты компании Symantec обнаружили новую разновидность вредоносного вируса Android.Lockdroid.E, превращающего атакованные Android-смартфоны в «кирпичи». В новой версии применяются технологии, ранее использовавшиеся лишь в компьютерных вирусах и не встречавшиеся на мобильных устройствах (InternetUA).

Как работали первые версии вируса

Ранее Android.Lockdroid.E распространялся вместе с приложениями и играми для взрослых. Попав на устройство, вирус блокировал аппарат, шифровал хранившиеся на нем данные и требовал отправить злоумышленникам деньги – лишь в этом случае гаджет обещали разблокировать.

Если требуемая сумма переведена не была, то вредоносная программа рассылала историю просмотренных сайтов для взрослых всем пользователям из списка контактов и сбрасывало устройство до заводских настроек с последующим удалением всех хранившихся на нем данных.

Позднее была выпущена еще одна модификация вируса – Android.Lockdroid.E стал устанавливаться в системный раздел и штатными средствами удалить его не представлялось возможным. При этом зараженный гаджет переставал реагировать на нажатия кнопок, а экран блокировался картинкой.

Вирус просит права администратора

Новая версия Android.Lockdroid.E по-прежнему распространяется через сторонние магазины приложений, спам, зараженные сайты и порноресурсы.

Если пользователь установил вредоносное приложение, вирус начинает проверять гаджет на наличие Root-прав – они предоставляют владельцу Android-устройства полный контроль над системой, что позволяет редактировать и изменять системные файлы и папки.

Если на устройстве их нет, то на экран выводится QR-код со ссылками на реквизиты для оплаты. Если есть, то вирус запрашивает в системе доступ на права администратора. Чтобы убедить владельца предоставить ему эти права, вирус обещает открыть доступ к тысячам фильмов для взрослых абсолютно бесплатно.

После этого APK-файл Android.Lockdroid.E копируется в системную папку и получает статус системного приложения, которое невозможно удалить. Зараженный аппарат перезагружается, и владелец видит сообщение о необходимости перевести деньги на счёт злоумышленников – при этом дисплей и физические кнопки блокируются.

Что делать, если гаджет уже заражен

Единственным доступным вариантом выхода из ситуации в случае заражения является полная перепрошивка устройства – личные данные, фотографии и прочие файлы будут удалены, но зато вы избавитесь от вируса и не переведете деньги мошенникам.

Не стоит скачивать приложения из любых непроверенных источников – на них могут содержаться вредоносные файлы. Если приложение запрашивает разрешения, которые в целом не нужны для его работы, не стоит его устанавливать.

Рекомендуется регулярно обновлять ПО, установленное на вашем смартфоне или планшете. Также нелишним будет загрузить на устройство надежный антивирус и регулярно проверять свой гаджет на наличие вредоносных программ.

***

10.02.2017

Базиленко Анна

З Google Play видалять мільйони додатків, які порушують політику конфіденційності

Google має намір видалити з Google Play всі програми, які не відповідають політиці конфіденційності даних користувача. Про це повідомляє The Next Web (Watcher).

Компанія почала розсилати листи розробникам, чиї додатки роблять запит на використання контактів та інших особистих даних користувача.

Google радить додати в правила попередження щодо використання конфіденційних даних або заборонити своїм сервісам робити запит на доступ до камери, мікрофона або контактів. Розробники повинні розібратися з

правилами політики конфіденційності в своїх додатках до 15 березня. В іншому випадку продукт буде заблокований і видалений з Play Store.

У The Next Web пояснюють, що через такі наміри Google з Google Play зникнуть мільйони додатків. За словами творця гри Hip Hop Ninja! Дж. Куні, це дозволить очистити сервіс від «трешових» ігор. Подібні програми зазвичай запитують багато конфіденційної інформації і нерідко є шкідливими.

***

13.02.2017

Пять правил безопасности в публичных сетях Wi-Fi

Подключаясь к сети Wi-Fi в кафе, гостинице, аэропорту или метро, вы фактически выкладываете свои данные на всеобщее обозрение. Перехватить ваш трафик в публичной сети способен любой школьник. Для этого нужно только скачать в Интернете одну из многочисленных «хакерских» программ и прочитать инструкцию к ней. Вот почему мы настоятельно рекомендуем ознакомиться с правилами безопасного поведения в публичных сетях и, конечно же, следовать им (InternetUA).

В статье мы расскажем об угрозах, подстерегающих вас при использовании публичных сетей, и простых способах защиты.

Векторы атак

Существует три основных типа атак, которые злоумышленник может предпринять при использовании общедоступного Wi-Fi. Наиболее простой и распространённый – сниффинг. Открытые точки доступа никак не шифруют пакеты, а потому перехватить их способен любой желающий. Ну а после того как пакеты оказались у хакера, вычленение из них важной информации, вроде данных авторизации, остаётся делом техники. Программ-снифферов существует немало, причём не только для настольных операционных систем, но и для смартфонов под управлением Android.

В разгар президентских выборов в США на съезде республиканской партии в Кливленде сотрудники компании Avast решили проверить, насколько американские политики заботятся о своей безопасности в Интернете. Для этого в месте проведения съезда было размещено несколько открытых точек доступа, а прошедший через них трафик был проанализирован специалистами. Невольными участниками эксперимента стали около 1200 человек. Его результаты красноречивы: Avast удалось раскрыть личность 68,3 % пользователей Wi-Fi и узнать, какие приложения они запускали и какие сайты посещали.

Второй возможный вектор – атака MitM (Man in the Middle, «человек посередине»), для чего нередко используется ARP-спуфинг. Протокол ARP предназначен для сопоставления внутри локальной сети IP- и MAC-адресов устройств, и в нём не предусмотрена проверка подлинности пакетов. Это даёт злоумышленнику возможность отправить на атакуемый аппарат и роутер пакеты с подменёнными MAC-адресами. В результате смартфон или ноутбук

посчитает, что IP-адресу роутера соответствует MAC-адрес устройства хакера, и будет посылать всю информацию последнему. Роутер также станет отправлять ответы взломщику вместо настоящего клиента.

Третий способ – использование переносной точки доступа (такие устройства обычно делаются компактными и автономными). Если рядом с настоящей точкой доступа появляется вторая с тем же именем сети (SSID), но более сильным сигналом, то окружающие устройства, скорее всего, будут подключаться именно к ней. SSID не всегда делают одинаковым: иногда сеть просто называют похожим образом, рассчитывая на невнимательность пользователей. И хотя второй способ не слишком надёжен и применяется нечасто, мы всё равно советуем в случае малейших сомнений в подлинности найденной вашим гаджетом сети обратиться к персоналу заведения.

В течение прошлого года злоумышленники неоднократно создавали поддельные точки доступа в Московском метрополитене. В результате вместо привычной страницы авторизации пользователи видели на экранах своих устройств нецензурные надписи.

Конечно, существует ещё множество различных типов атак – мы перечислили лишь некоторые. Обычный пользователь едва ли сможет обнаружить прослушку, поэтому о мерах безопасности стоит позаботиться заранее.

В начале статьи мы постарались вас припугнуть, однако на самом деле для сохранения в секрете передаваемой информации достаточно придерживаться ряда несложных правил, а также по возможности пользоваться шифрованными каналами связи. Подробнее об этом мы сейчас и расскажем.

Безопасное шифрованное соединение

Главное правило, которому необходимо следовать всегда и везде – не передавать данные в недоверенных сетях (да и в доверенных тоже) по небезопасным протоколам. Всё больше сайтов, особенно социальных сетей и различных сервисов, требующих авторизации, переходит на защищённый протокол HTTPS, использующий шифрование по протоколам SSL/TLS. Передаваемые по HTTPS данные шифруются вашим устройством и конечным сервисом, что значительно затрудняет использование перехваченной информации, но не делает его полностью невозможным. Все современные браузеры помечают открытые по HTTPS вкладки особым значком в адресной строке (обычно с использованием зелёного цвета) – на это стоит обращать внимание.

Также будет нелишним воспользоваться расширением HTTPS Everywhere, которое доступно для десктопных браузеров Chrome и Opera, а также для Firefox (включая Android-версию). Когда этот плагин работает, все запросы на сайтах с поддержкой HTTPS осуществляются именно по зашифрованному протоколу. Иными словами, расширение позволяет избавиться от ошибок веб-мастеров, которые включают поддержку HTTPS не для всех страниц сайта или размещают на защищённых страницах обычные HTTP-ссылки.

Безопасная аутентификация и оплата

HTTPS помогает сохранить данные в безопасности в большинстве случаев. Однако даже когда вы подключаетесь к сайту по безопасному протоколу, следует использовать двухфакторную аутентификацию – это сведёт к нулю вероятность взлома аккаунта, если ваши данные всё же перехватят и смогут расшифровать. Сейчас двухфакторную аутентификацию поддерживают практически все социальные сети и крупные сервисы.

Несмотря на то, что все платёжные системы сейчас тоже применяют HTTPS, мы рекомендуем использовать для онлайн-покупок отдельную дебетовую карту. Деньги на неё стоит переводить с основной непосредственно перед покупкой, чтобы красть было попросту нечего.

Самая надёжная защита – VPN

Наиболее надёжный способ защиты при использовании публичного Wi-Fi – это VPN-подключение. Здесь важно не совершить ошибку большинства неопытных пользователей и ни в коем случае не задействовать сомнительные программы, десятки которых доступны в магазинах приложений или просто в Интернете. О проблемах с бесплатными VPN-решениями говорили уже давно, но свежее исследование австралийской организации CSIRO дало и вовсе обескураживающие результаты: ряд приложений не шифрует трафик, а множество некоммерческих программ содержит вредоносный код. Если вы всё-таки твёрдо решили использовать бесплатное приложение для VPN-подключения, то применяйте только проверенные варианты, например, Opera VPN.

Если вы готовы немного заплатить за свою безопасность, приобретите подписку на один из надёжных VPN-сервисов. В отличие от некоммерческих программ, платные решения предлагают более высокую скорость, не ведут логов, не имеют ограничений по протоколам и IP-адресам, а также обеспечивают дополнительные опции, например, выбор местоположения выходного сервера. Базовые тарифы таких сервисов стоят 7-10 долл. в месяц – не такая уж и высокая цена за сохранность данных. Подобный вариант подойдёт тем, кто часто пользуется публичными точками доступа с различных устройств.

Если вы редко выходите в Интернет через незащищённые сети и не нуждаетесь в анонимизации, то неплохим решением станет настройка собственного VPN-сервера. Для этого в Сети можно найти множество несложных инструкций, а некоторые роутеры позволяют настроить VPN-сервер и вовсе за пару кликов. Учтите, что тому, кто надумал поступить именно так, потребуется озаботиться наличием «белого» IP-адреса. Некоторые провайдеры предоставляют их безвозмездно, а другие – за небольшую плату.

Взломать конфиденциальные данные британских политиков путём анализа трафика Wi-Fi получилось у компании F-Secure. Используя фейковую точку доступа, исследователи смогли узнать логин и пароль от аккаунтов Gmail и PayPal одного политика, прослушать VoIP-звонок другого и получить доступ к Facebook-аккаунту третьего. В первых двух ситуациях взлом удалось

осуществить с помощью сниффинга трафика, а в третьем – посредством внедрения вредоносного кода на веб-страницу. Отметим, что в случае использования шифрованного VPN-канала подобные атаки не увенчались бы успехом.

Наконец, третий способ – ввод учётных данных вручную. Такой метод используется для наиболее распространённых протоколов – PPTP, L2TP и IPSec, поддержка которых встроена в большинство ОС. В Android для подключения к VPN «вручную» необходимо открыть настройки, а затем найти пункт «Другие настройки» в категории «Подключения». После того как вы перешли в раздел VPN, нажмите «Опции» → «Добавить VPN». В открывшемся окне вам будет предложено выбрать тип подключения и ввести адрес сервера.

После этого вы можете выбрать в списке только что созданный профиль, единожды ввести логин и пароль и нажать «подключиться». Теперь передаваемые данные хорошо защищены, а в панели уведомлений появилась иконка ключа, показывающая статус соединения.

Не сложнее подключиться к VPN и на iOS-устройстве. В настройках вашего гаджета необходимо перейти в раздел «Основные» → VPN и нажать кнопку «Добавить конфигурацию VPN».

После ввода необходимых данных и сохранения вы вернётесь в список доступных VPN-подключений, где останется только нажать на кнопку «Статус». Как и в Android, в статус-баре iOS также появится значок, сообщающий о подключении к VPN-серверу.

Заключение

Итак, чтобы ваши данные не попали в руки злоумышленников или просто излишне любопытных подростков, соблюдайте пять простых правил.

1. Удостоверьтесь, что вы подключаетесь к официальной сети Wi-Fi отеля или заведения, в котором вы находитесь. И кстати, поддельные сети – важная причина выключать на вашем гаджете Wi-Fi тогда, когда он вам не нужен.

2. Старайтесь посещать не требующие авторизации сайты. Проверить почту или оставить комментарий на форуме можно, но только если подключение осуществляется по защищенному протоколу HTTPS.

3. Не проводите через публичную сеть никаких финансовых операций на сайтах. Если вам все же необходимо периодически совершать какие-то платежи через публичный Wi-Fi, используйте отдельную карту, где лежит небольшая сумма.

4. Используйте, где это возможно, двухфакторную авторизацию.

5. Установите на устройство VPN-клиент и обязательно задействуйте его при подключении к общедоступному Wi-Fi. Это самый безопасный способ, но, к сожалению, не всегда возможный: настройки публичных сетей могут не позволять устанавливать VPN-соединение. Кроме того, бесплатные VPN порой работают неприемлемо медленно.

***

13.02.2017

В Великобритании заявили об усилении киберугрозы со стороны РФ

Центр национальной кибербезопасности Великобритании (National Cyber Security Centre, NCSC) завил о росте числа хакерских атак на страну, в том числе со стороны «русских хакеров». Об этом сообщает издание The Sunday Times со ссылкой на руководителя центра К. Мартина (Ciaran Martin) (InternetUA).

По его словам, хакеры все чаще атакуют незащищенные цели, такие как сайты местных советов, благотворительных организаций и университетов, откуда злоумышленники пытаются украсть персональные данные и информацию о научных разработках. Также киберпреступники атакуют правительственные ведомства, в частности, дипломатические и оборонные, с целью хищения секретных сведений.

За последние три месяца на правительственные сайты было осуществлено 188 серьезных кибератак, некоторые из них «несли угрозу национальной безопасности», отметил К. Мартин. Он также добавил, что в последние два года Россия усилила «агрессию в киберпространстве», якобы совершив «серию кибератак на политические институты, политические партии, парламентские организации», чему есть доказательства.

***

13.02.2017

Хакеры атаковали более 100 организаций в 31 стране мира

Эксперты Symantec зафиксировали волну кибератак, направленных на организации по всему миру. В рамах кампании злоумышленники инфицируют компьютерные системы банков неизвестным вредоносным ПО. Согласно данным Symantec, вредоносная кампания продолжается по меньшей мере с октября 2016 г. (InternetUA).

Об операции стало известно после того, как в компьютерных системах ряда банков в Польше было обнаружено неизвестное вредоносное ПО. Как сообщалось, источником заражения стала Комиссия по финансовому надзору Польши. Злоумышленники скомпрометировали сайт регулятора и внедрили скрипт, перенаправляющий посетителей ресурса на страницу, содержащую набор эксплоитов, который загружал на компьютер жертвы вредоносное ПО.

В атаках злоумышленники используют кастомный эксплоит-кит, который заражает компьютеры посетителей на основе списка, включающего порядка 150 IP-адресов. Данные адреса принадлежат 104 организациям в 31 стране мира (в основном это банки и незначительное число телекоммуникационных компаний и интернет-провайдеров).

Как выяснилось в ходе анализа, код вредоносного ПО, получившего наименование Downloader.Ratankba, имеет схожие характеристики с вредоносом, применявшимся хакерской группировкой Lazarus, которую связывают со взломом компании Sony Pictures Entertainment и рядом

агрессивных кибератак на объекты в США и Южной Корее. В настоящее время аналитики Symantec продолжают изучение Ratankba.

***

14.02.2017

В IV квартале 2016 г. увеличилось число гибридных DDoS-атак

По данным компании Nexusguard, в IV квартале прошлого года существенно возросло число DDoS-атак смешанного типа с эксплуатацией четырех и более уязвимостей. Чаще всего подобные гибридные атаки осуществлялись на правительственные и финансовые организации (InternetUA).

Согласно отчету компании, посвященному киберугрозам в IV квартале 2016 г., имевшие место в III квартале атаки с использованием ботнета Mirai положили начало появлению множества ботнетов из устройств «Интернета вещей» (IoT).

В период с ноября по декабрь число DDoS-атак увеличилось на 150 %. Эксперты связывают это с публикацией в открытом доступе исходного кода трояна Mirai. Наибольшее количество IoT-ботнетов исследователи обнаружили в США (116 тыс. или 31,63 %) и Китае (41,2 тыс. или 19,85 %). Далее следуют Япония (13,68 %), Южная Корея (6,75 %), Вьетнам (6,33 %), Бразилия (5,64 %), Индия (4,57 %), Мексика (4,08 %), Европа (3,74 %) и Гонконг (3,74 %).

В 97,5 % DDoS-атак использовался протокол NTP – самый популярный метод во второй половине 2016 г. По мнению экспертов, в 2017 г. IoT-ботнеты по-прежнему будут одной из главных угроз в киберпространстве.

***

14.02.2017

РФ обвинили в атаках на серверы одного из лидеров президентской гонки во Франции

Один из лидеров президентской гонки во Франции Э. Макрон оказался под нападками российских СМИ, которые оказывают активную поддержку его противникам. Кроме того против политика совершаются хакерские атаки (Пресса Украины).

Об этом сообщил генеральный секретарь движения «На марше» Р. Ферран.

Он сообщил, что серверы и базы Э. Макрона ежедневно подвергаются тысячам попыток взлома, которые исходят из территории Российской Федерации. Также постоянно атакуется сайт предвыборной кампании политика.

Также подконтрольные кремлю СМИ распространяют лживую информацию про Э. Макрона, пытаясь выставить его в плохом свете по отношению к М. Ле Пен и Ф. Фийону.

В связи с этим штаб политика обращается к правительству Франции с просьбой «гарантировать, что не будет допущено какого-либо вмешательства в демократическую жизнь страны».

***

14.02.2017

Системы университета были атакованы собственными торговыми автоматами

Устройства «Интернета вещей» (IoT) приобретают у киберпреступников все большую популярность в качестве инструментов для осуществления DDoS-атак. В руках хакеров ботнеты из «умных» чайников, холодильников, камер видеонаблюдения и видеорегистраторов становятся мощным оружием (InternetUA).

В посвященном киберугрозам новом дайджесте компании Verizon описан случай, когда системы неназванного университета были атакованы собственными торговыми автоматами, смарт-лампочками и другими IoT-устройствами. Инцидент был обнаружен после того, как студенты университета стали испытывать проблемы с доступом к Интернету. Работник IT-отдела заподозрил неладное, обнаружив неожиданный всплеск числа запросов к сайтам, посвященным морепродуктам. DNS-сервер не справлялся с большим объемом трафика, и в результате возникли проблемы с доступом к Сети.

Администрация учебного заведения обратилась за помощью к команде Verizon RISK. Эксперты проанализировали логи DNS и межсетевых экранов и обнаружили, что установленные в университете и кампусе IoT-устройства были взломаны и каждые 15 минут отправляли DNS-запросы, связанные с морепродуктами.

Подключенные устройства были заражены вредоносным ПО и являлись частью ботнета. Поскольку в них использовались слабые пароли, взломать их не составило труда. Когда с помощью брутфорса нужный пароль был подобран, вредонос получал полный контроль над зараженной системой. ПО подключалось к своему C&C-серверу и получало от него обновления и новые пароли, в результате чего IT-отдел университета лишился контроля над 5 тыс. устройств.

Просто заменить инфицированные торговые автоматы и лампочки новыми было бы неэффективно, посчитали эксперты Verizon RISK, поскольку из-за ненадежных паролей они снова были бы взломаны. С помощью анализатора трафика исследователям удалось извлечь полученные вредоносом новые пароли для зараженных устройств. Эксперты написали скрипт, позволивший обновить пароли на инфицированных системах и удалить вредоносное ПО.

***

13.02.2017

Віккі Бойкіс

Facebook сканує всі обличчя і створює «цифровий біометричний шаблон». ФБ слідкує за вами, навіть коли ви на інших сайтах. Зібрані дані продають

Будь-яка дія, яку ви робите на Facebook, чи на інших веб-сайтах (якщо ви залогінилися на Facebook), потенційно відстежується і записується на їхніх серверах. Кожен лайк, який ви ставите повідомленню, кожен доданий вами друг, кожне місце, де ви зачекінилися, кожен продукт, лінк, який ви використали, кожне фото – все це фіксується і обробляється у Facebook (ТЕКСТИ.org.ua).

Facebook збирає дані про вас сотнями різних способів і через численні канали. Уникнути цього дуже складно, але прочитавши про те, що вони збирають, ви усвідомите ризики цієї платформи і станете більш обачними, користуючись Facebook.

Добре це чи погано, але Facebook став частиною нашої вітальні, місцем, де ми проводимо найбільше часу після дому та роботи. Тут ми спілкуємося з друзями, обговорюємо новини, організуємо події, сумуємо за померлими, радіємо з приводу народження немовлят, заручин, нової роботи, нової зачіски та відпусток.

Facebook як платформа зайняв надзвичайно велику частину нашого обміну думками, і почав служити нашим «резервуаром пам'яті». Тому важливо розуміти, як саме Facebook як компанія використовує наші надії, мрії, політичні заяви та фото наших дітей, коли він отримує до них доступ.

А він отримує їх по повній програмі. У 2014 р. інженери Facebook зазначали, що у щоденному режимі до них надходить близько 600 терабайт даних.

Для порівняння, розмір у байтах книги «Війна і мир» Толстого становить 3,1 мегабайти. Радянська екранізація цієї книги від 1966 р. триває 7 годин – це 8 гігабайт.

Тобто, люди щодня завантажують на Facebook еквівалент 193 млн примірників «Війни й миру», або 75 тис. примірників екранізації.

Політика даних Facebook окреслює, що саме він збирає з-поміж цих даних, і як використовує зібране. Утім, як це буває з більшістю компаній, Facebook не згадує про те, що відбувається з інформацією насправді.

Роздратована постійними спекуляціями про те, куди потрапляють усі натискання клавіш під час кожного оновлення мною статусу, я вирішила дослідити це питання. Уся інформація, наведена нижче, взята з технічних і наукових публікацій, і того, що я можу побачити сама як користувач Facebook. Я додала до цього тексту свої власні інтерпретації – як фахівець по роботі з даними, який має більш ніж 10-річний досвід у галузі опрацювання даних користувачів.

Якщо хтось, хто працює в Facebook, хоче додати виправлення до цієї публікації, я із задоволенням готова почути від них, що вони насправді не збирають і не обробляють стільки даних, скільки вказує викладене нижче.

Для розуміння того, як працює механізм збирання даних у Facebook, я намалювала (дуже-дуже) спрощену діаграму. Користувач вводить свої дані за допомогою інтерфейсу програми. Це – «фасад», або «фронт енд».

Після цього дані надходять у базу даних Facebook (а їх існує багато). Це «задній двір», або «бек енд».

Компоненти Facebook: інтерфейс користувача і база даних

Дані, які користувачі бачать «на фасаді», є підмножиною даних, зібраних на «задньому дворі».

Якщо вас цікавить більше технічних деталей, у гуглі є багато діаграм про цю архітектуру. Facebook знаходиться на передовому краї обробки «великих даних», і їхній інструментарій містить програми Hive, Hadoop, HBase, BigPipe, MySQL, Memcached, Thrift, і багато, багато інших. Усі вони діють на базі великої кількості дата-центрів, наприклад, таких, як у Прайнвіллі, штат Орегон.

Що знає Facebook ще до того, як ви запостили повідомлення?

Збирання даних у Facebook потенційно починається ще до того, як ви натисли «POST». Поки ви створюєте ваше повідомлення, Facebook отримує дані про те, які клавіші ви натискаєте.

Раніше Facebook використовував ці дані для вивчення явища самоцензури.

Ось що написали дослідники:

«Ми наводимо результати нашого дослідницького аналізу, який вивчав самоцензуру “останньої хвилини”, або контент, який був відредагований після того, як його написали на Facebook. Ми зібрали дані по 3,9 млн користувачів протягом 17 днів, і пов’язали дії з самоцензури з ознаками користувачів, їхньою мережею особистих контактів і взаємодією між ними.

Ось види даних, які використовувалися під час дослідження:

Demographic	Behavioral	Social Graph
Gender [GEN]	Messages sent [AUD]	Number of friends [DIV]
Age [AGE]	Photos added [CTRL]	Connected components [DIV]
Political affiliation [CTRL]	Friendships initiated [CTRL]	Biconnected components [DIV]
Media (pic/video) privacy [CTRL]	Deleted posts [CTRL]	Average age of friends [AGE]
Wall privacy [CTRL]	Deleted comments [CTRL]	Friend age entropy [DIV]
Group member count [AUD]	Buddylists created [CTRL]	Mostly (conservative/liberal/moderate) Friends [CTRL]
Days since joining Facebook [CTRL]	Checkins [CTRL]	Percent male friends [GEN]
	Checkins deleted [CTRL]	Percent friends (conservative/liberal/moderate) [DIV]
	Created posts [CTRL]	Friend political entropy [DIV]
	Created comments [CTRL]	Density of social graph [DIV]
		Average number of friends of friends [DIV]

Види даних: 1) демографічні (вік, стать, політичні уподобання, приватність медіа, приватність записів на «стіні», кількість членства в групах, тривалість перебування на Facebook; 2) поведінкові (послані повідомлення, додані фото, ініційована дружба, видалені повідомлення тощо); 3) соціальні графи (кількість друзів, поєднані компоненти, компоненти з подвійним зв'язком, середній вік друзів, відсоток друзів-чоловіків тощо.

Що тут цікаве: видалені пости, видалені коментарі та видалені геомітки (чек-іни). Тобто, так само як видалення вами написаного не гарантує, що ця інформація зникне, нема гарантії й того, що видалені вами дані дійсно видаляються.

Тож, навіть якщо ви видалите пост, Facebook продовжує відстежувати цей пост.

Facebook зберігає метадані, тобто, дані про ваші дані. Наприклад, дані про телефонний дзвінок - це те, про що ви розмовляли. Метадані про дзвінок – це коли ви дзвонили, звідки, як довго тривала розмова тощо.

Для Facebook метадані такі ж важливі, як і реальні дані, і він використовує ці дані для екстраполяцій про те, ким ви є. За допомогою інструмента Developer Tools в браузері Chrome порівняно нескладно побачити той потік даних, який надходить до Facebook від клієнтської програми до «заднього двору» через функції мови HTML.

Я не є гуру з роботи фронт-енду (але хотіла би поговорити з таким, щоб дізнатися, що ще можна витягти), але з цього фрагмента видно, що Facebook відстежує, скільки часу ви робите... щось? Не зрозуміло, що саме, але це, імовірно, час, проведений вами на його сайті, про що повідомляє Facebook.

Між іншим, те ж саме стосується і видалення екаунтів.

Про те наскільки багато систем інтегровано у Facebook, настільки багато місць, де дані можуть змішуватися, написав колишній консультант Facebook:

«Відповідаючи на ваше перше запитання: "Чи можна заплатити Facebook, щоб той належним чином видалив усю інформацію про вас?" – якщо слова "належним чином" означають повністю витерти будь-які сліди того, що ви взагалі існували на Facebook – то відповідь буде "ні"».

Те ж і з видаленими постами: нема гарантії, що Facebook не залишає пост у базі даних на «бек енді»; просто він не буде показаний на клієнтській стороні веб-сайту.

Як тільки ви написали пост, завантажили картинку чи змінили будь-яку інформацію, усе це абсолютно легально використовується для внутрішніх цілей Facebook – досліджень, перепродажу компаніям зі збору маркетингової

інформації, таким як Acxiom, та передачі владі Сполучених Штатів Америки – через установи на кшталт Агентства національної безпеки, у її систему PRISM.

Ви розмістили повідомлення: що про вас збирає Facebook після цього?

Facebook, що очевидно, збирає всі дані, які ви добровільно йому передали: ваші політичні вподобання, місце вашої роботи, улюблені фільми, улюблені книги, місця, де ви поставили геомітку («зачекінилися»), зроблені вами коментарі та будь-які реакції на пост. Facebook дає вам змогу завантажити частину набору даних, яку вони мають щодо вас у своїй базі даних.

У моєму особистому наборі я побачила:

– Фото – завантажені мною, і там, де мене «тегнули» інші.
– Відео.
– Все, що я хоч колись постила в своєму профілі (включно з подіями, щодо яких я вказала зацікавленість, записами інших людей у моєму профілі, спогадами, якими я ділилася тощо).
– Друзі на Facebook, і коли сама я їх зафрендила.
– Події, на які я пішла.
– Усі мої приватні повідомлення.
– Назва всіх пристроїв, з яких я вводила пароль і логін для доступу в Facebook.

А ще – яка реклама мене може зацікавити. А ось це я сама не вводила. Це те, що Facebook згенерував алгоритмічно, виходячи з усього того, що я розмістила.

Але ми поговоримо про це в розділі про рекламу.

На додачу до даних і метаданих Facebook також відстежує наміри. Один із способів, як це робиться, ми вже дослідили: нерозміщені пости. Ще один – це відстеження т. зв. теплової карти на відео (з неї можна зрозуміти, на що саме ви дивилися, коли користувалися круговими панорамними відео).

На додачу до всього, що Facebook знає про вас, він знає все і про вашу дружбу. Таким чином, Facebook має про вас чимало інформації, навіть якщо ви не поповнюєте ваш профіль або не є активним користувачем сайту.

Які внутрішні процеси Facebook застосовує до ваших даних?

Facebook активно користується зібраними ним даними.

По-перше, він виконує до баз даних прості запити, щоб покращити продуктивність сайту, або для бізнесової звітності (наприклад, скільки часу люди провели на сайті, скільки є користувачів Facebook, який дохід від реклами отримано сьогодні тощо). Так робить будь-яка інша компанія.

Утім, у випадку з Facebook тут є особливість. У компанії працює ціла команда розробників, яка створює інструментарій для спрощеного аналізу даних за допомогою запитів до них на мові, подібній до мови запитів SQL, яка «надбудована» над платформою опрацювання великих даних Hadoop, разом із системою Hive. І хоч Facebook стверджує, що доступ до даних користувачів суворо контролюється, деякі приклади говорять інакше.

П. Сільямакі, директор рекордингової фірми Anjunabeats, привернув увагу до такого випадку: коли він відвідував офіс Facebook у Лос-Анжелесі, співробітник без проблем зайшов до його екаунту, не питаючи про пароль.

Ось ще кілька прикладів того, як співробітники Facebook передивлялися приватні дані.

По-друге, Facebook проводить наукові дослідження, використовуючи своїх користувачів у якості піддослідних морських свинок. Цей факт не згаданий в Політиці даних. Це цікаво, якщо врахувати, що заголовок на головній веб-сторінці Facebook Research стверджує: «У Facebook дослідження пронизують усе, що ми робимо».

Це величенька команда науковців даних (41 особа за останніми підрахунками). Для порівняння, компанія аналогічного розміру – 15 тис. співробітників – наймає п'ять науковців, що працюють з даними, якщо вона має наміри агресивно просувати власну програму з дослідження даних.

Утім, станом на 2014 р. не було процедур, які перевіряли, до яких даних надається доступ, і для яких саме досліджень. Як написав колишній співробітник Facebook, що досліджував дані:

«Коли я працював у Facebook, не існувало наглядового органа, який оцінював би рішення щодо проведення експериментів заради внутрішніх цілей. Як тільки хтось отримував результат, який вони хотіли опублікувати в науковому журналі, вони постійно контактували з піар-службою та юридичним відділом щодо того, чи можна це публікувати.

А якщо ви хотіли провести тест і побачити, чи натискатимуть люди на зелену кнопочку замість синьої кнопочки, ніякого погодження не треба було. Точно так само, якщо ви хотіли перевірити нову систему "націлювання" реклами і побачити, чи люди стали більше переходити по рекламних оголошеннях, і чи зріс доход, вам не треба було отримувати офіційне погодження».

І хоч автор відзначає, що це нормально для будь-якої компанії, яка надає програмні послуги як сервіс, більшість таких компаній не збирають ретельно найбільш інтимні деталі людських життів протягом уже більш ніж 10 років.

Співробітник далі зауважує:

«Фундаментальна ціль більшості людей, які працюють над даними у Facebook – це впливати та змінювати настрій і поведінку людей. Вони роблять це постійно, щоб ви частіше натискали на "лайк", клацали на більшій кількості реклами і проводили на сайті більше часу».

Попри те, що це, зрозуміло, є метою більшості веб-сайтів, вам слід подумати двічі, чи варто вам проводити довше ніж 40 хвилин на день на сайті, спрямованому на підрив вашого емоційного стану.

На додачу до того, що Facebook досліджує тексти й вивчає наші емоції, він ще й маніпулює ними.

Стрічка новин – це основа для маніпуляції, особливо тому, що Facebook навмисне розробив її так, щоб вона була максимально привабливою: це синаптичні ласощі для нашої нервової системи. Facebook хоче бути певним, що

ви проводите за переглядом стрічки новин стільки часу, скільки можете, і тому збільшує кількість появи в ній фото немовлят та інших позитивних речей, так само як і новин, що генерують суперечки та обурення, і зменшує кількість нормальних статусів на кшталт «я сьогодні поснідав», на які нема реагування.

Ось так і працює так звана «бульбашка фільтрів». Через те, що люди клацають мишкою на речах, які їм цікаві, Facebook демонструє лише ті речі, що для них є вагомими.

Це означає, що інші точки зору, друзі та картинки усуваються зі стрічки новин певної особи. Чудовим прикладом того, як це працює, є стаття «Червона стрічка, синя стрічка», яка демонструє, наскільки по-різному виглядають лінійки новин на Facebook для користувача-ліберала і користувача-консерватора.

Що ще вони вивчають? Для початку – частоту, з якою геї відкрито заявляють про свої уподобання. Звідки вони про це дізнаються? «За минулий рік приблизно 800 тис. американців змінили свій профіль, вказавши схильність до осіб своєї статі або вказавши гендерну орієнтацію».

Багато досліджень Facebook зосереджені навколо теорії графів: як ми пов’язані з нашими друзями. Інакше кажучи, вони провадять антропологічні дослідження над особами, які ніколи не давали на це згоду.

Наприклад, нещодавно команда науковців даних оприлюднила дослідження про соціальні зв’язки спільнот іммігрантів у Сполучених Штатах Америки, де дослідники використовували такі дані:

«Межею нашого аналізу був збір даних, заснованих на інформації зі знеособленої соціальної мережі, про людей із США, які використовували Facebook хоча б один раз за тридцять днів, що передували аналізу. Ми використовували дані про місто їхнього народження, вказане у профілі особи, щоб визначити його рідну країну.

Ми також обмежили наш аналіз вибіркою людей, які мають як мінімум двох друзів, що проживають у рідній для нього країні, і ще двох друзів, які зараз живуть у США. Наші результати базуються на вибірці з понад 10 млн людей, що відповідають цим критеріям. Усі подальші згадки про користувачів Facebook у цій статті неявно беруть до уваги вищезгадані обмеження.

Це – дослідження, які були опубліковані. А що ще вони роблять приховано?

Інше явище, яке люблять досліджувати у Facebook – це обличчя (що цілком зрозуміло). Кожного разу як ви ставите помітку про вас на фото, Facebook розпізнає, що це ви, і пристосовується до цієї інформації.

Facebook заохочує користувачів «тегати» людей на фото, які вони завантажують в своїх особистих постах, і соціальна мережа зберігає зібрану таким чином інформацію. Компанія використовує програму під назвою DeepFace для співставлення різних фото одної людини.

Програма DeepFace – просто фантастичний спосіб отримувати більш точні теги. Це також фантастичний спосіб порушувати чужу приватність. Наприклад, а що як ви не хочете, щоб вас «тегали» на фото? Бо ви, наприклад,

берете участь в акції протесту проти влади? Або ще простіше – пішли на концерт з одним другом замість іншого, і не хочете, щоб про це хтось знав?

На жаль, про захист приватності пересувань скоро можна буде забути. Facebook працює над способами ідентифікації людей, які сховані на фото.

Стаття Facebook про DeepFace вказує, що «соціальні та культурні наслідки технологій розпізнавання облич є далекосяжними», але взагалі не веде мову про можливу загрозу для приватності. Наприклад: «Скоро в магазинах будуть камери спостереження, які ідентифікують людей під час шопінгу».

Звідки вони все це знають?

Бо всі ці дані ми даємо їм добровільно, кожного разу, як доповнюємо статус, завантажуємо і «тегаємо» фотографію, кожного разу, коли пишемо повідомлення другу, «чеканимося» в певному місці, кожного разу, коли ми входимо Facebook, і система генерує повідомлення – «Так-так, ця людина зараз перебуває у всесвіті Facebook» – а він зараз включає ще й месенджер Whatsapp і фотосервіс Instagram.

Тіньові профілі

А що робить Facebook, якщо ви не розміщуєте про себе стільки даних, скільки йому хотілося б? Він створює тіньовий профіль, або колекцію даних, які Facebook зібрав про вас і які ви не надали йому самостійно».

Як зазначено в статті:

«Навіть якщо ви ніколи не надавали цих даних, Facebook, дуже імовірно, має ваші альтернативні адреси електронної пошти, ваші телефонні номери і домашню адресу – все це люб'язно забезпечили ваші друзі, які намагалися знайти вас і зв'язатися з вами».

Ще гіршим є те, що Facebook збирає… ваше обличчя – в буквальному сенсі.

«Один нещодавній судовий позов стосувався не електронних адрес чи телефонних номерів, а "шаблонів обличчя": щоразу, коли користувач завантажує фото, Facebook сканує всі обличчя і створює «цифровий біометричний шаблон».

Усе це давало б підстави тривожитися навіть якби Facebook збирав ці дані лише для власного вжитку. Але на них є зовнішні покупці.

Як Facebook пов'язаний з маркетологами?

Політика даних Facebook вказує, що він у партнерстві з іншими вендорами збирає про вас дані:

«Ми отримуємо інформацію про вас та ваші дії у Facebook та за його межами від партнерів-"третіх сторін", наприклад, інформацію від партнера, з яким ми спільно пропонуємо вам послуги, або від рекламодавця про ваш досвід чи взаємодію з ними.

Вони збирають «близько 29 тис. демографічних індикаторів, і близько 98 % їх засновані на активності користувача на Facebook».

Близько 600 типів даних, тим часом, надходять від незалежних брокерів даних, таких як Experian, Acxiom та ін. Користувачі, зазвичай, не отримують доступу до цих демографічних даних, зібраних третіми сторонами.

На додачу до збирання всіх деталей, які ви добровільно повідомили про себе, таких як повне офіційне ім'я, дата народження, хобі, релігія, місця вашого навчання та роботи, Facebook також робить припущення про речі, які йому не відомі, щоб він міг поділитися цими даними з Acxiom чи іншими впливовими рекламними сервісами, щоб ті більш ефективно скеровували на вас рекламу.

Наприклад: дохід домогосподарства, на основі якого створюється профіль даних, який надсилають маркетологам – а ті, зрештою, є клієнтами, які платять. Маркетологи після цього можуть купувати «відбірну» рекламу, яка містить наступне:

Місце проживання, Вік, Стать, Мова, Рівень освіти, Галузь освіти, Школа, Етнічна належність, Дохід, Майновий рівень, Нерухомість, Вартість нерухомості, Площа нерухомості, Площа оселі, Рік спорудження будинку, Структура помешкання.

Звідки Facebook про це знає? З припущень, заснованих на відомих йому даних та даних, отриманих з Experian та аналогічних сервісів?

Ці дані можна потім використовувати для «націлювання» реклами на користувачів Facebook. Види таргетингу, які можна реалізувати за допомогою Facebook, багато говорять про те, які дані вони тримають «за сценою».

Наприклад, відбір реклами може відбуватися не тільки за місцем проживання/віком/статтю/мовою, тут можуть бути й хобі та етапи життя (щойно заручилися, заручилися півроку тому, діти молодшого шкільного віку тощо). Можна застосовувати настільки вузькі критерії, і все одно вони будуть стосуватися певної кількості людей (у моєму прикладі їх було 100–200).

Ці дані можна перепродати далі по ланцюжку, де вони будуть поєднані з іншими даними, які існують щодо вас – інформацією від використання кредитних карток та іншими маркетинговими джерелами – для створення сайтів на кшталт цього, де буде здійснено спробу створити ваш повний профіль. І нема легких способів усе це видалити, бо як тільки дані створені, ліквідувати їх повністю стає набагато складніше. Ось чому одна з першочергових вимог активістів, що вимагають захисту приватності – це змусити компанію видаляти всі дані «оптом» після певного періоду часу.

Які дані Facebook передає владі?

Ми не знаємо про все, що Facebook надає в розпорядження влади. На Facebook існує сторінка про запити урядових інстанцій різних країн щодо надання інформації. Вона не оновлювалася з червня 2016 р. Утім, ми знаємо, що влада вимагає дедалі більше інформації.

Ці дані приводять до звіту, який показує, до якої кількості даних були запити, і скількох користувачів це стосувалося, але нічого не повідомляє про тип наданої інформації, і які установи робили запит (місцеві, державні, ФБР/АНБ тощо).

М. Цукерберг навіть зробив із цього приводу заяву:

«Facebook не є і не буде частиною жодної програми, яка надає США чи іншим урядам прямий доступ до наших серверів. Ми ніколи не отримували вимоги чи судового припису від будь-якої урядової установи про надання

інформації або метаданих у значних обсягах, як вимоги, яку начебто отримував Verizon. А якби отримали, ми б агресивно з цим боролися. Ми навіть не чули про PRISM (система шпигування за інтернет-трафіком у США – Ред.) до вчорашнього дня».

Знову ж таки, тут важливо читати написане між рядками. Прямий доступ до серверів зовсім не є необхідністю для пересилання масивів даних. І нема потреби знати про те, як називається система PRISM.

Також складно встановити, чи Агентство з національної безпеки збирає дані з Facebook у інший спосіб. У Європі, принаймні, з цього приводу тривають судові процеси.

Але наразі просто візьмемо до уваги те, що таке спостереження триває.

Що відстежує Facebook після того, як ви вийшли з сервісу?

За межами сайту Facebook стежить за вами за допомогою сервісу «єдиної реєстрації» (коли ваш екаунт у Facebook використовується для користування іншими сайтами – наприклад, коментування – Ред.) Якщо ви вилогінилися, Facebook усе одно стежить за вами за допомогою «кукіз». Як стверджує їхня політика приватності:

«Ми збираємо інформацію, коли ви відвідуєте треті сайти чи користуєтеся програмами, які використовують наші сервіси. Це включає інформацію про веб-сайти чи програми, які ви відвідуєте, ваше використання наших сервісів на цих веб-сайтах і програмах, а також інформація, яку розробник чи видавець програми або веб-сайту надав нам щодо вас».

Facebook також намагається відстежувати, або і вже відстежує, як ваш курсор рухається по екрану. Починаючи з 2011 р., він також почав стежити за тим, як ви робите переходи в Інтернеті, якщо ви не вилогінилися з Facebook.

Facebook стежить за тим, де ви є в Інтернеті після того, як залогінилися на Facebook – без вашої згоди. Н. Кубрілович копнув трохи глибше і виявив, що Facebook може відстежувати вас і тоді, коли ви вилогінилися. Facebook, зі свого боку, спростував цю заяву.

Але можна достовірно сказати, що він збирає інформацію про ваші відвідування сайтів у Інтернеті – для того, щоб більш точно показувати вам рекламу.

Про що слід задуматися користувачам Facebook

І що це все означає? По суті це значить, що будь-яка дія, яку ви робите на Facebook, чи на інших веб-сайтах (якщо ви залогінилися на Facebook), потенційно відстежується у Facebook і записується на їхніх серверах.

Слід чітко розуміти, що будь-яка компанія зараз у певний спосіб відстежує своїх користувачів. Просто нема іншого способу оцінити свої операції.

Але цілком очевидно, що Facebook тихцем проник за ті межі, які протягом тривалого часу вважалися етично прийнятними діловими практиками щодо даних. Навіть якщо Facebook зараз і не робить чогось із згаданих мною речей (запис повідомлень до публікації, маніпуляції з лінійкою новин), вони виконують дуже схожі завдання, і нема гарантії збереження вашої приватності,

чи що вас не використовують в якомусь експерименті. Це також означає, що навіть якщо ви не активізували Facebook, за вами все одно можна стежити.

Кожен лайк, який ви ставите повідомленню, кожен доданий вами друг, кожне місце, де ви зачекінилися, кожен продукт, лінк, який ви використали, кожне фото – все це записується й обробляється у Facebook.

Як саме обробляється? Важко сказати. Можливо, як частина соціального експерименту. Можливо, ваші дані передають урядовим установам. Можливо, окремі працівники Facebook, у яких не обов'язково є на це права, мають доступ до вашої сторінки і до історії ваших працевлаштувань. Можливо, ця історія працевлаштувань надходить до страхових компаній.

Це включає всі приватні групи, всі закриті групи і всі повідомлення месенджера. І як вказує Facebook, у ньому не існує такої речі, як приватність.

Це по суті означає, що, заходячи на Facebook, ви маєте усвідомлювати, що все, що ви там робите, може стати публічним, або використане для реклами, або проаналізоване урядовою установою.

Що мені робити, якщо я не хочу, щоб Facebook використовував мої дані?

Facebook був започаткований як засіб спілкування між студентами коледжу, і зрештою дійшов до рівня, коли він змінює поведінку людей, відстежує користування, і, можливо, збирає інформацію для влади.

Проблема в тому, що будь-яка особа, користується вона Facebook чи ні, є втягнутою в систему стеження, визначення взаємних стосунків і створення тіньових профілів. Але це особливо справедливо, якщо ви є активним користувачем Facebook.

Тож найважливіше – це усвідомлювати, що відбувається. І передавати у Facebook якнайменше даних.

Ось список речей, які я роблю, аби мінімізувати свій показ на Facebook:

1. Не розміщуйте зайву особисту інформацію.
2. Не розміщуйте фотографії ваших дітей, особливо коли вони ще у віці, який не дозволяє їм висловити згоду на це.
3. Виходьте з Facebook, коли ви не користуєтеся цим сайтом у вашому браузері. Використовуйте для Facebook окремий браузер, і окремий – для всього іншого.
4. Використовуйте програми, що блокують рекламу.
5. Не використовуйте Facebook і особливо його компонент Messenger для організації чи участі в політичних заходах. Якщо вам потрібно це зробити, починайте з Facebook як з відправної точки, а потім переходьте на іншу платформу. Рекомендовані платформи: Signal є наразі золотим стандартом для приватного чату. Whatsapp підходить для групового чату, але я не рекомендую його, бо він пов'язаний із системою метаданих Facebook. Telegram теж годиться, але не настільки, бо його код закритий. І знову ж таки, усе залежить від рівня ризику, який ви готові прийняти.
6. Не встановлюйте програму Facebook на телефоні. Вона вимагає надати їй багато неадекватних дозволів.

7. Не встановлюйте на телефон Messenger. Використовуйте мобільний сайт. Зараз Messenger заблокований на мобільних пристроях, тому використовуйте обхідний шлях – дозволяйте браузеру запускати на смартфоні десктопну версію сайта.

Не всі робитимуть те, що роблю я. Але найважливіше те, що навіть якщо ви вирішили продовжити користуватися Facebook як раніше, ви будете усвідомлювати, що Facebook робить з вашими даними, і йти на цей компроміс, пов'язаний із можливістю спілкування в соцмережі.

Дуже прикро, що соціальна мережа, яка зробила стільки добрих справ, є водночас і найгіршим явищем у Інтернеті, але поки люди не підуть з цієї платформи або не почнуть чинити на неї певний економічний тиск, нічого не зміниться.

Ми – соціальні істоти, і всі ми прагнемо бути пов'язаними, отримувати схвалення, ділитися повідомленнями й організовуватися на платформі, де присутні всі ми. І це наразі є перевагою Facebook.

При цьому не слід казати, що Facebook – це суцільне зло: він дійсно поєднує людей, він дійсно допомагав організовувати зустрічі та події, і він дійсно зробив світ більш взаємопов'язаним.

Але ми, користувачі Facebook, та наші дані – це його продукт. І, краще усвідомлюючи те, як ці дані використовують, ми все ще можемо бавитися на майданчику Facebook, де діють його правила, але робити це розумніше.

***

14.02.2017
Роман Черный
Подводные камни бесплатных мобильных приложений

На первый взгляд, это выглядит как честный обмен. Вы бесплатно пользуетесь приложением, но взамен вынуждены смотреть назойливую рекламу. Но всё ли так безоблачно? Увы, не всегда (IGate).

Неочевидный обмен

Очень часто за бесплатное пользование приложением пользователь платит не только просмотром рекламы, но и предоставлением огромного количества персональных данных. Мобильные приложения могут собирать целую кучу информации о владельце мобильного устройства. Это могут быть данные о локациях и перемещениях пользователя, онлайн-история и контакты, планировщик задач и история поиска. Такая информация нужна рекламным сетям, чтобы те могли подобрать лучшую рекламу для конкретного человека и подсунуть ему ее в нужном месте и в нужное время.

В общем, происходит не обмен «приложение за просмотр рекламы», как принято считать, а обмен «приложение за возможность следить за каждым вашим шагом». Соглашаясь использовать поддерживаемые рекламой продукты, вы соглашаетесь с тем, что за вами все время будут подсматривать.

Зачем это нужно маркетологам? Дело в том, что смартфон – устройство, которое пользователь практически всегда носит с собой. Оно обрабатывает огромное количество персональной информации всех типов. Благодаря этому рекламщики могут более точно таргетировать свою рекламу. К примеру, пользователь оказывается около магазина электроники, и тут же получает рекламу с предложением купить какой-то электронный товар. В некоторых случаях такое вмешательство может переходить рамки дозволенного. К примеру, по сетевой активности молодой женщины ритейлер может узнать, что она беременна, еще до того, как она расскажет об этом своим близким.

Серьезная проблема

Хотя все вышеперечисленное уже выглядит жутковатым вмешательством в личную жизнь пользователя, у такой системы есть еще одна серьезная проблема. Речь идет не только о безопасности самого пользователя, но и о безопасности всех структур, в которые он вовлечен. Иными словами, бесплатные мобильные приложения могут являться серьезной угрозой для бизнеса. Чем больше личных устройств вовлечено в бизнес, тем выше риски корпоративных взломов, утечек данных и кибератак.

Приложения сливают кучу информации из корпоративных сетей

К примеру, если компания позволяет своим сотрудникам синхронизировать корпоративный календарь событий со своими смартфонами или планшетами, то обо всех планах автоматически узнают посторонние. А сбор данных о рабочих контактах пользователя может заметно упростить хакеру фишинговую атаку или взлом методами социальной инженерии.

Все усложняется еще и тем, что разработчики приложений продают данные одной рекламной сети, а та, в свою очередь, делится информацией с другими. Таким образом, конфиденциальная информация оказывается в руках огромного количества посторонних людей, и утечку отследить просто нереально.

Хакерам же не нужно даже пытаться взламывать устройства конкретных пользователей. Намного более лакомым кусочком выглядит база данных какой-нибудь рекламной сети, откуда можно почерпнуть информацию о тысячах потенциальных мишеней.

Что со всем этим делать

Учитывая опасность, исходящую от пользовательских устройств, многие компании вынуждены жестко регулировать использование личных гаджетов на работе. Впрочем, удается это далеко всегда. Ведь, по сути компания должна начать контролировать, какими приложениями пользуются сотрудники, а за этим уследить практически невозможно.

Специалисты по безопасности со все большим скепсисом глядят на политику BYOD (Bring Your Own Device), позволяющую пользователям работать со своих личных устройств. В то время как она считается довольно прогрессивной и комфортной для сотрудников, слишком высок риск утечки данных.

Пожалуй, наиболее эффективным методом для бизнеса было бы обучение персонала хотя бы основам безопасности и сетевой гигиены. Но даже это не всегда может сработать, особенно если речь идет о персонале неайтишных специальностей. В общем, бизнесу еще предстоит найти решение проблемы утечки данных через приложения.

Что же до рядовых пользователей, то здесь ситуация вряд ли изменится. В обмен на бесплатные приложения люди все так же будут отдавать личные данные в руки посторонних, поскольку, очевидно, такая система вполне устраивает большинство пользователей.

Соціальні мережі

як чинник інформаційної безпеки

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

Упорядник Терещенко Ірина

Редактор О. Федоренко

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.