СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(29.03–13.04)

2015 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(29.03–13.04)
№ 7

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

Відповідальний редактор
Л. Чуприна, кандидат наук із соціальних комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

На конференции F8 для разработчиков приложений, работающих с Facebook, главный инженер компании М. Шропфер объявил о прорыве, совершённом в области искусственного интеллекта (ИИ). Поводом для заявления послужила работа двух систем ИИ.

Первая система способна распознать, какой из 487 различных видов спорта показан на видео. При этом, например, она отличает фигурное катание от хоккея. Неизвестно, насколько это проще или сложнее для ИИ, чем отличить кошку от собаки, но в любом случае, это очень интересная система. Уже хочется опробовать её, подсунув для распознавания фрагмент батальной сцены из «Властелина колец».

Вторая система, которой гордится СТО Facebook, умеет понимать простые предложения, в которых сообщается о неких понятиях, и затем выстраивать взаимоотношения описанных понятий.

Система выделяет из текста истории субъектов и объекты и разбирается в отношениях между ними. А поскольку в соцсетях люди общаются обычно довольно простыми предложениями, то через пару лет Facebook сможет уверенно ответить вам на вопрос, кто сколько вам должен и где вы вчера оставили ключи от машины.

Facebook уже давно пытается освоить ИИ. В начале года компания приобрела стартап Wit.AI, алгоритмы которого способны распознавать живую речь и записывать её в виде текста.

И всё это делается для того, чтобы успешнее перенаправлять пользователям сети именно тот контент, который им интересен. Ну, или чтобы было проще шпионить за всеми сразу, если вам эта цель кажется более интересной ***(Facebook распознаёт происходящее на видео и находит смысл в тексте // InternetUA (http://internetua.com/Facebook-raspozna-t-proishodyasxee-na-video-i-nahodit-smisl-v-tekste). – 2015. – 29.03).***

***

Соціальна мережа Facebook готує до використання дрони, що працюють на сонячних батареях і мають забезпечувати доступом до Інтернету сільські місцевості. Про це повідомляє The Guardian.

За словами гендиректора та засновника соцмережі, тестування відбуваються в небі Великої Британії. Безпілотники спрямовують на землю лазери, за допомогою яких забезпечують Інтернетом сільські та інші місцевості, непокриті доступом до мережі.

«Як частину нашого проекту Internet.org, що має на меті об’єднати світ, ми створили безпілотники, які можуть посилати інтернет-сигнал з неба на землю, – написав М. Цукерберг у своєму блозі. – Ми успішно завершили перший тест цих дронів у Великій Британії».

За словами гендиректора Facebook, такі літальні апарати дадуть можливість підключити до мережі всю планету, адже можуть з невеликими затратами обслуговувати 10 % населення, що живе у віддалених населених пунктах без інтернет-інфраструктури.

Ця ініціатива є частиною проекту компанії Facebook Internet.org. Вона має на меті забезпечити доступом до Інтернету ще один мільярд жителів планети. Як зауважує The Guardian, таким чином будуть створені нові ринки для соцмережі, яка нині об'єднує 1,39 млрд активних користувачів щомісяця.

Влітку Internet.org частково забезпечив Замбію вільним доступом до мобільного Інтернету.

Згідно з прогнозами дослідної компанії eMarketer, до 2018 р. половина населення світу буде онлайн.

Нагадаємо, із 4,3 млрд людей, які досі не мають доступу до Інтернету, 90 % живе у країнах, що розвиваються ***(Facebook тестує дрони, що мають забезпечувати інтернетом мешканців сіл // MediaSapiens (http://osvita.mediasapiens.ua/web/social/facebook_testue_droni_scho_mayut_zabezpechuvati_internetom_meshkantsiv_sil/). – 2015. – 29.03).***

***

Украинская аудитория социальной сети Facebook за последний год возросла на 800 тыс. человек, или на 25 %, и в марте 2015 г. составила 4 млн пользователей.

По методологии Facebook пользователями считаются люди, которые хотя бы раз в течение последних 30 дней заходили в соцсеть, будучи при этом залогинены. То есть в этой статистике не учитываются, например, зарегистрированные пользователи, которые не заходят в социальную сеть.

По данным издания Watcher, за последние шесть лет количество украинских пользователей Facebook возросло в 64 раза – с 62 тыс. в апреле 2009 г. Аудитория Facebook в Украине уже третий год подряд увеличивается на 700–800 тыс. новых пользователей ***(За год в Украине число пользователей Facebook выросло на четверть // Вся Власть (http://www.vv.com.ua/news/88453). – 2015. – 31.03).***

***

На Полтавщині створили альтернативу російським соціальним мережам

Пирятинці С. Довженко та Д. Москалець переконують, що розробили сайт, який не буде відстежуватися ФСБ. Вони вважають, що створення сайту «Укрлайф» – перший крок до популяризації українських соціальних мереж, пише 0532.ua (http://www.0532.ua/article/783340).

Ідея створити свій сайт з'явилася ще під час революційних подій на Майдані, а сам сайт запустили 18 травня 2014 р. Нині хлопці активно працюють над популяризацією інтернет-ресурсу, повідомляють «Події та коментарі».

«Ми чудово розуміли, що "ВКонтакте" та "Одноклассники" – це російські сайти, які з легкістю відстежує ФСБ. Мій товариш, Д. Москалець, дуже гарний

програміст. Ми дійшли висновку, що в Україні фактично немає популярної соціальної мережі. Ми побували на різних сайтах, подивилися відгуки і взяли до уваги всі їхні недоліки для того, щоб не повторювати подібних помилок. Дуже шкода, що адміністратори та розробники тих сайтів часто ігнорують зауваження від користувачів. Ми ж прагнемо постійного вдосконалення. Головна наша мета – це якість. Думаю, це буде з гідністю оцінено. Наш сайт постійно оновлюється, ми експериментуємо, міняємо дизайн. А головне, що це наше, українське. До того ж ми несемо відповідальність за конфіденційність листування на нашому сайті. І хоча зараз маємо лише віртуальний хостинг, але думаю, що найближчим часом створимо власні сервери, тоді це буде стовідсотковий захист від несанкціонованих втручань», – розповідають розробники соціальної мережі.

На сьогодні сайт «Укрлайф» має 276 користувачів, але молоді програмісти з Пирятина вірять, що це лише початок ***(На Полтавщині створили альтернативу російським соціальним мережам // 0532.ua (http://www.0532.ua/article/783340). – 2015. – 31.03).***

***

Twitter тестирует новый блок «Вам также может понравиться», предлагая пользователям еще больше контента для просмотра.

Редакторы Marketing Land заметили, что на страницах некоторых твитов справа появляется блок «Вам также может понравиться», предлагающий твиты, одни из которых связаны с главным постом по тематике, другие – нет.

Twitter часто обвиняют в недостаточном показателе активности пользователей на страницах соцсети. Вполне возможно, что таким образом, сервис пытается повысить показатель вовлеченности ***(Twitter тестирует блок с рекомендуемыми твитами // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_testiruet_blok_s_rekomenduemymi_tvitami). – 2015. – 31.03).***

***

Twitter выпустил новый медиа-инструмент под названием Curator, который предназначен для отображения потока релевантных твитов и видео Vine за пределами социальной сети – во время передач и сюжетов по всему Интернету и на мобильном телевидении. Контент будет добавляться на сайты в режиме реального времени. Сообщается, что Curator позволит издателям фильтровать твиты по хэштегам, авторам, количеству подписчиков и языку. Об этом пишет searchengines.ru

Новый инструмент поможет Twitter в построении самой большой ежедневной аудитории. Издатели представляют собой значительную группу пользователей сервиса микроблогов, которые распространяют самый привлекательный контент платформы – последние новости и события в реальном времени.

Некоторые сторонние партнеры, такие как Flowics, Spredfast и Storify Livefyre, уже предлагают платные сервисы по размещению твитов на экранах телевизоров, например, во время игры в баскетбол в прямом эфире. В Twitter утверждают, что новый инструмент будет бесплатным, но урезанным вариантом этих продуктов.

В IV квартале 2014 г. рост пользовательской аудитории сервиса замедлился. Компания сообщила о всего лишь 288 млн активных пользователей в месяц, что только на 2 % выше по сравнению с 284 млн в Q3 2014 г. По мнению руководства компании, низкий темп роста аудитории сервиса по результатам IV квартала 2014 г. – эпизодическое явление. В течение ближайших кварталов показатели должны подняться ***(Twitter запускает инструмент Curator для размещения твитов на медиа-сайтах // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42944/118/lang,ru/). – 2015. – 1.04).***

***

YouTube внедрил автопроигрывание рекомендованных видео в десктопной версии сервиса. Новая опция установлена по умолчанию. Её запуск призван увеличить количество просмотров видеороликов в рамках видеохостинга.

Нововведение означает, что после просмотра видео пользователям будет показан релевантный ролик, подобранный исходя из их истории просмотров. Его воспроизведение будет начато автоматически.

В последнее время отрасль наблюдает за усилением конкуренции между YouTube и Facebook. Недавно социальная сеть заявила, что количество просмотров видео в её рамках составляет более 3 млрд в день. YouTube в последнее время не предоставлял такой статистики, но в 2012 г. компания сообщала о 4 млрд просмотров видео в день.

По данным аналитической компании Socialbakers за январь 2015 г., большинство брендов загружают видео напрямую в Facebook, минуя YouTube. В этом контексте запуск автоматического воспроизведения видео может рассматриваться как конкурентоспособный ответ, призванный укрепить позиции видеохостинга на рынке. Пользователи могут отключить автопроигрывание, нажав на кнопку-переключатель в правом верхнем углу страницы видео.

YouTube также выпустил ролик, демонстрирующий работу новой опции.

Тестирование автоматического проигрывания рекомендованных видео проходило с конца 2014 г. ***(YouTube запустил автопроигрывание рекомендованных видео // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/youtube_zapustil_avtoproigryvanie_rekomendovannyh_video). – 2015. – 31.03).***

***

Анонсы и слухи создают впечатление, что Facebook прокладывает маршрут к мировому онлайн-господству.

Messenger – больше не приложение

Не успели улечься страсти вокруг того, что Facebook заставляет пользователей скачивать Messenger отдельным мобильным приложением, как выяснилось, что он вовсе и не приложение! На мартовской конференции для разработчиков f8 представители Facebook называли Messenger не иначе как платформой, пишет Lenta.ru.

Во-первых, разработчики теперь могут создавать сторонние приложения для Messenger. Пользователи же с их помощью получили возможность обмениваться не только текстом, фото и стикерами, но и «гифками», аудиоклипами и другим контентом, а также устанавливать новые приложения напрямую из мессенджера.

Кроме того, разработчики смогут встраивать кнопку Messenger в свои приложения – например, если пользователь купил онлайн-билет в кино, он может сразу рассказать об этом другу.

Однако наиболее интересная история – Messenger Business. Идея в том, что бренды получают прямой и личный канал для общения с покупателем. Если пользователь совершает покупку на сайте, а через Messenger получает информацию о статусе заказа и доставке или заказывает столик в ресторане, то для бизнеса это означает возможность перевести всю службу поддержки клиентов на платформу Facebook, избавившись от колл-центров.

Что это значит для Facebook? Очевидно – новые каналы для монетизации. Этот вопрос – один из главных для инвесторов соцсети, чья выручка сейчас почти полностью полагается на рекламу. Как минимум Facebook сможет запустить новые форматы рекламы приложений, а модели коммерческого сотрудничества в рамках Messenger Business практически не ограничены.

Что это значит для пользователей? Во-первых, почти наверняка в Messenger появятся платные функции, пусть даже в формате сторонних приложений. Разговоры о платных стикерах шли давно, но Facebook пошел дальше, – не исключено, что поделиться каким-то типом контента бесплатно не удастся. Кроме того, изменится само понимание личных сообщений: коммуникация с брендами явно отличается по содержанию от дружеских диалогов.

Facebook как глобальное издательство

Для издателей, размещающих на сайтах плагины Facebook для комментариев, новостью стало решение соцсети транслировать эти комментарии на их страницы. В результате если пользователь прокомментировал статью на Huffington Post, его комментарий увидят друзья по соцсети вне зависимости от того, видели ли они статью и подписаны ли на страницу издания.

Однако, как это часто бывает, в отношениях Facebook со СМИ более интересны недавние слухи. Газета The New York Times недавно сообщила, что

Facebook хочет перенести на свою платформу статьи из газет и журналов, чтобы уменьшить время загрузки контента. С одной стороны, эта информация пока не подтверждена, с другой – сама NYT названа в числе вероятных партнеров Facebook по новой инициативе.

Facebook давно вынашивает идею стать для своей аудитории новостным хабом. В настоящее время пользователи соцсети могут поделиться анонсами и ссылками на интересную статью и даже сохранить эти ссылки в список для чтения. Однако соглашение со СМИ о новом формате превратит соцсеть в самостоятельную издательскую платформу, – пользователям не придется переходить на сайт издания, чтобы прочитать свежий номер.

Пока не известно, планирует ли Facebook размещать полнотекстовые статьи (наиболее предпочтительный для соцсети вариант) или это будут развернутые анонсы либо модифицированные версии материалов.

Напомним, что крупнейшая российская соцсеть «ВКонтакте» в 2012 г. создала похожий механизм, – пользователи могут читать статьи из СМИ по ссылкам друзей, без перехода на другие сайты.

Что это значит для Facebook? Конечно, соцсеть выходит на переговоры с позиции силы, – для многих СМИ Facebook является бесценным источником трафика и обратной связи с читателем. Однако важно и то, что заставив СМИ размещать статьи на своей платформе, Facebook многократно увеличит время пребывания пользователей на сайте, а как следствие – и свои рекламные тарифы.

Что это значит для издателей? Очевидно – потерю рекламных доходов и доходов от подписки. Хотя, по слухам, Facebook планирует делиться с партнерами рекламной выручкой. Возможно – размывание медиабренда, ведь говоря о новой статье, пользователь заявит, что прочитал ее не в газете, а на Facebook. Но есть и положительная сторона: мелкие СМИ получат охват аудитории, о которой вряд ли могли мечтать.

Что это значит для пользователей? Facebook продвигает идею экономии трафика и времени на загрузку статей со сторонних серверов, что важно для пользователей мобильных устройств. Но есть и другая мотивация: социальная сеть уходит от самого понятия социальности, пресловутого user-generated content.

Контент, создаваемый одними пользователями для других, – это вполне рабочая модель для обычного онлайн-сервиса. Однако для одной из крупнейших в мире публичных компаний этого явно недостаточно: соцсеть хочет стать полноценным медиапорталом. Сможет ли пользовательский контент конкурировать с профессиональными репортажами National Geographic или популярными подборками с Buzzfeed – большой вопрос.

Видео с телепортацией

Продолжая идею соцсети как медиапортала, Facebook анонсировала несколько важных нововведений относительно видеоконтента. Во-первых, это плагин для вставки загруженных на Facebook видеороликов на сторонние

сайты. Ничего не напоминает? Правильно, соцсеть передала вполне однозначное сообщение YouTube.

Во-вторых, анонсирована поддержка трехмерного видео в ленте новостей. Трехмерные видео будут доступны для очков дополненной реальности Oculus Rift, – точки обзора меняются при повороте головы. В компании нововведение называют функцией «телепортации».

В более ограниченном варианте такую функцию уже тестирует тот же YouTube: при просмотре некоторых видеороликов можно переключаться между различными точками, с которых велась съемка.

Что это даст Facebook? Скорее всего, соцсеть будет внедрять в ролики видеорекламу, а доходами делиться с сайтами, которые встраивают их в свой контент. Не случайно на F8 представители компании объявили, что клиенты принадлежащей ей сети для размещения видеорекламы LiveRail получат доступ к данным пользователей соцсети.

В свою очередь, сферические видео – заявка на инновационность и интеграция технологий ранее приобретенной компании Oculus VR со своим основным продуктом. Не стоит списывать со счетов и вовлеченность молодой аудитории, с которой у Facebook в последнее время не ладится.

Что получат пользователи? Больший охват для собственного видеоконтента, который, однако, должен быть достойным перепоста на сторонних ресурсах. Это еще один звоночек от Facebook как новостной платформы, – профессиональные СМИ нередко обращаются к пользовательскому контенту, освещая происшествия, стихийные бедствия и другие события, где важны свидетельства очевидцев. Ну и 360-градусные ролики должны стать принципиально новым опытом для пользователей.

Подводя итог, можно сказать, что глобальные приоритеты Facebook лежат в сфере бизнеса, профессионального контента и популяризации видео. К первому десятилетию работы в прошлом году Facebook подошла как мобильная платформа для всевозможных коммуникаций: почти 86 % глобальной аудитории соцсети в 1,4 млн пользователей – мобильные. Не исключено, что второй юбилей Facebook отметит как медиапортал с диверсифицированными источниками монетизации.

Однако эта траектория не может не напомнить другую историю из мира Интернета – взлеты и падения MySpace. Начав как соцсеть, которую на повороте обошла сама Facebook, MySpace попытался найти источник развития в развлекательном контенте. Успешным начинание назвать можно с большой натяжкой. Хочется верить, что Facebook в попытках оправдать ожидания инвесторов и реализовать амбиции глобального контент-хаба не забудет о главном: более чем миллиарде пользователей, для которых социальная сеть – одна из важнейших площадок для общения ***(«Фейсбук» намерен стать YouTube, газетой и колл-центром 3 // Хартия'97 (http://www.charter97.org/ru/news/2015/4/2/145855/). – 2015. – 2.04).***

***

Подразделение по сторонним проектам Facebook Creative Labs выпустило приложение для общения с помощью видео под названием Riff, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-vypustil-prilozhenie-dlja-kollektivnyh-video-43837/).

В нём можно опубликовать 20-секундный ролик с названием и тегами. Друзья пользователя, у которых тоже установлен Riff, получают уведомление о публикации. Они могут ответить своим 20-секундным роликом, уведомление о котором получат их друзья. Последние также могут ответить на первое видео своей записью. Такое расширение может происходить любое количество раз. Видео в одной теме воспроизводятся одно за другим. Таким образом из них, например, можно составить одну историю

The Verge отмечает, что Riff подходит для вирусных кампаний формата ALS Ice Bucket Challenge, в которых каждый участник связан с будущим или предыдущим участником. Классические социальные медиа (например, YouTube или Vimeo) для этого не подходят, поскольку на них видео таких кампаний выглядят разрозненными. В настоящее время Riff доступен для iOS и Android ***(Facebook выпустил приложение для коллективных видео // Marketing Media Review (http://mmr.ua/news/id/facebook-vypustil-prilozhenie-dlja-kollektivnyh-video-43837/). – 2015. – 2.04).***

***

Сервис микроблогов Twitter запустил новый способ ретвитов, при котором пользователи получают больше пространства для собственных комментариев. Об этом сообщает Cnet.

Около пяти лет назад в популярном сервисе микроблогов появилась специальная кнопка для цитирования записей друзей, но некоторые пользователи сервиса до сих пор предпочитают старый стиль ретвитов. Он также не лишен недостатков – чтобы уложиться в 140 символов, зачастую приходится сокращать цитируемое сообщение. Новая функция Twitter объединяет преимущества обоих способов.

Вместо дословного цитирования, новый метод вставляет в запись пользователя только ссылку на оригинальный твит, оставляя все пространство под собственный комментарий. Оригинальная запись при этом остается без изменений, и независимо от ее длины, для выражения собственных мыслей доступно 116 символов. Сторонние пользователи видят запись целиком в виде карточки, словно это прикреплённое изображение или видео.

Новая функция доступна для пользователей веб-версии Twitter и в официальном приложении для iPhone. В клиенте для Android такие публикации отображаются в правильном формате, однако поддержка самой функции появится лишь в будущих обновлениях программы.

До этого в Twitter использовалась другая схема цитирования: текст оригинального твита заключался в кавычки, а пользователь мог дописать к

нему всё, что пожелает. Но чем длиннее оригинальная запись, тем меньше места оставалось для комментария.

Первые испытания нового режима цитирования в Twitter проводились летом прошлого года ***(Twitter запустил новый способ комментирования сообщений при ретвитах // InternetUA (http://internetua.com/Twitter-zapustil-novii-sposob-kommentirovaniya-soobsxenii-pri-retvitah). – 2015. – 7.04).***

***

Facebook запустил новую функцию, позволяющую подписываться на мероприятия, созданные конкретными компаниями, страницами или группами.

В разделе «Мероприятия» появилась кнопка «Подписаться». Если раньше пользователи были вынуждены регулярно проверять наличие новых мероприятий или ждать приглашений от друзей – теперь для этого есть специальный функционал. Благодаря этому нововведению пользователи также смогут следить за событиями, на которые они подписались.

Это приятный бонус не только для рядовых пользователей, но и для администраторов страниц. Если пользователь подписан на мероприятия сообщества, то он точно узнает о предстоящем событии, и алгоритм новостной ленты Facebook не сможет ему в этом «помешать» ***(Facebook поможет не пропустить важные мероприятия // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_pomozhet_ne_propustit_vazhnye_meropriyatiya). – 2015. – 8.04).***

***

Бесплатное приложение для обмена фотографиями и видеозаписями Instagram не устает радовать своих пользователей. На этот раз они представили две новые функции для обработки снимков – Fade («Тусклый») и Color («Цвет»).

С помощью Color можно регулировать светлые и темные оттенки фотографии.

Фильтр Fade поможет сделать цвета фотографии более мягкими. Для обработки будут доступны ключевые цвета: оранжевый, красный, зеленый, синий, розовый, желтый, фиолетовый и голубой.

Обновление будет представлено 8 апреля для пользователей операционной системы Android и в течение нескольких дней – для iOS ***(Instagram запустил два новых инструмента для обработки фото // Mainpeople.ua (http://mainpeople.ua/mpnews/celebrities/instagram-zapustil-dva-novyh-instrumenta-dlya-obrabotki-foto). – 2015. – 8.04).***

***

Компания Facebook запустила веб-версию мессенджера, о разработке которой стало известно еще в прошлом году. Используя браузер, пользователь может общаться с помощью Messenger на компьютере так же, как и на смартфоне. Все сообщения будут синхронизироваться – то есть переписка на

компьютере будет отражена в мобильном приложении, а переписка в приложении – на компьютере.

Для пользователей из России сервис пока что предлагает скачать приложение для iOS и Android. Однако, как выяснили пользователи, если зайти по прямой ссылке messenger.com/login, то можно войти в приложение с помощью своего логина и пароля от Facebook. Также в сервисе есть кнопки для обычного и видеозвонка, но эта функция пока что не доступна.

В марте в рамках конференции F8 соцсеть анонсировала значительное изменение в проекте Messenger. Из обычного мессенджера сервис решили превратить в платформу для интеграции сторонних приложений. Инструменты, которые Facebook предоставит разработчикам, помогут им внедрить использование некоторых функций прямо из Messenger – например, съемку фотографий или видеороликов. Ранее Facebook включила в мессенджер функцию денежных переводов.

В минувшем году этим приложением для обмена мгновенными сообщениями и видео пользовались 700 млн участников соцсети ***(Facebook запустила веб-версию своего мессенджера // InternetUA (http://internetua.com/Facebook-zapustila-veb-versiua-svoego-messendjera). – 2015. – 10.04).***

***

Twitter явно недолюбливает пользователей Android

Android – самая популярная и распространенная мобильная операционная система в мире, которая практически захватила весь рынок смартфонов. В Google Play больше приложений, чем в любом другом виртуальном магазине, и мы знаем, что покупая смартфон на Android, мы сможем ни в чем себе не отказывать. Или нет? Похоже, что последнее утверждение не до конца правдиво, и популярный сервис микроблогов Twitter в очередной раз это доказал.

Совсем недавно в Twitter появилась новая функция, которая выводит ретвиты на совершенно другой уровень.

Судя по комментариям, пользователи тепло встретили новую функцию и готовы активно ее использовать. Эта функция уже заменила обычные ретвиты в веб-версии Twitter и в приложении для iPhone, а вот пользователи Android новую функцию не получили, и дата выхода обновления неизвестна.

Любопытно то, что за последние несколько недель Twitter уже несколько раз проигнорировал популярность Android. Обновление Vine с поддержкой видео высокого качества прошло мимо Android, новый сервис Pericsope, которым активно пользуются в редакции ресурса, тоже не вышел на Android, зато пользователи iPhone радуются новинкам прямо в эти минуты.

Нам известны случаи, когда разработчики платных приложений не выпускали обновление для Android по той причине, что мобильная ОС от Google приносит недостаточно дохода из-за развитого пиратства на платформе.

Но по какой причине Twitter не торопится выпускать свои бесплатные сервисы для наших читателей – это остается загадкой.

Единственным подходящим объяснением является низкая активность пользователей Android. Многочисленные данные и исследования подтверждают, что, несмотря на огромное количество пользователей Android, далеко не все из них используют Интернет и приложения. В свою очередь пользователи iPhone значительно более активны. Но важно не это. Важно то, что покупая смартфон на Android, мы не можем быть уверены в том, что он будет поддерживать все современные сервисы и приложения ***(Twitter явно недолюбливает пользователей Android // InternetUA (http://internetua.com/Twitter-yavno-nedoluablivaet-polzovatelei-Android). – 2015. – 9.04).***

***

Google запатентовала систему блокировки спойлеров в социальных сетях

У каждого из нас есть такой знакомый, который постоянно говорит: «А я уже видел этот фильм. Там в конце главного героя убивают». Подобные высказывания в народе называют «спойлерами», когда один человек рассказывает другому детали какого-либо произведения, намеренно или случайно раскрывая важные сюжетные детали, тем самым лишая собеседника удовольствия от личного знакомства с фильмом, книгой, игрой или телесериалом. Похоже, что в компании Google серьёзно обеспокоены этим явлением, так как они запатентовали способ борьбы с любителями «спойлерить».

Новый патент поискового гиганта был замечен сотрудниками портала Quartz. В патенте кратко изложен принцип работы некоей интеллектуальной системы, которая потенциально может быть встроена в любую социальную сеть вроде Facebook или «ВКонтакте». Её суть заключается в том, что пользователи отмечают книги и фильмы, с которыми они собираются ознакомиться в ближайшее время или уже дочитали/досмотрели до конца. В случае с сериалами, человек отмечает уже просмотренные серии.

После активации защиты от спойлеров, умная система автоматически находит и прячет от вас сообщения от людей, которые содержат информацию о фильмах, книгах и сериях телешоу, до которых вы пока не добрались. В случае, если система обнаруживает намёк на спойлер в сообщении, она замазывает его с помощью эффекта blur. При этом вы можете снять эту защиту и прочесть сообщения в обход системы в любой момент. Похоже, что если эта система найдёт применение в социальных сетях, любителям портить другим людям впечатления от разного рода произведений станет жить чуточку сложнее ***(Google запатентовала систему блокировки спойлеров в социальных сетях // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/google-zapatentovala-sistemu-blokirovki-s.html). – 2015. – 10.04).***

***

Рейтинг популярных сайтов за I квартал 2015 г.

По данным исследования CMeter компании TNS, список самых популярных сайтов среди украинских интернет-пользователей в I квартале возглавляют Vk.com, Google.com.ua, Youtube.com, пишет Marketing Media Review (http://mmr.ua/news/id/rejting-populjarnyh-sajtov-za-i-kvartal-2015-goda-43941/).

В целом в I квартале снизились охваты (средненедельные и накопительные за месяц) сайтов odnoklassniki.ru и kinopoisk.ru.

Также в феврале наблюдалось увеличение интереса к информационным сайтам, таким как tsn.ua, segodnya.ua, obozrevatel.com, korrespondent.net, pravda.com.ua, unian.net, censor.net.ua. Однако в марте охватные показатели этих сайтов вернулись к январским значениям ***(Рейтинг популярных сайтов за I квартал 2015 года // Marketing Media Review (http://mmr.ua/news/id/rejting-populjarnyh-sajtov-za-i-kvartal-2015-goda-43941/). – 2015. – 10.04).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Администраторы крупнейших харьковских интернет-пабликов договорились о сотрудничестве в условиях информационной войны. Соответствующий меморандум был подписан на закрытом круглом столе 4 апреля, сообщили «SQ» организаторы.

В круглом столе приняли участие представители самых авторитетных и охватывающих наибольшую аудиторию интернет-ресурсов Харькова: «Харьковфорум», «Типичный Харьков», IT-Sector, «Харьков 1-я столица», «Харьков LIVE», MyKharkov.info, «Ху**ый Харьков», «Харьков City».

Участники обсудили актуальные вопросы, с которыми сталкиваются в своей деятельности ежедневно: пропаганда и фейки, проверка достоверности информации, борьба с платными «троллями» и «ботами», продвижение паблика, вовлечение пользователей, создание «вирусных» постов.

Одной из серьезных проблем, по словам администраторов, является пророссийская пропаганда, которая проявляется в сообщениях так называемых «троллей»: в комментариях появляются тысячи идентичных сообщений, написанных от имени разных людей. «Боты» провоцируют или даже «разыгрывают» конфликты между пользователями, в том числе с помощью намеренных оскорблений на национальной почве.

«Создание единых правил работы и определение обязательств и ответственности администраций интернет-площадок могут стать залогом

поддержания мира и спокойствия в Харькове», – уверены в Фонде «Мир и порядок», который выступил инициатором и организатором круглого стола.

«Мы поддержали инициативу: сотрудничать в интересах города и страны – это то, что нам необходимо. Кроме того, одним из аспектов соглашения является взаимное обучение и взаимопомощь. Встреча прошла очень конструктивно, все настроены на позитивный рабочий лад. Мы все работаем на благо нашего города и надеемся, что сотрудничество приведет к ощутимым результатам», – подчеркнула сооснователь и главный координатор IT-Sector В. Думенко.

Основной лейтмотив меморандума, который подписали участники, – ответственность администраторов за содержание пабликов, противостояние попыткам раскола общества, борьба с дискриминацией и деструктивной пропагандой, а также координация дальнейшей деятельности на благо интернет-пользователей Харькова.

Справка «SQ». Паблики – публичные страницы в социальных сетях, ориентированные на жизнь города и городские новости ***(Шевченко М. Крупнейшие харьковские паблики договорились об общей политике в соцсетях // STATUS QUO (http://www.sq.com.ua/rus/news/obschestvo/06.04.2015/krupnejshie_harkovskie_pabliki_dogovorilis_ob_obschej_politike_v_socsetyah/). – 2015. – 6.04).***

***

«Канцелярская сотня», которая занималась расшифровкой документов, найденных в Межигорье, запустила очередной антикоррупционный проект. Волонтеры создали сайт declarations.com.ua: на котором отныне будут публиковать декларации о доходах министров, прокуроров, судей, депутатов и других чиновников. В настоящее время на сайте уже 2500 деклараций, и он продолжает активно наполняться, пишет AIN.UA (http://ain.ua/2015/04/02/573268).

Как рассказывает основатель «Канцелярской сотни» Д. Бигус, проект вырос из январской идеи, когда волонтеры в Facebook расшифровали по несколько деклараций каждый. Работа над проектом продолжалась три месяца. Всех желающих помочь проекту команда призывает поучаствовать в его заполнении – на одну декларацию уходит от пяти минут до пары часов. Для этого нужно залогиниться на сайт через Facebook (через кнопку «Долучитись до розшифровки»).

Информацию с сайта может брать любой – API открыт. По словам Д. Бигуса, уже есть договоренность с несколькими министерствами о централизованной подаче деклараций. Но пока это не работает, каждый может подать линки на pdf-файлы с декларациями с официальных сайтов и они попадут в обработку.

«С новыми инструментами у нас есть все шансы получить полный официальный срез доходов и имущества чиновников. А потом мы “залинкуем” поиск с “ГарнойХатой”», – пишет Д. Бигус.

Напомним, «Гарна Хата» – это антикоррупционный проект об элитарной недвижимости и ее владельцах, который «Канцелярская сотня» запустила в феврале этого года ***(«Канцелярская сотня» запустила сайт, где публикуются все декларации чиновников // AIN.UA (http://ain.ua/2015/04/02/573268). – 2015. – 2.04).***

***

Официальные аккаунты Министерства иностранных дел Украины в социальных сетях работают под логотипами крымскотатарского телеканала ATR, который прекратил вещание на полуострове из-за отказа Роскомнадзора в регистрации, сообщает Крым.Реалии.

В частности, логотипы первого крымскотатарского телеканала размещены на главных страницах украинского МИДа в Twitter и Facebook ***(МИД Украины в социальных сетях работает под логотипом ATR // MIGnews.com.ua (http://mignews.com.ua/sobitiya/inukraine/5302612.html). – 2015. – 6.04).***

***

Суд разрешил оформить развод через Facebook

Бюрократия в той или иной форме проявления является больным местом управляющих органов многих стран мира. Она не только тормозит развитие самих стран, но попутно успевает портить жизнь обычным гражданам. Яркий пример того, как стоит обходить устоявшиеся бюрократические процедуры, был показан Верховным судом Манхэттена, который в ходе разбирательства дела о разводе разрешил американке отправить соответствующие уведомления мужу… через Facebook.

Как сообщает New York Daily News, Верховный суд посчитал этот способ единственным, который может иметь какой-либо эффект. Узнать настоящее местонахождение мужа американки не представляется возможным: с 2011 г. он не имеет постоянного места жительства, но при этом иногда пользуется социальными сетями.

Женщина нанимала частного детектива, но даже он не помог выследить неуловимого мужа. По этой причине суд вошел в положение истца и постановил, что через ее учетную запись в Facebook адвокат должен еженедельно отправлять мужу документы на развод. Это будет продолжаться в течение трех недель либо до получения подтверждения от супруга. Первое сообщение, кстати, уже было отправлено, но какого-либо ответа от своего мужа жительница Бруклина так и не получила.

И хотя данный случай является исключением из правил, прецедент уже создан, а в подобных делах он может играть очень весомую роль. Поэтому можно ожидать, что это первый, но не последний случай, когда в рамках судебного разбирательства разрешено прибегать к помощи социальных сетей ***(Суд разрешил оформить развод через Facebook // InternetUA***

(http://internetua.com/sud-razreshil-oformit-razvod-cserez-Facebook). – 2015. – 8.04).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

В Китае, где социальная сеть Facebook запрещена, компания пытается нарастить усилия, чтобы заработать деньги, пишет «Зеркало недели. Украина» (http://zn.ua/TECHNOLOGIES/facebook-nameren-privlech-reklamodateley-iz-kitaya-171324_.html).

Компания Facebook намерена развить в Китае кампанию, которая поможет привлечь рекламодателей, сообщает The Wall Street Journal.

При этом цель кампании – убедить рекламодателей, что 1,39 млрд активных пользователей могут принести выгоду, несмотря на запрет на пользование Facebook в самом Китае.

Facebook ищет больше клиентов, таких как Youzu Interactive Co. – шанхайский разработчик онлайн-игр. Компания Youzu после размещения рекламы в Facebook за 10 млн юаней (1,6 млн дол.) в два раза увеличила количество ежедневно играющих пользователей.

Facebook не раскрывает информацию о выручке, которую она получает от Китая. Но аналитики считают, что китайских рекламодатели играют все большую роль для компании в сегменте рекламных доходов из Азии. Так, в IV квартале 2014 г. выручка из Азии от рекламодателей составила 531 млн дол., что на 67 % больше по сравнению с предыдущим годом ***(Facebook намерен привлечь рекламодателей из Китая // Зеркало недели. Украина (http://zn.ua/TECHNOLOGIES/facebook-nameren-privlech-reklamodateley-iz-kitaya-171324_.html). – 2015. – 31.03).***

***

«ВКонтакте» предоставит информацию об охвате и эффективности каждого сообщения, которое было опубликовано в сообществе. Об этом lenta.ru сообщил пресс-секретарь соцсети Г. Лобушкин. Нововведение уже доступно администраторам пабликов, которые перешагнули отметку 10 тыс. подписчиков, с 31 марта, пишет Marketing Media Review (http://mmr.ua/news/id/vkontakte-ocenit-effektivnost-kazhdogo-posta-v-pablikah-43807/).

«Запуск нового инструмента – это значительный шаг в сторону превращения сообществ “ВКонтакте” в полноценные медиа», – сказал «Ленте.ру» Г. Лобушкин. Он отметил, что нововведение будет запускаться в несколько этапов. На первом этапе администраторы сообществ получат доступ к веб-интерфейсу нового инструмента, а на втором – к данным через API. «В дальнейшем мы подумаем о том, чтобы дать возможность смотреть статистику

не только записей сообществ, но и в личных профилях», – добавил Г. Лобушкин.

На странице к каждой записи будут отображаться данные о количестве взаимодействий с ней. Эта информация включает в себя число отметок «Мне нравится», репостов, комментариев, переходов по ссылке, которая была опубликована в тексте сообщения или в качестве сниппета, переходов в сообщество из записи, вступивших в сообщество из записи, количество жалоб на публикацию. Также можно посмотреть число пользователей, скрывших конкретную запись из новостной ленты, общее количество таких записей. Помимо этого соцсеть подсчитает и суммарный охват публикации – это все пользователи, которые увидели запись (но не являются подписчиками сообщества) вместе с числом вступивших в группу.

По данным компании, на сообщества и новостную ленту приходится около половины всех просмотров, совершаемых пользователями в соцсети ***(«ВКонтакте» оценит эффективность каждого поста в пабликах // Marketing Media Review (http://mmr.ua/news/id/vkontakte-ocenit-effektivnost-kazhdogo-posta-v-pablikah-43807/). – 2015. – 31.03).***

***

Mail.ru Group хочет полностью консолидировать продажи рекламы внутри себя и может отказаться от эксклюзивного сотрудничества с селлером видеорекламы Gazprom Media Digital (GPMD, входит в холдинг «Газпром-медиа»). Об этом vedomosti.ru рассказал сотрудник компании-владельца авторских прав, а человек, близкий к Mail.ru Group, это подтвердил.

Окончательное решение еще не принято, уточняет второй собеседник «Ведомостей», но, скорее всего, сотрудничество с GPMD прекратится, так как группа постепенно переводит продажи рекламы на себя. Тем более что Mail.ru Group, по его словам, не очень довольна тем, как монетизируются видеоролики на ее ресурсах.

GPMD продает рекламу не на всех ресурсах Mail.ru Group, а в основном в социальной сети «ВКонтакте»: с ней селлер еще в 2013 г. заключил эксклюзивный контракт. Также GPMD монетизирует часть видеороликов в «Одноклассниках», но это небольшая ниша и речь там идет в основном о пользовательском контенте, говорит близкий к группе человек.

Представители Mail.ru Group и GPMD отказались от комментариев. А представитель «ВКонтакте» Г. Лобушкин сказал, что пока соцсеть не отказывается от сотрудничества с GPMD. Контракт «ВКонтакте» и GPMD действует до конца года, он не был пересмотрен, говорит человек, близкий к участникам переговоров между этими компаниями.

С точки зрения аудитории «ВКонтакте» – крупнейшая рекламная площадка для GPMD, следует из данных TNS. В феврале 2015 г. аудитория видеороликов «ВКонтакте», в которых GPMD продает рекламу, составила, по данным TNS, 24,6 млн пользователей. Если учитывать аудиторию самых крупных площадок GPMD, то тех, кто смотрел в феврале видео во «ВКонтакте»

и мог увидеть в нем рекламу от GPMD, оказалось16,9 млн пользователей, говорит руководитель интернет-проектов «TNS Россия» И. Ишунькина. Не реже раза в день ролики «ВКонтакте» смотрели 4 млн пользователей из 5,9 млн, составляющих ежедневную аудиторию площадок GPMD. А по показам доля «ВКонтакте» во всех роликах, где могла быть реклама GPMD, составляла в феврале почти 80 %, следует из данных TNS.

Сколько «ВКонтакте» зарабатывает на видеорекламе, неизвестно. Топ-менеджер крупной рекламной группы оценивает продажи GPMD во «ВКонтакте» в 2014 г. в пределах 500 млн р. Вся выручка соцсети в этот период составила 4,3 млрд р.

Mail.ru Group стала владельцем 100 % «ВКонтакте» в сентябре 2014 г. и постепенно перевела продажи всей рекламы, кроме видео, под свой контроль. Например, группа отказалась от сотрудничества с крупнейшим селлером рунета IMHO Vi, который продавал рекламу в приложениях «ВКонтакте» через платформу «Креара медиа». Mail.ru Group заявила, что будет сама искать рекламодателей на медийные форматы рекламы (баннеры и др.) во «ВКонтакте».

Кроме того, в феврале этого года Mail.ru Group объявила о создании единой платформы мобильной рекламы MyTarget: она позволяет достучаться до аудитории трех крупнейших российских соцсетей – «ВКонтакте», «Одноклассники» и «Мой мир».

Продажи рекламы не должны зависеть от другого крупного участника рынка и переход на собственные продажи видеорекламы – стратегически правильный ход, уверен человек, близкий к Mail.ru Group. Но решение этого вопроса не быстрое, тем более что, отказавшись от сотрудничества с GPMD, «ВКонтакте» может потерять доступ к части легального контента «Газпром-медиа», замечает он.

Взять под контроль продажи видеорекламы особенно уместно, когда продажи баннеров падают и нужно сконцентрироваться на растущих сегментах – видео- и мобильной рекламе, рассуждает топ-менеджер крупной рекламной группы. Да и сама GPMD в кризис больше заинтересована в продаже рекламы на площадках холдинга «Газпром-медиа», считает он. Другое дело, что «Газпром-медиа» нужна «ВКонтакте» как источник легального контента – прежде всего это телеканал ТНТ, который дает инвентарь для большей части лицензионного контента в соцсети, продолжает собеседник «Ведомостей» ***(Mail.ru Group хочет сама продавать видеорекламу во «ВКонтакте» // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42924/118/lang,ru/). – 2015. – 31.03).***

***

Facebook ведёт переговоры с несколькими издателями контента, включая Vox, Vice и The Onion, по поводу создания коротких спонсируемых

видеороликов, которые будут публиковаться напрямую в Facebook. Новый проект для рекламодателей получил название Anthology.

Facebook хочет наполнить свою новостную ленту высококачественными видео. Это даст компании возможность заработать ещё больше на видеорекламе. Путём повышения качества видео социальная сеть также хочет сделать просмотр рекламы более комфортным для пользователей.

По данным The Information, Facebook и его контент-партнёры в ближайшие недели попытаются убедить рекламодателей проспонсировать эти видео. Запуск роликов ожидается позже в этом году.

Компания намерена раскрыть больше деталей проекта Anthology во время конференции NewFronts, которая состоится в апреле.

В течение последнего года количество репостов видео в Facebook росло огромными темпами. В январе компания представила статистику, которая показала увеличение количества видео, публикуемого одним пользователем платформы, до 94 %. Кроме того, 50 % пользователей Facebook в США просматривают, по меньшей мере, одно видео в день.

Проект Anthology – ещё один знак того, что компания всё больше внимания уделяет видео в социальной сети, при этом оказывая конкурентное давление на YouTube ***(Facebook наполнит ленту высококачественными спонсируемыми видео // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_napolnit_lentu_vysokokachestvennymi_sponsiruemymi_video). – 2015. – 2.04).***

***

Переход торговли, финансовых сервисов и других услуг в онлайн-пространство провоцирует создание новых способов идентификации личности в сети. Вместо традиционных паспортов, водительских прав, или именных платежных карт специалисты предлагают использовать профили в социальных сетях.

Британская компания Veridu разработала программу авторизации клиентов для финучреждений и ритейлеров, которые специализируются на онлайн-сервисах.

Эта программа позволит не только идентифицировать существующих клиентов по их профилям в социальных сетях, но и оценивать риски, связанные с предоставлением того или иного сервиса потенциальному потребителю на основе указанной им информации.

Р. Грот, основатель и генеральный директор Veridu, утверждает, что профили социальных медиа могут обеспечить более надежный уровень проверки клиента, чем сканы документов, котоые легко подделать.

Сначала ритейлер, или онлайн-банк должен установить программу Veridu на свой сайт. После этого он сможет предлагать потенциальным клиентам регистрироваться в системе, или входить в свой аккаунт через социальные сети (например, Facebook, Twitter и LinkedIn).

Система оценки профилей Veridu использует 100-бальную систему. Теоретически, более высокий балл означает, что потенциальный клиент является кредитоспособным. Ниже 50 баллов означает недостаточную надежность пользователя.

Для того, чтобы просто зарегистрироваться на торговой площадке, необязательно иметь высокую кредитоспособность. Однако для того, чтобы получить какую-либо услугу в банке, авторизировавшись через Facebook, необходимо, чтобы профиль как можно более точно и правдиво отображал информацию о клиенте ***(Соцсети станут онлайн-паспортами // InternetUA (http://internetua.com/socseti-stanut-onlain-pasportami). – 2015. – 2.04).***

***

Три факта об Instagram, о которых вы могли не знать

В декабре 2014 г. стало известно, что количество зарегистрированных в Instagram пользователей превысило 300 млн. Соцсети удалось обойти Twitter, число пользователей которого равнялось на тот момент примерно 288 млн. Эти два факта обратили пристальное внимание маркетологов всего мира на Instagram, а также послужили причиной проведения многочисленных исследований. Давайте рассмотрим несколько наиболее любопытных открытий.

1. Пользователи Instagram любят покупать

Маркетологи начали радостно хлопать в ладоши, когда исследования показали, что многие пользователи используют Instagram как канал для совершения покупок. Они расшаривают посты брендов, комментируют, делятся мнениями насчет товаров. В то время как Facebook служит средством общения, Instagram является отличным драйвером продаж.

Если обратиться к цифрам, то 70 % из 16 000 опрошенных компанией Iconosquare пользователей заявили, что в Instagram они ищут определенные бренды.

В то время как многие владельцы бизнеса ищут способ развлечь свою аудиторию, устраивая конкурсы, опросы, распродажи в соцсетях, 62 % подписчиков брендов в Instagram становятся фолловерами только потому, что «любят» конкретный бренд. А 41 % заявили, что подписались бы на новости той или иной компании, только чтобы получать различные бонусы и скидки. И наконец, 65 % пользователей признались, что им льстит получать отметки «мне нравится» от брендовых аккаунтов.

2. Пользователи Instagram любят взаимодействовать с брендовым контентом

В то время как компании вроде Iconosquare и Business Insider проводят исследования с целью изучить мотивацию пользователей в соцсети и их демографию, другие предпочитают заниматься иными вычислениями. Подсчет лайков и расшариваний помогает маркетологам понять, какие действия вызывают наибольший отклик у их целевой аудитории.

Сейчас многие маркетологи очень радуются тому факту, что интернет-пользователи гораздо активнее взаимодействуют с брендовым контентом в

Instagram, чем в других соцсетях. Результаты исследования от Socialbakers за IV квартал 2014 г. показали, что процент вовлеченности брендовой аудитории гораздо выше, чем в Twitter.

Пост в Instagram, который увидят 10000 тыс. пользователей, получит примерно 331 отметку «мне нравится», в то время как твит, который увидит то же количество людей, расшарят всего 7 раз.

Разница между степенью вовлеченности пользователей в Facebook и Instagram тоже довольно велика. Согласно результатам исследования от компании L2, подписчики брендовых аккаунтов в Instagram в 18 раз активнее, чем в Facebook.

Несмотря на то что в настоящее время Instagram – это очень активно развивающаяся социальная сеть, ее рост со временем замедлится, как это уже было с Facebook.

3. Аудитория Instagram очень молодая

Компании Cowen & Company, Frank N. Magid Associates и AVG с небольшой разницей во времени озадачились возрастом аудитории Instagram. Результаты исследований были собраны вместе специалистами из eMarketer. Оказалось, что 44 % интернет-пользователей в возрасте от 19 до 29 лет и 62 % молодых людей 11–16 лет использовали Instagram в ноябре 2014 г.

Для сравнения, только 18 % тех, кому исполнилось от 45 до 60 лет и 10 % отпраздновавших шестидесятилетие использовали Instagram в то же время.

Возрастная группа от 18 до 29 лет, хотя и не является самой многочисленной в Instagram, все же предпочитает эту социальную сеть Facebook (23 % заходили в Facebook хотя бы раз в течение месяца). Также среди этих пользователей очень популярны сервисы Snapchat и Tumblr.

Компания Pew Research Center выяснила, что 53 % пользователей в возрасте от 18 до 29 лет любят Instagram, а больше половины из них используют его каждый день.

Так как в большинстве своем аудитория Instagram – это молодежь, то неудивительно, что самыми популярными являются аккаунты брендовой одежды и технологических компаний. В 2014 г. 14 самых популярных автомобильных брендов размещали посты в соцсети в среднем 40 раз в месяц, 10 известных технологических компаний публиковали около 15 постов в месяц, а пятерка известных брендов одежды размещала свой контент в Instagram 45 раз в месяц. Иными словами, маркетологи хорошо поняли, что если твоя целевая аудитория моложе 30 лет, ее чаще всего следует искать в Instagram.

Но возраст – это не основной фактор определения целевой аудитории. Компания Iconosquare провела исследование в 2015 г., объектом которого стали 16 000 пользователей Instagram. Выяснилось, что 64 % изучаемой аудитории составили женщины. Около 30 % опрошенных проживают в США, остальные 70 % – в других странах мира. 48 % являются выпускниками вузов.

И что из этого?

Несмотря на то что большинство известных брендов уже есть в Instagram, осталось еще множество малоизвестных и узкоспециализированных компаний,

которые пока слабо обозначили там свое присутствие. У некоторых из них может даже не быть аккаунта в соцсети, но благодаря хэштегам пользователи могут находить контент, так или иначе связанный с интересующим их брендом. А компании могут узнать больше о том, что хочет их целевая аудитория, также используя хэштеги.

Если вы являетесь владельцем компании, товары и услуги которой предназначены для молодой аудитории, Instagram – ваше будущее. Следите за результатами исследований и не бойтесь экспериментировать ***(Три факта об Instagram, о которых вы могли не знать // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/tri_fakta_ob_instagram_o_kotoryh_vy_mogli_ne_znat). – 2015. – 3.04).***

***

Мировой рынок рекламы в социальных медиа в 2014 г. возрос на 41 % в годовом сравнении, достигнув 15,3 млрд дол. Facebook по-прежнему удерживает лидирующую позицию на этом рынке, несмотря на недостаточное присутствие в Китае, сообщает Marketing Media Review со ссылкой на Strategy Analytics (http://mmr.ua/news/id/75-mirovogo-rynka-reklamy-v-socialnyh-media-v-2014-godu-zanimal-facebook-43845/).

Статус лидера на мировом рынке социальных медиа прочно закрепился за Facebook, и нет никаких признаков, что эта ситуация изменится в ближайшем будущем. В 2014 г. на Facebook приходилось 75 % мировых затрат на рекламу в социальных сетях (11,4 млрд дол. из 15,3-миллиардного рынка). Доля Twitter, заработавшего 1,2 млрд дол. в 2014 г., составила 8 %.

Аналитики Strategy Analytics прогнозируют, что мировой рынок рекламы в социальных медиа достигнет 19,8 млрд дол. к концу этого года и 24,2 млрд дол. к концу 2016 г.

В отчёте компании также указывается, что количество пользователей социальных сетей в 2014 г. впервые перешагнуло отметку в 2 млрд человек. Из них 68 % – пользователи Facebook, чья аудитория составляет 1,4 млрд активных пользователей в месяц. 25 % пользователей социальных сетей проживают в Китае.

«В целом, рынок социальных медиа продолжает демонстрировать устойчивый рост по всем регионам, в то время как ведущие социальные платформы привлекают потребление и вовлечённость за счёт улучшенной интеграции цифрового медиа-контента», – отмечает автор отчёта Л. Кавасаки.

«Facebook в настоящее время доминирует на рынке социальных медиа, но его отсутствие в Китае позволяет местным социальным платформам, таким как QZone и Tencent Weibo получить свою долю на стремительно растущем китайском рынке цифровой рекламы».

Отчёт также включает другие интересные выводы:

Почти половина (46 %) пользователей социальных сетей проживают в Азиатско-Тихоокеанском регионе.

В 2014 г. Северная Америка имела максимальное соотношение количества пользователей социальных сетей к населению страны (64 %). За ней следовала Западная Европа (55 %).

Наибольшая доля мировых затрат на рекламу в социальных медиа приходилась на США (41 %). Здесь этот показатель в общей сумме достиг 6,2 млрд дол., что на 35 % больше, чем в 2013 г.

Великобритания – второй по величине рынок рекламы в социальных медиа. В 2014 г. на неё приходилось 8,2 % мировых затрат на этот рекламный канал. На Китай – 8 %.

В США рекламодатели больше всего тратили на рекламу в социальных медиа из расчёта на одного пользователя социальных сетей (31,37 дол.). В 2015 г. эта сумма достигнет 39,84 дол., увеличившись на 27 %, прогнозируют аналитики.

В 2015 г. количество пользователей социальных сетей в мире возрастет до 2,2 млрд человек, составив 31 % мирового населения.

К концу 2019 г. этот показатель возрастет до 2,72 млрд человек и составит 36 % населения планеты ***(75 % мирового рынка рекламы в социальных медиа в 2014 году занимал Facebook // Marketing Media Review (http://mmr.ua/news/id/75-mirovogo-rynka-reklamy-v-socialnyh-media-v-2014-godu-zanimal-facebook-43845/). – 2015. – 3.04).***

***

Facebook продолжает наращивать аудиторию пользователей, которые используют аккаунт социальной сети для авторизации на сторонних сайтах. Об этом свидетельствуют данные отчёта компании Janrain за Q1 2015 г. Ситуации способствовало увеличение доли на B2B рынке и на сайтах потребительских брендов. Об этом пишет searchengines.ru.

В I квартале текущего года доля Facebook достигла 45 %, что на 2 процентных пункта выше, чем в Q4 2014 г. Доля Google – второго по величине игрока на этом рынке – сократилась до 37 %. Доли других социальных медиа остались практически без изменений: ни один из игроков рынка не смог получить более 5 % авторизаций.

Важно отметить, что отчёт Janrain – мгновенный снимок рынка авторизации на сайтах с помощью аккаунтов в социальных сетях. Компания Gigya, также исследующая этот рынок, пока не представила свой отчёт за I квартал 2015 г.

Вице-президент Janrain по маркетингу и продукту Д. Бэклэнд считает, что достижения Facebook связаны с увеличением использования мобильных приложений потребителями. «В iOS-устройствах Apple Facebook интегрирован в операционную систему, в то время как Android-устройства Google имеют встроенную интеграцию с Google+. По мере роста количества пользователей iPhone 6 и iPhone 6 Plus, мы видим увеличение мобильных регистраций в Facebook».

Больше всего доля Facebook возросла на B2B-рынке и на сайтах потребительских брендов. Компания увеличила свою долю на B2B-рынке на 11 процентных пунктов – до 35 %, отвоевав лидерство в этой отрасли у LinkedIn. Доля социальной сети для профессионалов в I квартале этого года сократилась на 10 процентных пунктов – до 25 %. Тем не менее, аналитики Janrain отмечают, что LinkedIn может вернуть свои позиции после внедрения изменений в API этой весной. В частности тех, что связаны с добавлением кнопки «Подать заявку через LinkedIn» (Apply with LinkedIn) на корпоративных сайтах.

На сайтах потребительских брендов доля Facebook в Q1 2015 г. составляла 58 %, что на 9 % выше, чем в Q4 2014 г. Доля Google сократилась на 9 пунктов, составив 29 %.

Janrain также мониторит другие отрасли: музыкальную, игровую, розничную торговлю и развлечения. В этих категориях были отмечены лишь небольшие изменения ***(45 % пользователей регистрируются на сайтах при помощи профилей Facebook // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42990/118/lang,ru/). – 2015. – 6.04).***

***

В 2014 г. украинцы покупали онлайн бытовую технику, электронику, одежду, косметику и парфюмерию, постепенно увеличивая долю покупок, сделанных через социальные сети.

Больше всего украинцы покупали бытовую технику, электронику и компьютерную технику – 72 % онлайн-покупателей интересовались этой категорией товаров.

Второе место по популярности занимает покупка одежды: около 50 % приобретали обновки через Интернет. Тройку лидеров замыкает косметика и парфюмерия – 37 %.

Украинцам всё больше нравится покупать через социальные сети. За минувший год 39 % покупателей делали заказ через социальные сети. Чаще всего таким образом покупают одежду, аксессуары, обувь, косметику и парфюмерию, товары для детей.

93 % украинских онлайн-покупателей в 2014 г. продолжили пользоваться торговыми площадками и сайтами с объявлениями. Наиболее популярным среди сайтов для сравнения цен остался ресурс price.ua, второе место занял hotline.ua.

Лидером среди торговых площадок и сайтов с объявлениями по показателю пользования стал slando.ua/olx.ua, сдвинув aukro.ua на второе место. Третье место по показателю пользования занял prom.ua.

Напомним, за 2014 г. 51 % транзакций на оплату покупок пластиковыми картами украинцы делали в продуктовых магазинах и супермаркетах. Данными поделились эксперты ПриватБанка в ходе анализа объёмов оплаты товаров в сети POS-терминалов банка ***(Украинцы стали чаще покупать через соцсети***

– 40 % от общего числа онлайн-покупок // Блог Imena.UA (http://www.imena.ua/blog/online-retail-2014-gfk/). – 2015. – 6.04).

***

Аналитическая компания Strategy Analytics представила прогноз состояния глобального диджитал-рынка, согласно которому в текущем году затраты на продвижение в социальных сетях увеличатся на 29 % по сравнению с прошлым годом, но для 2014 г. этот показатель составлял 41 %, пишет Marketing Media Review (http://mmr.ua/news/id/rost-bjudzhetov-na-reklamu-v-socsetjah-v-etom-godu-zamedlitsja-43874/).

Тем не менее, по данным Strategy Analytics, в 2015 г. компании вложат в социальные медиа около 20 млрд дол. против 15,3 млрд дол. в предыдущем периоде.

Большую часть этих бюджетов будет аккумулировать Facebook. В прошлом году рекламодатели потратили на продвижение в глобальной соцсети 75 % всех денег, запланированных на social media-рекламу (около 11,5 млрд дол.). К тому же, аудитория ресурса в 2014 г. составляла 68 % от пользователей всех социальных сетей.

Микроблоговый сервис Twitter в прошлом году получил только 8 % рекламных бюджетов. Также, по подсчетам Strategy Analytics, в 2014 г. количество пользователей соцсетей впервые преодолело рубеж в 2 млрд человек ***(Рост бюджетов на рекламу в соцсетях в этом году замедлится // Marketing Media Review (http://mmr.ua/news/id/rost-bjudzhetov-na-reklamu-v-socsetjah-v-etom-godu-zamedlitsja-43874/). – 2015. – 7.04).***

***

Издание Adweek опубликовало исследование аналитической компании Simply Measured, которая проанализировала 100 тыс. новых подписчиков наиболее популярных брендов в Twitter, чтобы узнать число общих пользователей их аккаунтов, пишет Marketing Media Review (http://mmr.ua/news/id/naskolko-silno-peresekajutsja-auditorii-populjarnyh-amerikanskih-brendov-v-twitter-43869/).

Помимо этого, компания представила сведения о потреблении пользователями Twitter брендированной информации.

«Главная причина такого совмещения – клиенты разных брендов очень похожи друг на друга, – утверждает старший стратег аналитической компании Simply Measured К. Шивли. – Около 40 % продаж Starbucks происходят благодаря людям 18–24 лет. Для компании они являются самым быстрорастущим сегментом. Точно такая же демографическая группа приносит 30 % трафика на сайт H&M».

Однако генеральный директор маркетинговой компании LiveWorld П. Фридман совсем не удивлен пересечением аудитории брендов. «В частности, подписчики Starbucks с ее активным присутствием на рынке будут ожидаемо дублироваться с читателями аккаунтов других компаний», – говорит он.

«Вы можете найти интересную психографическую информацию о своих клиентах, основываясь на том, кого они читают в соцмедиа и о чем говорят, – добавляет П. Фридман. – Как оказалось, бренды часто удивляются беседам своих подписчиков в соцсетях».

Здесь собраны другие данные из исследования Simply Measured:

Когда пользователь присоединяется к Twitter, сервис рекомендует ему 40 аккаунтов на основе его цифровых интересов.

Пользователь начинает читать только четыре из них.

68 % пользователей, которые следят за 10 крупнейшими брендами, публикуют по крайней мере один твит каждые 30 дней.

26 % читателей Burberry также следят за страницей Louis Vuitton.

Меньше 1 % пользователей читают четыре или более брендов.

Только 14 % следят более чем за одним брендом.

Большинство пользователей читают примерно 50 аккаунтов в целом.

У Google и Microsoft 16 % общих читателей, а у Google и Intel – только 9 %. Зато у Intel с Microsoft аудитория пересекается на 32 % ***(Насколько сильно пересекаются аудитории популярных американских брендов в Twitter // Marketing Media Review (http://mmr.ua/news/id/naskolko-silno-peresekajutsja-auditorii-populjarnyh-amerikanskih-brendov-v-twitter-43869/). – 2015. – 6.04).***

***

Facebook представил функцию покупки в один клик – FacePay

Новое приобретение социальной сети порадует страстных любителей онлайн-магазинов: теперь совершать покупки можно будет гораздо быстрее, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-predstavil-funkciju-pokupki-v-odin-klik-facepay-43900/).

Недавно Facebook объявил, что его приоритетной задачей остается ускорение процесса электронных покупок. И вот цель достигнута. Новое приобретение FacePay по принципу работы схоже с Facebook Messenger. В программе заводится ваш личный аккаунт с данными банковской карты, который хранит всю историю покупок. Из бонусов – функция «купить сейчас» и отказ от рекламы и прочих объявлений в один клик.

С помощью новой программы сокращается весь процесс онлайн-покупки. Еще до создания FacePay Facebook наладил отношения с марками, которые продают в этой социальной сети. И специально для этого создана поисковая система в FacePay под названием The Find, которая делает выборку из брендов для каждого пользователя в соответствии с его интересами. Например, если человек «лайкнул» какой-либо велосипедный бренд, то ему предлагаются магазины с таким ассортиментом ***(Facebook представил функцию покупки в один клик – FacePay // Marketing Media Review (http://mmr.ua/news/id/facebook-predstavil-funkciju-pokupki-v-odin-klik-facepay-43900/). – 2015. – 8.04).***

***

Пятнадцать лет назад провокационные мечты Р. Левина, К. Лока, Д. Сирлза и Д. Уайнбергера создали платформу для эры маркетинга в социальных медиа с выходом публикации «Манифест пути» и смелым заявлением о конце традиционного бизнеса, пишет Marketing Media Review (http://mmr.ua/news/id/majk-prulks-socialnyh-media-bolshe-net-est-reklama-43905/).

Некоторое время казалось, что бренды начали использовать онлайн сообщества как возможность прямого контакта с пользователями. Но через несколько лет это идеалистическое видение двустороннего обмена разрушилось. Бренды обленились, размещая нерелевантный контент, а социальным сетям нужно зарабатывать деньги.

Давайте назовем это тем, что оно есть: маркетинг в социальных медиа – это сейчас реклама. Это главным образом медиа планирование и покупка – делая ударение на просмотренных показах. Бренды должны платить, если они хотят, чтобы их сообщение просмотрели. Это противоположно слушанию или установлению контакта – это опять вещание.

Недавно Д. Костоло отметил, что реклама появится в каждом 20 твите. Также не секрет, что органический охват Facebook также нуждается в поддержке. И когда Snapchat запустил Discover, он быстро указал, что «это не социальные медиа».

Идеалистический конец традиционного бизнеса, как предусматривали в Манифесте, также не наступил. После обещающего начала – проблеска надежды – мы вернулись к традиционному бизнесу. Конечно, в рекламных технологиях произошли сильные изменения. Медиа более таргетированны, более оптимизированы, автоматизированы, чем раньше. Но есть ли в них что-то социального?

Когда вы осознаете реальность, существует ряд вещей, которые помогут извлечь максимум из этой эры #НеСовсем соц.медиайного маркетинга. Вот пять из них:

1. Откройте свой кошелек. Помните, когда социальные медиа называли бесплатными медиа? Эти дни прошли. Для маркетинга в социальных медиа сегодня нужна перемена мышления, которая рассматривает социальные медиа, такие как Facebook и Twitter, в качестве любого другого медиа канала. Они обладают массовой аудиторией, которую можно достичь, если вы желаете выделить кусок вашего медиа бюджета. Факт: вам придется потратить больше денег в социальных медиа, чем вы это делали в прошлом.

2. Сыграйте в блэкджек. В отличие от других медиа каналов, социальные платформы имеют моментальный фидбек в форме лайков, комментариев, ретвитов и так далее. Начните с распределения небольшого количества денег на все продвигаемые посты. Затем используйте присущие платформе социальные сигналы, чтобы определить, для какого контента повысить ставки. Продолжайте удваивать ставку для топ-игроков, увеличивая количество долларов. Подумайте об этом как о краудсорсинговом медиа планировании.

Более популярные посты – это верная ставка, чтобы распространить их для более широкой аудитории.

3. Покажите сдержанность. Не будьте вовлеченными в размещении безобидного контента и его продвижении. Нельзя забыть об искусстве креативности и науке стратегии бренда только потому, что вы можете мгновенно постить. Оставайтесь верными своему бренду и размещайте только то, что релевантно, полезно или ценно.

4. Измеряйте то, что имеет значение. Хотя метрики по вовлечению помогают увидеть популярный контент, ваш успех платных медиа нужно измерять в отношении специфических маркетинговых целей (подсказка: увеличение лайков и фолловеров – это не бизнес цель). Чтобы измерить влияние бизнеса, нужен более основательный аналитический подход за рамками того, что обычно предлагают социальные платформы, включая экспериментальный дизайн и моделирование атрибуции.

5. Составьте полную картину. И, наконец, социальные медиа не существуют разрозненно. Медиа привычки потребителей стали мэшапом девайсов, платформ и контента. Используйте это в качестве преимущества, чтобы спланировать и привести в действие программы, которые работают на разных платформах. Ваши продвигаемые посты должны дополнять, соединять и усиливать в рамках более крупной маркетинговой стратегии. А контент, который вы создаете? Он должен быть кастомизирован под уникальные сильные стороны и нюансы каждый социальной платформы в вашем миксе.

Все медиа сегодня по существу социальные медиа, и секрет кроется в том, что они не очень социальные. Но для тех, кто руководствуется принципами, изложенными в Манифесте, есть и хорошие новости: маркетинг это намного больше, чем продвижение. И хотя социальная рекламная стратегия это новая мораль, бренды не должны забывать о своей социальной бизнес стратегии, о которой говорили Р. Левин, К. Локк и др.

Пришло время снова действовать. Наши социальные сети все еще являются золотой жилой нетронутого пользовательского инсайта и возможностей. Нет причин, почему бренды не могут использовать социальные медиа для трансформации своего бизнеса – чтобы положить конец традиционному бизнесу, продолжая рекламировать в нем ***(М. Прулкс: социальных медиа больше нет, есть реклама // Marketing Media Review (http://mmr.ua/news/id/majk-prulks-socialnyh-media-bolshe-net-est-reklama-43905/). – 2015. – 8.04).***

***

У одних специалистов рекламная платформа Facebook вызывает дрожь и трепет – разобраться в настройках, ценообразовании, целях и инструментах подчас практически невозможно. Другие же наоборот виртуозно запускают одну кампанию за другой.

Редакция «Лайкни» решила узнать немного больше о том, как ведутся рекламные кампании в Facebook в Рунете: какие цели выбирают специалисты, какие размещения считают наиболее эффективными, что вызывает сложности.

Итак, чаще всего рекламные кампании в Facebook запускаются с целью продвинуть страницу или публикацию, а также получить переходы на сайт.

Для создания рекламных кампаний специалисты чаще всего используют Менеджер рекламы (58 %). Только 9 % предпочитают Power Editor. 33 % специалистов используют оба инструмента.

70 % респондентов используют Таргетинг по интересам аудитории, 41 % – Индивидуализированные аудитории, а Похожие аудитории – только 27 %.

Самое популярное место размещения рекламных объявлений – Новостная лента (десктопы и мобильные).

Такой выбор специалистов неудивителен, по словам 44 % специалистов, самый высокий CTR у объявлений, которые размещаются в Новостной ленте (десктоп и мобильные). 28 % респондентов отметили мобильную Новостную ленту, а десктопную – 21 %. Еще 14 % специалистов считают, что самый большой CTR у объявлений, расположенных в правой колонке.

42 % респондентов отметили, что у объявлений в правой колонке самый низкий CPC. Затем идет Новостная лента (мобильные) – 25,5 %, Новостная лента (десктоп) – 18,5 % и Новостная лента (десктоп и мобильные) – 14 %.

Самые большие сложности при работе и ведении РК в Facebook:

– не всегда получается правильно распределить бюджет в соответствии с нужным форматом ценообразования – 53 %;

– не всегда получается разобраться с настройками аудитории, которых слишком много –37 %;

– постоянно меняющиеся форматы объявлений – непонятно как их использовать – 32,5 %;

– непонятные отчеты, из-за которых сложно посчитать эффективность рекламы – 30 %;

– рекламные инструменты в принципе настолько сложные, что проблемы возникают на каждом этапе создания и ведения РК – 11 %;

– проблемы с обратной связью – трудно добиться от площадки ответов при нестандартных проблемах.

При этом 51 % специалистов считают, что стоимость рекламы в Facebook себя полностью оправдывает. 42 % респондентов ответили, что РК в западной соцсети дорогие и не всегда эффективные. А 7 % считают рекламу в Facebook дешевой для того эффекта, что она дает ***(Лайкометр 2.0: стоимость рекламы в Facebook себя полностью оправдывает // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/laykometr_2_0_stoimost_reklamy_v_facebook_sebya_polnostyu_opravdyvaet). – 2015. – 9.04).***

***

Какой контент любят расшаривать пользователи

Все еще не можете понять, почему ваш потрясающий контент не расшаривают, а невзрачный видеоролик конкурента разошелся по всей сети? Тогда вы пришли по адресу: здесь и сейчас мы приоткроем завесу тайны над неразрешимой загадкой. Так какой же контент любят расшаривать пользователи и почему? Marketing Media Review решил разобраться (http://mmr.ua/news/id/kakoj-kontent-ljubjat-rassharivat-polzovateli-43925/).

1. Участились расшаривания с мобильных устройств

Согласно исследованию, проведенному компанией ShareThis в 2014 г., активность пользователей в сети значительно возросла, и они стали в два раза чаще расшаривать контент. 20 % времени, отводимого ими на использование смартфонов, уходит на то, чтобы рассказать друзьям о понравившихся постах. С десктопными устройствами дела обстоят несколько хуже: в 2014 г. количество раз, когда пользователи захотели поделиться какими-то интересными материалами, сократилось на 30,2 %.

Что это значит? Во-первых, то, что если вы хотите, чтобы пользователи вас заметили, выстраивайте свою маркетинговую стратегию, в первую очередь опираясь на мобильные устройства. А во-вторых, не забывайте, что смартфоны и планшеты используются вашей аудиторией в основном для личных нужд, в то время как десктопы служат рабочим целям, так как многие работодатели сейчас закрывают доступы к социальным сетям в офисах.

2. Facebook – абсолютный чемпион по количеству расшариваний

В своем исследовании, уже упомянутом выше, компания ShareThis сравнила пользовательскую активность в Facebook, Twitter, Pinterest, Tumblr и еще трех социальных платформах. В частности, их интересовал процесс расшаривания материалов. Оказалось, что Facebook в 10 раз превосходит своего ближайшего конкурента – Pinterest по количеству расшариваний. В 2014 г. 81 % всей шеринговой активности во всех исследуемых соцсетях происходил именно в Facebook. Однако тут есть одно но – исследование не затронуло Instagram.

Как показали исследования, рейтинг вовлеченности пользователей Instagram гораздо выше, чем у любой другой соцсети. Если учесть, что понятие вовлеченности включает в себя множество действий, совершаемых пользователями, можно считать, что расшаривания занимают одну из лидирующих позиций в Instagram.

Специалисты из TrackMaven в течение двух лет занимались анализом деятельности 8800 брендов в соцсетях. Было изучено около 13,8 млн единиц контента, размещаемого этими брендами. Выяснилось, что в январе 2013 г. одна компания публиковала в среднем 25 постов в каждой социальной сети. К сентябрю 2014 г. эта цифра удвоилась. А вот количество расшариваний пошло в обратном направлении, уменьшившись за год почти вдвое. Как отметили специалисты, хуже всего дела обстоят в Twitter. Поэтому маркетологам следует сосредоточиться на Facebook и Instagram.

3. Статьи-списки и познавательные посты расшаривают чаще всего

С июня по ноябрь 2014 г. компании BuzzStream и Fractl изучили 220 тыс. единиц контента, размещенного в социальных сетях десятью самыми популярными и десятью малоизвестными предприятиями. Оказалось, что статьи, структурированные по пунктам, а также познавательные посты расшаривают чаще всего. А вот видео и практические руководства вообще не пользуются популярностью среди пользователей.

Имея огромное количество информации для изучения, специалисты также выяснили, какие темы популярнее всего в конкретных соцсетях. Например, в Facebook каждый найдет себе компанию по душе и сможет обсудить что угодно, в то время как в другие сети можно условно обозначить как узкоспециализированные. Пользователи Pinterest любят говорить о еде, красоте, фитнесе и шоппинге. А в Twitter в 2014 г. был отмечен всплеск обсуждений различных спортивных событий.

Что следует запомнить:

Компаниям с более молодой целевой аудиторией следует обратить свое пристальное внимание на Instagram. Те, кто во всем полагается на Facebook, могут упустить неплохие возможности в других, менее популярных соцсетях.

Маркетологи, занимающиеся раскруткой спортивных товаров, должны обратить свое внимание на Twitter. А выбравшие Pinterest основной маркетинговой платформой могут рассчитывать на отличный результат, создав интересную кампанию, которая будет не только полезна для бренда, но и для пользователей, ведь расшаривая контент, они продвигают и свой аккаунт, находя таким образом больше друзей ***(Какой контент любят расшаривать пользователи // Marketing Media Review (http://mmr.ua/news/id/kakoj-kontent-ljubjat-rassharivat-polzovateli-43925/). – 2015. – 9.04).***

***

Лише кожен десятий «білий комірець» користується Інтернетом виключно для вирішення робочих питань. Інші ж не проти відволіктися на читання новинних стрічок на сайтах та в соціальних мережах. Разом з тим 57 % офісних працівників відводять на це не більше 30 хв робочого часу. Про це свідчать результати опитування Міжнародного кадрового порталу HeadHunter Україна.

Події останнього часу призвели до того, що більшість українців стали уважніше стежити за новинами. Зрозуміло, на це витрачається і робочий час. За даними опитування hh.ua, 9 з 10 опитаних використовують Інтернет у робочий час із метою ознайомлення з новинами. У кожного четвертого на це йде всього 5–10 хв. Ще третина жертвує 30 хв робочого часу. 17 % читає новини приблизно годину. А ось 5 % вивчають підбірки останніх подій більше кількох годин, проведених на роботі.

При цьому на соціальні мережі та інші сайти, які не мають відношення до роботи, іде ще більше робочого часу. Число тих, хто витрачає на це менше півгодини, тут сягає 49 %. А ось кожен п’ятий офісний співробітник «висить» у

соц. мережах або на інших сайтах більше години, а то й більше декількох годин.

Витрачений працівниками «даремно» робочий час компаніям загрожує втратами, тому деякі роботодавці закривають доступ до соцмереж, блогів, файлообмінників та інших сайтів. Це робиться ще й з метою убезпечити компанію від витоку інформації. Нещодавнє дослідження HeadHunter Україна показало, що 76 % співробітників виносять корпоративні дані та робочі матеріали з офісу ***(Безкоштовний інтернет на роботі – шлях в соціальні мережі // Дніпроград (http://dniprograd.org/ua/news/economy/22277). – 2015. – 10.04).***

***

Капіталізація сервісу мікроблогів Twitter зросла на 1,5 млрд дол. після появи чуток, що компанію, що володіє соціальною мережею для публічного обміну короткими повідомленнями, може купити Google, пише Корреспондент.net (http://ua.korrespondent.net/business/companies/3501312-kapitalizatsiia-Twitter-rizko-zrosla-cherez-chutky-pro-yoho-prodazh).

Акції Twitter зросли на 4,8 % після повідомлень у ЗМІ, що американська компанія найняла інвестиційний банк Goldman Sachs як консультанта з боротьби з можливими поглинаннями.

Раніше ЗМІ повідомляли, що до Twitter проявляли «серйозний» інтерес дві компанії, одна з яких – Google, нагадує видання The Telegraph.

Як повідомляв Кореспондент.net, за підсумками 2014 р. збитки Twitter становили 578 млн дол. ***(Капіталізація Twitter різко зросла через чутки про його продаж // Корреспондент.net (http://ua.korrespondent.net/business/companies/3501312-kapitalizatsiia-Twitter-rizko-zrosla-cherez-chutky-pro-yoho-prodazh). – 2015. – 8.04).***

***

Google планирует ввести до конца 2015 г. подписку на видеохостинге YouTube, которая позволит смотреть ролики без рекламы. Об этом сообщило агентство Bloomberg со ссылкой на письмо, которое Google разослал производителям видеоконтента.

«Запустив новое платное предложение, мы добавим еще один источник выручки, который дополнит ваши быстрорастущие рекламные сервисы», – сообщил разработчикам видеоконтента Google, не приведя подробностей.

Платный сервис заработает до конца 2015 г., рассказал Bloomberg осведомленный источник. Подписка будет стоить около 10 дол. в месяц, отметил источник изданию The Verge.

Подписчики YouTube смогут смотреть видео без рекламы, а также сохранять ролики в памяти своих устройств для дальнейшего просмотра, сообщил Google создателям контента. По данным Google, больше половины времени просмотра видеороликов на YouTube приходится на мобильные устройства.

В Северной Америке YouTube второй по популярности видеосервис стриминга: на него во второй половине 2014 г. пришлось до 14 % всего видеотрафика, по оценке компании Sandvine. По этим данным, самым популярным стриминговым видеосервисом в Северной Америке был Netflix, доля которого в трафике превысила 30 %. Netflix – платный сервис, подписка стоит от 8 дол. в месяц ***(YouTube введет до конца года плату за просмотр видео без рекламы // InternetUA (http://internetua.com/YouTube-vvedet-do-konca-goda-platu-za-prosmotr-video-bez-reklami). – 2015. – 9.04).***

***

Социальная сеть LinkedIn подписала договор о приобретении обучающего сайта lynda.com за 1,5 млрд дол. Об этом говорится в пресс-релизе LinkedIn.

Пятьдесят два процента от суммы сделки соцсеть оплатит деньгами, остальное – своими акциями. Закрыть ее стороны планируют во II квартале 2015 г.

По словам исполнительного директора LinkedIn Д. Уинера, которые приводятся в релизе, оба интернет-ресурса выполняют схожие функции, помогая профессионалам улучшать достижения в своей сфере деятельности.

Число пользователей профессиональной сети LinkedIn, запущенной в мае 2003 г., составляет более 340 млн человек. Штат компании насчитывает 6,8 тыс. человек. Выручка компании по итогам прошлого года составила 2,2 млрд дол.

Аудитория сайта Lynda.com, работающего с 1995 г., оценивается в 4 млн пользователей. На его страницах размещены тысячи образовательных курсов, включая сферу бизнеса ***(Соцсеть LinkedIn купит образовательный сайт за 1,5 миллиарда долларов // InternetUA (http://internetua.com/socset-LinkedIn-kupit-obrazovatelnii-sait-za-1-5-milliarda-dollarov). – 2015. – 13.04).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Согласно исследованию психологов Йельского университета, доступность систем вроде Google и Yahoo! заставляет людей ошибочно думать, что они умнее, чем есть на самом деле. Об этом сообщает The Telegraph.

В исследовании Йельского университета приняло участие более тысячи студентов, которых попросили пройти через серию экспериментов. По их завершении выяснилось, что возможность поиска информации в Интернете

даёт людям «крайне неточное» представление об их умственных способностях и излишнюю уверенность в принятии решений.

Участники исследования, которым было разрешено пользоваться Google, считали, что они знают о предмете намного больше, чем те, чьи возможности ограничили книгами и другими классическими способами поиска информации.

«Интернет – это мощная среда, в которой вы можете задать любой вопрос и получить доступ ко всем знаниям мира, находящимся буквально на кончиках пальцев. Становится намного легче спутать наши собственные знания с информацией из внешнего источника. Сами по себе люди могут иметь крайне неточное представление о том, что они знают и как зависят от Интернета», – комментирует М. Фишер, кандидат наук в области психологии

В одном из тестов студентов разделили на две группы, одной из которых предложили ответить на вопрос о том, как работает застёжка-молния, с помощью ссылки в Интернете, а другой – с помощью информации на листке бумаги.

Затем обеим командам задали второй вопрос, никак не связанный с первым: «Почему в облачную погоду ночи теплее?» Группа, которой до этого дали найти информацию в Интернете, отвечала на него более уверенно, несмотря на то что не имела возможности воспользоваться сетью снова.

Как отметил профессор психологии из Йельского университета Ф. Кейл, эффект «пребывания в режиме поиска» оказался настолько сильным, что сохранялся значительное время после того как человек выходил из Интернета. По словам исследователей, это явление может быть особенно опасным, когда речь идёт о принятии важных решений, от которых могут зависеть человеческие жизни.

Авторы эксперимента предполагают, что в некоторых случаях людям может понадобиться нечто вроде «сетевой депривации» – выхода из состояния излишней уверенности в себе для получения более трезвых выводов о сложившейся ситуации. Они отмечают, что из-за развития мобильного Интернета граница между знаниями человека и знаниями всего человечества постепенно стирается, однако это заметно усложняет процесс становления экспертом в какой-либо области, а не упрощает его ***(Из-за поисковых систем люди переоценивают уровень своего интеллекта // InternetUA (http://internetua.com/iz-za-poiskovih-sistem-luadi-pereocenivauat-uroven-svoego-intellekta). – 2015. – 2.04).***

***

У многих людей, проводящих ежедневно по нескольку часов в сетях, заметно снижается самооценка.

Сейчас сложно найти человека, который бы не был зарегистрирован в одной из социальных сетей и не имел бы своей странички в ней. Но в целом полезное виртуальное общение с другими людьми может стать причиной снижения самооценки и развития депрессии, пишет Сегодня

(http://www.segodnya.ua/life/health/socialnye-seti-dovodyat-lyudey-do-depressii-issledovanie-606787.html).

Американские психологи предупреждают о скрытой опасности слишком продолжительного пребывания в социальных сетях, пишет health-ua.org. Сотрудники университета в американском городе Хьюстон (University of Houston) установили, что у многих людей, проводящих ежедневно по нескольку часов в сетях, заметно снижается самооценка, развивается стойкая угнетенность настроения, которая затем переходит в депрессию.

Хьюстонские ученые провели два практически одинаковых исследования, но с разными участниками. В первом случае их было 180 человек, во втором – более 150. Все участники в обоих случаях являлись активными пользователями популярнейшей социальной сети Facebook.

Анализ данных о продолжительности пребывания участников в социальной сети на протяжении каждого дня показал наличие прямой связи между временем виртуального общения и риском развития депрессии.

Авторы объясняют обнаруженную связь феноменом так называемого социального сравнения. Общаясь с виртуальными «друзьями», человек подсознательно начинает сравнивать себя с ними. Сравнение идет сразу по нескольким параметрам, начиная от внешности и заканчивая моделью смартфона или маркой автомобиля. Однако подавляющее большинство пользователей социальных сетей сообщают о себе и своей жизни только положительную информацию, скрывая весь негатив. Иногда это делается неумышленно, но чаще намеренно – с целью подчеркнуть свою успешность и превосходство.

Многие попадаются на эту уловку и в результате невольного сравнения начинают страдать комплексом неполноценности, от которого до начала депрессии один шаг. Такая опасность грозит в первую очередь тем пользователям социальных сетей, у которых уже имеются определенные психологические проблемы, проблемы бытового характера, а также те, которые живут в состоянии хронического стресса.

В этом случае социальные сети оказывают деструктивное влияние на психику ***(Социальные сети доводят людей до депрессии – исследование // Сегодня (http://www.segodnya.ua/life/health/socialnye-seti-dovodyat-lyudey-do-depressii-issledovanie-606787.html). – 2015. – 13.04).***

Маніпулятивні технології

В последнее время часто можно слышать о том, что Украина проигрывает в информационной войне. Тем не менее, в уанете есть волонтерские проекты, которые поставили себе целью чистить информационное пространство от фейков и вбросов, которые в социальных сетях тиражируются со скоростью мысли. Сайту StopFake уже год, его уникальная аудитория за это время составила 5 млн пользователей, 16 млн просмотров, а число подписчиков в

соцсетях достигает 155 тыс. человек, пишет AIN.UA (http://ain.ua/2015/03/31/572790).

В команде 16 человек, среди них дизайнеры, переводчики, журналисты, у которых есть основное место работы. В StopFake они трудятся на волонтерских началах. В настоящее время проект существует частично благодаря краудфандингу. Любая коммерциализация просто убьет изначальную идею StopFake, убеждена соосновательница проекта – бывшая журналистка «Громадського», Espreso.TV и рок-музыкант М. Гонтар. В блиц-интервью AIN.UA она рассказала о том, как редакция определяет фейки, как оценивать правдоподобность информации в Facebook и «ВКонтакте», а также о том, какие СМИ реже всего попадаются на вранье.

Об основании и команде проекта

В марте прошлого года директор Могилянской школы журналистики Е. Федченко кинул клич в Facebook: давайте соберемся и подумаем, что могут в текущей ситуации сделать журналисты. Одной из основных информационных проблем тогда был постоянный поток антиукраинской информации. У нас была журналистская тусовка из студентов Могилянской школы журналистики и участников программы DFJ – мы точно знали, как делать и проверять новости. Так родилась идея опровергать фейки в онлайне. Правда, со временем сформировалась еще одна цель: стать архивариусом и собирать «в шкатулку» все примеры вранья и манипуляций.

Лично для меня главным было то, что, на мой взгляд, я не в достаточной мере успела поучаствовать в Майдане. И многие, кто помогал StopFake, руководствовались тем же. Это такой персональный Майдан – сделать что-то полезное для Украины. Помню, как в начале многие люди помогали нам с сайтом, дизайном, контентом бесплатно и дико обижались, когда мы предлагали деньги. Тогда очень чувствовался этот дух: сделать что-то ради Украины. Сейчас все чуть прозаичнее.

Раскрутиться нам очень помогло медиасообщество: сразу после основания многие редакторы и журналисты о нас написали, в третий день после запуска уже было интервью на «Громадському». Помню первый рабочий день: села за компьютер в 12:00, работала не отрываясь, встала из-за компьютера в 22:00.

О том, как отбирают фейки для разоблачения

Часто линки на новости присылают читатели. Кто что из команды видит – кидает в закрытую рабочую группу на Facebook. Что именно отбираем – зависит от периода. Обычно действует правило: если разгоняет новость совсем маргинальное медиа и если мы будем выглядеть более бредово, чем они, пытаясь ее опровергать, то однозначно не берем.

Что же касается критериев отбора… На мой взгляд, любая ложь опасна. Даже какие-то маленькие истории типа «В Украине сносят памятник Ватутину». Вроде мелочь, но она отсылает читателя к общему фону: «украинцы – фашисты, нелюди, память не чтят, освободителя Киева не уважают, еще и родственников его обижают».

Иногда случаются очень громкие кейсы – та же история со сбитым «Боингом». Мы писали разоблачение на историю об испанском диспетчере, якобы работавшем в «Борисполе» и заметившем два украинских самолета рядом с «Боингом». Конечно, этот пост собрал тысячи шеров, ведь все ждали и хотели узнать, что же случилось на самом деле. Это громкая новость, но если брать тот общий фон, к которому она апеллирует, то разницы с мелкой новостью о Ватутине нет. Просто «Боинг» случился «сейчас», а фашистами украинцев называли весь год. Кажется, что «ой, да мы привыкли», но это на самом деле страшно.

То, что российские СМИ так долго рассказывают о бесчеловечности украинцев – это очень известный пропагандистский прием, необходимый для того, чтобы привить россиянам мысль: убивать других – нормально, они ведь нелюди.

О фейках в украинских СМИ

Каждый раз, когда украинские коллеги постят неправдивую новость, в мире грустит один котик. Нет, не так: в мире радуется один киселев. Потому что у российских медиа появляется возможность сказать: ох уж эти врущие украинские журналисты!

Отвечаю на ваш вопрос: кто из украинских общественных СМИ самый аккуратный? Мы никогда не имели дела с «Днем», с «Зеркалом недели». Бывало, что ловили ТСН, «Цензор», «Обозреватель», «Интер», «Украину». Хорошо помню видео ракеты с Байконура, подписанное, как обстрел Донецка сепаратистами.

Но все же нашим очень далеко до российских LifeNews, «Первого канала», «России 24» в объемах вранья. Интересно, что самая большая аудитория StopFake сразу после Украины – читатели из России. И по объему donation на развитие проекта тоже РФ идет сразу после Украины.

О том, как определить вранье и вброс в новости

Очень помогает вопрос: кому эта новость может быть выгодна. Сейчас в ситуации информационной войны любая антиукраинская новость выгодна Кремлю. Дальше идет обычная журналистская работа: проверить источники, имена, документальную базу. Часто именно действующие законы, нормы, правила говорят о том, что либо «случившееся» в принципе невозможно, либо фигуранты истории некомпетентны. Как было с тем же испанским диспетчером: когда начали проверять историю, узнали, что к подготовке диспетчеров у нас в стране допускаются иключительно граждане Украины.

Как очень просто определить фейк? О фейковости может свидетельствовать:

Общая неадекватность, история идет вразрез со здравым смыслом.

Засилье малопонятных терминов, общих фраз вроде «общеизвестно», «западные СМИ утверждают», «доказано учеными», «эксперты говорят». Если что-то происходит в тексте, это должно базироваться на факте, наблюдении, доказанном в исследовании, или на мнении конкретного человека, институции, на документе. Сейчас пытаются маскировать фейки якобы англоязычными

источниками. Хороший пример: история с мнимым приездом Д. Боуи в Донецк со ссылкой на его заявление. Хотя любому человку, говорящему по-английски, ясно, что Д. Боуи не мог так сказать, скорее это написал русскоязычный человек, владеющий английским не в совершенстве. И концертов Д. Боуи не дает с 2003 г.

Излишняя эмоциональность. Это главный, самый простой критерий. Чем больше эмоциональных эпитетов, чем меньше фактов, тем больше вероятность, что это вброс. Отличный пример очень эмоциональной новости – «распятый мальчик». Это, кстати, кочующий сюжет. Помню, на конференции фонда Белля в ноябре прошлого года местные историки рассказывали, что сюжет с «распятым мальчиком» гулял еще в прессе 20-х годов прошлого столетия.

Несоответствие заголовка и текста. Заголовки сейчас живут своей жизнью в агрегаторах, Twitter, и воспринимаются сами по себе как новости. Этим часто пользуются.

Неприкрытая попытка подвести читателя к определенному выводу (кто виноват, что делать). В видеосюжетах (и не только) дикторы часто стоят на позиции «они – мы».

Категоричность утверждений, не подкрепленных четкими доказательствами.

О панике в социальных сетях

Сейчас почему-то даже журналисты считают, что «нет времени размышлять, быстро перепости» – это хороший метод. Но он изначально гиблый. Не понимаю, как оперативность может быть важнее правдивости. Если в угоду скорости публикуется неправда – нивелируется сам смысл действия.

Одно дело, если это важные (и авторитетные) сообщения о передвижении, например, вооруженных группировок, как было во время Майдана. Другое: если информация может потерпеть несколько часов, чтобы ее проверить. Все фокусируются на том, чей сайт быстрее появится в поиске, кто соберет больше лайков, а факты не проверяют. У нас, к сожалению, вообще нет практики фактчекинга, хотя в западных редакциях за это отвечают отдельные сотрудники и даже отделы.

Беда еще в том, что мы все еще склонны верить журналистам, отдельным людям. Нам хочется верить, что люди хорошие и не врут. Если мы – не тролли и не боты, значит и в соцсетях тоже пишут настоящие люди. Если на глаза нам попадается невероятная жизненная история и она соответствует нашему представлению о том, как это могло бы произойти, рука так и тянется лайкнуть или поделиться.

Обращайте внимание на аргументацию, последовательность событий. Если в посте – крики, призывы, капслок, а сам текст – с ярковыраженной анти-позицией, лучше его перепроверить. Помню историю о том, как кто-то прифотошопил на руку татуировку российской дивизии и запостил фото на фейковом аккаунте пресс-центра АТО. Это нам не помогает: ведь любой ламер может проверить фото и рассказывать всем, что украинские СМИ тоже врут.

О планах проекта StopFake

Хотим со временем завести полноценный отдел мониторинга новостей в редакции. Сейчас мы, конечно, не успеваем мониторить медиаполе полностью ***(Теория лжи, или как бороться с фейками и вбросами: интервью с основательницей StopFake // AIN.UA (http://ain.ua/2015/03/31/572790). – 2015. – 31.03).***

***

Скориставшись пошуковою системою в мережі Інтернет, можна натрапити на соціальні спільноти, як українські так і закордонні, учасники яких поширюють заклики сепаратистського характеру, активно пропагують антиконституційну діяльність. Сфальсифіковані інформаційні матеріали завдають великої шкоди, маніпулюючи свідомістю людей, дезінформують їх та спонукають до протиправних дій.

Інформаційна безпека – тема нашої розмови з начальником профільного відділу управління СБ України в Кіровоградській області Д. Куценком.

«Ні для кого не є таємницею, що проти України ведеться потужна інформаційна війна. Велику роль у ній відведено Інтернету, зокрема соціальним мережам. Службою безпеки України через соціальні мережі щодня виявляється величезна кількість груп сепаратистської та антиукраїнської спрямованості. Встановлено, що понад 80 % з них адмініструються з території РФ, тимчасово окупованих територій АР Крим та Донецької і Луганської областей.

Найпершою загрозою є маніпулювання свідомістю українців у напрямі формування вигідної іноземній стороні, її спецслужбам громадської думки.

По-друге, це координація проросійськи налаштованих громадян та представників проросійських об’єднань для підбурювання антидержавних акцій. По-третє, − дестабілізація суспільно-політичної обстановки в регіоні.

Управлінням СБ України в Кіровоградській області здійснюється постійний моніторинг спільнот регіонального сегмента мережі Інтернет на предмет виявлення протиправних проявів та загроз державній інформаційній безпеці. Вживаються заходи щодо блокування їхньої роботи, виявляємо та припиняємо протиправну діяльність осіб, які адмініструють антиукраїнські спільноти, втягують у них молодь.

До речі, багато свідомих користувачів мережі повідомляють нам про такі сайти та спільноти сепаратистів. Ми дуже вдячні громадянам за їхню активність та небайдужість. Тим, хто не знає куди звернутися, хочу нагадати телефон довіри управління. Якщо у вас є інформація про такі спільноти і сайти, чи то людей, які займаються їх наповненням, звертайтесь за номером (0522) 36-13-06 та на електронну адресу управління usbu_kvg@ssu.gov.ua. Кожне повідомлення буде ретельно розглянуте. У випадку підтвердження викладеної інформації, вживатимуться заходи відповідно до чинного законодавства.

Протягом 2014 р. розпочато п’ять кримінальних проваджень, до кримінальної відповідальності притягнуто чотирьох мешканців Кіровоградської області, які поширювали через Інтернет матеріали деструктивного характеру, пропагували ідеї сепаратизму та екстремізму. Вироком суду зловмисникам

призначено покарання від двох до чотирьох років позбавлення волі з випробувальним терміном. Якщо вони й надалі здійснюватимуть таку протиправну діяльність − покарання буде суворим.

З початку 2015 р. управлінням здійснюється досудове розслідування в трьох кримінальних провадженнях за ознаками злочинів, передбачених ч. 2 ст. 109 та ч. 1 ст. 263 Кримінального кодексу України. Щодо фігурантів справ, то обрано міру запобіжного заходу у вигляді тримання під вартою. Під час санкціонованих обшуків у зловмисників вилучено комп'ютерну техніку, матеріали із закликами до повалення конституційного ладу і захоплення державної влади, символіку терористичних організацій самопроголошених "ДНР" і "ЛНР" та бойові припаси.

Чому люди на це йдуть?

Куратори з РФ обіцяють гроші за антиукраїнську інформаційну діяльність у соціальній мережі. Але, як правило, люди не отримують жодної копійки. А от перспектива притягнення до кримінальної відповідальності є цілком реальною».

Д. Куценко радить уникати користування російськими соціальними мережами та сайтами. Вони контролюються спецслужбами РФ і використовуються для дезінформації та дестабілізації ситуації в нашій державі, вербування спільників терористів і фінансування бойовиків.

Кращий спосіб захистити себе від дезінформації – критично оцінювати джерела її надходження і, звісно, бути пильними ***(Скільки інтернет-сепаратистів було викрито на Кіровоградщині? // Week (http://week.kr.ua/uk/sotsium/4631-skilki-internet-separatistiv-bulo-vikrito-na-kirovogradshchini.html). – 2015. – 3.04).***

***

Известный интернет-аналитик Л. Александер провел расследование и пришел к выводу, что только в Twitter существует около 20,5 тыс. аккаунтов, которые, вероятно, являются кремлевскими ботами.

Исследование опубликвано на сайте Global Voices.

Отправной точкой исследования послужил набор аккаунтов, через несколько часов после убийства Б. Немцова 27 февраля разместивших идентичную фразу – о том, что Немцова убили украинцы.

Исследовав социальные связи всех таких аккаунтов, исследователь выяснил, что 2900 из них – тесно связанная группа, топология которой резко отличается от естественной (случайной выборки аккаунтов). Кроме того, 87 % профилей не имели информации о часовом поясе и 92 % не имели любимых профилей Twitter. Для «человеческой» сети соответствующие показатели – 51 % и 15 %.

Ту же методику Л. Александер применил к еще четырем фразам, которые пользователи рунета определили как исходящие от «кремлеботов» – о «Новой газете», боях под Мариуполем, начале «большой войны» – и попавшему в поток по ошибке сообщению о сбое RSS.

Из четырех групп оказалось возможным выделить 17 590 «социально изолированных» аккаунтов, в 93 % профилей которых не было информации о местоположении, в 96 % не было часового пояса и в 97 % – любимых профилей Twitter. Кроме того, хотя аккаунты всех четырех групп были выделены по независимым признакам, все они оказались тесно связаны друг с другом.

«Эта картина сильнейшим образом отличается от рандомизированной контрольной выборки: финальная выборка вообще не содержала изолированных групп. Она соответствует гипотезе, что это боты, созданные общим агентом – и комплекс улик четко указывает на Москву», – пишет исследователь ***(В Twitter насчитали более 20 тысяч «кремлеботов» // Українська правда (http://www.pravda.com.ua/rus/news/2015/04/3/7063616/). – 2015. – 3.04).***

***

Британская газета The Guardian, которая ранее жаловалась на «троллинг» в комментариях, объявила о раскрытии группы проплаченных «троллей» в Санкт-Петербурге. Журналисты издания якобы связались с двумя сотрудниками «фабрики троллей», которые писали посты и комментарии в блогах и на форумах, продвигая смартфон YotaPhone 2.

Бывшие «тролли» рассказали, что они не были трудоустроены официально. Самые большие суммы – около 65 тыс. р. – получали те, кто писал комментарии на английском. О существовании подобных групп издание написало в прошлом году, но тогда предполагалось, что они преследуют лишь политические цели.

Как уверяет The Guardian, «тролли» работали командами из трех человек. Первый начинал дискуссию, остальные двое подключались, размещая ссылки на нужные сайты. В результате каждого обсуждения ее участники должны были прийти к некоему «выводу».

Технические задания придумывались членами группы не самостоятельно, а выдавались «сверху». Они должны были писать хвалебные отзывы о YotaPhone, делать его обзоры, оставлять положительные отзывы и выставлять высокие рейтинги. Оплата за подобные услуги производилась в конвертах, и никаких контрактов, кроме договора о неразглашении, сторонами не заключалось.

Утверждается, что главный офис российских «троллей» находился на улице Савушкина, 55 в Санкт-Петербурге. Работа велась круглосуточно: продолжительность смены составляла 12 часов. Помимо восхваления YotaPhone, в задачи группы входила иная пропагандистская деятельность ***(Британцы раскрыли группу российских «троллей», которые продвигали YotaPhone // InternetUA (http://internetua.com/britanci-raskrili-gruppu-rossiiskih--trollei---kotorie-prodvigali-YotaPhone). – 2015. – 4.04).***

Современные смартфоны и приложения с высокими степенями защиты не позволяют эффективно бороться с проявлениями терроризма, заявил глава Европола Р. Уэйнрайт

По мнению полицейского, скрытые сегменты Интернета, обмен зашифрованными смс-сообщениями препятствуют проведению оперативно-розыскных мероприятий, ведению наблюдения за лицами, которые подозреваются в причастности к терроризму, сообщает BBC.

Р. Уэйнрайт говорит, что понимает коммерческий интерес компаний-производителей смартфонов и приложений с особо надежными системами защиты, однако считает, что данные фирмы должны осознавать последствия применения своих «непробиваемых» шифров с точки зрения борьбы с терроризмом, передает Gpclub.ru.

Вопрос ужесточения защиты личных данных в Интернете остро встал после раскрытия Э. Сноуденом широкомасштабной программы спецслужб США, связанной со слежением за абонентами телекоммуникационных систем по всему миру ***(Главными врагами в борьбе с терроризмом признаны смартфоны // Индустриалка (http://iz.com.ua/mir/67217-glavnymi-vragami-v-borbe-s-terrorizmom-priznany-smartfony.html). – 2015. – 31.03).***

***

Facebook отслеживает страницы, посещаемые европейскими пользователями, даже если они отключили соответствующую опцию или вообще не имеют аккаунта в соцсети. Об этом сообщает газета The Guardian со ссылкой на исследование Бельгийского агентства по защите данных.

Слежение в Европе за теми, кто вообще не зарегистрирован в Facebook, а также за пользователями, которые вышли из учетной записи, происходит за счет плагинов соцсети. В частности, речь идет о кнопке «Нравится», которая встраивается на около 13 млн сайтов.

Facebook отслеживает действия в браузере при помощи cookie-файлов на компьютерах пользователей, когда они посещают любую страницу в домене facebook.com, утверждают исследователи. Это также происходит и в том случае, если пользователь посещает открытую страницу поклонников какой-нибудь знаменитости, для которой не требуется иметь профиль в соцсети. Кроме того, слежение осуществляется даже тогда, когда не происходит никакого взаимодействия с сервисами Facebook на сторонних ресурсах: например, не используется кнопка «Нравится» и не подключается аккаунт соцсети как авторизация для сайта.

Согласно европейскому законодательству, любой сайт должен получить предварительное разрешение пользователя перед тем, как он захочет установить какие-либо cookie-файлы на компьютерах граждан. Кроме того, закон требует от интернет-ресурсов уведомлять пользователей, когда они

впервые посещают сайт, которые использует cookie, и также спрашивать разрешение на их применение.

Facebook в свою очередь сообщила, что доклад Бельгийского агентства по защите данных содержит фактические неточности. «Авторы [исследования] никогда не связывались с нами и даже не пытались прояснить ни одно из предположений, на которых построен их доклад. При этом они не запросили у нас комментарий касательно этой темы перед публикацией доклада», – цитирует представителя соцсети портал The Next Web. Кроме того, по словам компании, она детально объяснила неточности в ранней версии исследования после того как оно было опубликовано напрямую Бельгийскому агентству по защите данных и даже предложила встречу с разъяснением. Однако организация отклонила это предложение, утверждает Facebook.

В обновленных в этом году правилах пользования соцсетью говорится, что компания собирает информацию при посещении пользователем сторонних сайтов и приложений, если они используют сервисы Facebook. Все эти данные требуются компании, чтобы делать таргетинг рекламы более конкретизированным.

Cookie – это файлы, которые хранят на компьютере данные с посещаемых пользователем сайтов, например, это может быть история действий на ресурсе и прочая информация. При каждом визите на конкретный сайт они заново отправляются и могут впоследствии использоваться для идентификации пользователя и слежения за его активностями в сети ***(Facebook уличили в слежке за незарегистрированными в соцсети пользователями // InternetUA (http://internetua.com/Facebook-ulicsili-v-slejke-za-nezaregistrirovannimi-v-socseti-polzovatelyami). – 2015. – 31.03).***

***

Социальная сеть Twitter предоставила владельцам подтвержденных (помеченных синим флажком) аккаунтов возможность бороться с троллями в комментариях. Благодаря новому фильтру верифицированные пользователи смогут удалять оскорбительные твиты, одинаковые сообщения, а также подозрительных и незнакомых участников из своей ленты.

Главная особенность фильтра в том, что он недоступен для обычных пользователей, а владельцы подтвержденных аккаунтов пока могут воспользоваться им только в приложении для iOS. Будет ли этот фильтр доступен для веб-версии сервиса и для Android, пока неизвестно. Однако все пользователи, как и раньше, смогут сообщать о нарушениях в правоохранительные органы, а также применять специальные инструменты для сообщения о преследовании и оскорблениях.

Новая функция была запущена всего через несколько недель после того, как исполнительный руководитель Twitter Д. Костоло заявил, что компания не справляется с потоком оскорблений в соцсети. Он также пообещал, что в будущем для борьбы с троллями будут предприниматься более активные меры ***(Twitter поможет верифицированным пользователям удалить***

оскорбительные твиты из ленты // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_pomozhet_verifitsirovannym_polzovatelyam_udalit_oskorbitelnye_tvity_iz_lenty). – 2015. – 2.04).

***

Російські депутати стурбовані можливістю іноземного впливу на громадську думку.

Голова партії «Родіна», депутат Держдуми від фракції «Єдина Росія» О. Журавльов готує поправки до законодавства, що забороняють в'їзд до Росії іноземцям, які негативно відгукуються про Росію в соцмережах.

Про це повідомляють «Известия».

Парламентарій хоче дати можливість Роскомнагляду на підставі моніторингу ЗМІ та соціальних мереж вести список «неблагонадійних», на базі якого служба зможе забороняти їм в'їзд у країну.

«Дехто з доволі відомих людей, зокрема і з України, приїжджає в Російську Федерацію після того, як вони намагалися максимально дискредитувати її, і влаштовуються на роботу. Та ще й влаштовуються в такі структури, які здатні формувати громадську думку і впливати на політику російської держави», – пояснив О. Журавльов причини появи такої ініціативи.

Ініціатива депутата пов'язана, зокрема, із ситуацією навколо нового ведучого НТВ Д. Грачова. До того як влаштуватися на роботу на російському телебаченні, журналіст критикував у соцмережах позицію Росії і захищав інтереси рідної України. Потім колишній український ведучий вирішив виправдатися і звернувся до російського народу з проханням пробачити йому опубліковані антиросійські пости.

Як повідомив виданню прес-секретар Роскомнагляду В. Ампелонський, у службі поки що не готові прокоментувати очікувані поправки.

На сьогодні підставою для відмови іноземцям у в'їзді на територію Росії можуть стати порушення пропускного, візового режиму, наявність судимостей або несплаченого штрафу, порушення терміну перебування. Право встановлювати заборону на в'їзд мають Міністерство внутрішніх справ, Федеральна служба безпеки, Служба зовнішньої розвідки, Міноборони, Росфінмоніторинг, Мін'юст, Міністерство закордонних справ, Федеральна служба контролю за обігом наркотиків, Федеральна міграційна служба, Росспоживнагляд і Федеральне медико-біологічне агентство ***(У Держдумі запропонували розширити список «нев'їзних» критиками Росії в соцмережах // LB.ua (http://ukr.lb.ua/news/2015/04/02/300626_derzhdumi_zaproponuvali_rozshiriti.html). – 2015. – 2.04).***

***

Через допис у Facebook ФСБ запідозрила мешканку Севастополя в екстремізмі

4 квітня співробітники ФСБ провели обшук у мешканки Севастополя О. Денисової, повідомляє «Центр журналістських розслідувань».

О. Денисову звинуватили в заклику до тероризму в соцмережах через її запис у Facebook у серпні 2014 р. При цьому «правоохоронці» не вказали, який саме запис у соцмережі викликав їх інтерес.

Після обшуку у О. Денисової вилучили комп'ютер.

Як пише сайт «Інформатор», представники ФСБ повідомили О. Денисовій, що судитимуть її за Кримінальним кодексом. Також вона дізналася, що не зможе виїхати на територію України. «Мені заявили, що до суду я не можу поїхати в Україну, хоч я і є українською громадянкою – паспорт на російський не міняла», – розповіла журналістам О. Денисова.

О. Денисова – безробітна вдова з двома неповнолітніми дітьми. Рік тому вона відмовилася від російського громадянства, не підтримавши анексію Криму.

Як зазначає «Центр журналістських розслідувань», 2 квітня проходили масові обшуки в місцях компактного проживання кримських татар в Євпаторії, Джанкої, у Сімферополі, Ленінському, Кіровському, Сімферопольському районах ***(Через допис у Facebook ФСБ запідозрила мешканку Севастополя в екстремізмі // InternetUA (http://internetua.com/cerez-dopis-u-Facebook-fsb-zap-dozrila-meshkanku-sevastopolya-v-ekstrem-zm). – 2015. – 6.04).***

***

Социальный сервис Snapchat выпустил свой первый отчет о доступности сервисов и данных, в котором говорится о сотнях запросов, поступивших от американских и иностранных спецслужб.

Так, в период между 1 ноября 2014 г. и 28 февраля 2015 г. Snapchat получил 375 запросов о предоставлении данных от правоохранительных ведомств США и в 92 % случаев хотя бы частично предоставил требуемые сведения. Об этом пишут Новости ИТ со ссылкой на 3D-News.

«В то время как большинство пользователей Snapchat используют сервис просто для развлечения, важно, чтобы правоохранительные органы имели возможность проводить расследование нелегальной активности. Мы четко заявляем, что будем удовлетворять все правомерные запросы», – указывается в блоге соцсервиса.

За пределами США Snapchat получил 28 запросов из Британии, Бельгии, Франции, Канады, Ирландии, Венгрии и Норвегии. Требуемая информация была предоставлена в шести случаях.

Snapchat пополнил ряды крупных технокомпаний, среди которых Google, Yahoo!, Facebook, Twitter и Microsoft, выпускающих подобные доклады. Так же, как и большинство своих собратьев, социальный сервис выступает против внедрения бэкдоров, позволяющих спецслужбам получить доступ к данным пользователей.

Пока Snapchat не включал в свой первый отчет данные о запросах, касающихся национальной безопасности США, поскольку они могут быть

опубликованы только по прошествии шести месяцев. Компания намерена обнародовать более детальную информацию о государственных запросах и требованиях об удалении определенного контента в следующем докладе, который будет выпущен в июле этого года ***(Snapchat предоставляет информацию по запросу спецслужб в 92 % случаев // Новости ИТ (http://www.novostiit.net/snapchat-predostavlyaet-informatsiyu-po-zaprosu-spetssluzhb-v-92-sluchaev-00018692). – 2015. – 5.04).***

***

АНО «Центр исследований легитимности и политического протеста» в России работает над электронной базой несанкционированных акций и митингов. Речь идет об информации о планируемых мероприятиях, которая будет автоматически обновляться каждые 10 минут.

Акция протеста

Директор АНО Е. Ведендиктов сообщил, что новая система сможет мониторить экстремистские группы в соцсетях – Facebook, «ВКонтакте», LiveJornal и Twitter – и делать анализ появляющегося контента и действий пользователей. Информация о месте и времени незапланированной акции новая система будет передавать в правоохранительные органы, а также – через специальное мобильное предложение – пользователям, которые хотят избежать столкновений с радикально настроенными гражданами.

Запуск нового сервиса запланирован на сентябрь текущего года. Разработчики отмечают, что заимствовали опыт египетских коллег, которые выпустили подобную базу для наблюдения за массовыми протестами против бывшего президента страны М. Мурси в 2013 г. Однако ближневосточные специалисты анализируют только хэштэги и сообщения в Twitter, в то время как сотрудники российского центра хотят отслеживать популярные социальные сети комплексно.

В LiveJornal особое внимание будет уделено текстам и комментариям, в Facebook и «ВКонтакте – лайкам и репостам, поскольку аналитики из Египта уже вывели взаимосвязь между ростом их количества и приближением даты акции.

В России проведение несанкционированных митингов без предварительного уведомления запрещено федеральным законом и влечет за собой наложение штрафа в размере 20–200 тыс. р. (суммы разнятся для граждан, должностных и юридических лиц) ***(В России создают ПО для отслеживания массовых акций протеста // IT новости (http://itnovosti.org.ua/2015/04/internet/socialnye-seti/v-rossii-sozdayut-po-dlya-otslezhivaniya-massovyx-akcij-protesta.html). – 2015. – 6.04).***

***

Журналист Я. Элма из провинции Газиантеп на юго-востоке Турции получил условный 23-месячный тюремный срок, поставив «лайк» к сообщению в Facebook с критикой президента страны Т. Эрдогана.

Как передает РИА «Новости», критический комментарий в адрес президента Турции суд Газиантепа счел «оскорблением государственного служащего», а журналиста, которому он понравился, приговорил к 28-месячному тюремному заключению, снизив затем срок до 23 месяцев и постановив считать его условным.

«Я просто использовал функцию “нравится” в Facebook, прочитав комментарий о президенте. Я удалил свой лайк через полчаса, но ко мне уже приехала полиция. Не знал, что это является преступлением», – сказал Я. Элма в интервью агентству DHA.

Его адвокат Д. Демирель заявила, что будет обжаловать это судебное решение, подчеркнув, что суд принял осуждение за оскорбление, не конкретизируя эти понятия. «Мы считаем, что постановление суда противоречит закону. Политические деятели должны мириться даже с жесткой критикой», – сказала она.

По турецким законам за оскорбление суды могут назначать наказание в виде реального тюремного заключения сроком до трех месяцев. Однако если истец является государственным служащим, тюремный срок может быть увеличен до одного года. Если оскорбление нанесено через средства массовой информации, закон предусматривает дополнительное увеличение тюремного срока.

Более 70 человек в Турции были подвергнуты уголовному преследованию за оскорбление Т. Эрдогана после того, как он был избран президентом страны в августе 2014 г. Сотни подобных дел возбуждались, когда он находился на посту премьер-министра Турции ***(Журналиста в Турции приговорили к 23 месяцам тюрьмы условно за «лайк» против президента // InternetUA (http://internetua.com/jurnalista-v-turcii-prigovorili-k-23-mesyacam-tuarmi-uslovno-za--laik--protiv-prezidenta). – 2015. – 7.04).***

***

6 апреля представители патриотически настроенной организации Правый сектор лишились одного из своих важнейших ресурсов в Интернете.

В частности, на их официальном сайте в социальной сети «ВКонтакте» появилась надпись: «Данный материал заблокирован по требованию Роскомнадзора на основании решения Генеральной прокуратуры № 27-27-2014/Ид670-14 от 10.04.2014.»

Пока что лидеры организации не комментируют эту ситуацию. Хотя много вопросов вызывает то, каким образом на территории нашей страны могут действовать законы другого государства ***(Сайт херсонского Правого сектора заблокирован русскими спецслужбами! // Kherson.in (http://kherson.in/news/sajt_hersonskogo_pravogo_sektora_zablokirovan_russkimi_spetssluzhbami). – 2015. – 6.04).***

***

Служба безопасности Украины прекратила функционирование ряда украинских интернет-сайтов, которые, как утверждается, использовались для проведения акций информационной агрессии со стороны России. Об этом на своей странице в Facebook написал советник главы СБУ М. Лубкивский, сообщает Корреспондент.

По его словам, сотрудники СБУ на основании судебного решения изъяли серверы крупного доменного регистратора Nic.ua, с помощью которых осуществлялась техническая поддержка «пророссийских интернет-ресурсов».

«Вскоре мы предоставим общественности более расширенную информацию о прекращении нами деятельности интернет-ресурсов и сайтов, которые пропагандировали сепаратизм, терроризм, прославляли так называемые “ДНР” и “ЛНР”, распространяли московскую пропаганду», – отметил М. Лубкивский.

Как сообщалось, накануне компания Nic.ua заявила, что представители госорганов проводят обыск и изымают их сервера из дата-центра ***(СБУ продолжает закрывать украинские сайты за распространение московской пропаганды // Индустриалка (http://iz.com.ua/ukraina/67871-sbu-prodolzhaet-zakryvat-ukrainskie-sayty-za-rasprostranenie-moskovskoy-propagandy.html). – 2015. – 8.04).***

***

Власти Китая создали новое кибероружие, и если «Великий китайский файрвол» (Great Firewall) служит средством обороны, то новый инструмент – средством нападения, сообщила исследовательская лаборатория Citizen Lab при Университете Торонто в Канаде. Аналитики назвали новую систему «Великой китайской пушкой» (Great Cannon).

«Великая китайская пушка» перехватывает трафик, идущий к серверам китайской поисковой системы Baidu, и в ответный трафик внедряет вредоносные скрипты JavaScript. Они подключают компьютер пользователя, изначально отправившего запрос, к ботнету, с помощью которого власти Китая проводят DDoS-атаки.

По словам исследователей, неважно, из какой страны поступает запрос к Baidu. Если этот запрос соответствует определенным критериям, Great Cannon внедряет в обратный трафик вредоносный скрипт. Аналитики определили, что такие скрипты помещаются приблизительно в 1,75 % случаях.

Новая система не предназначена для проверки содержимого трафика, эту функцию выполняет «Великий китайский файрвол». Она также не отвечает за цензуру, то есть не блокирует доступ к материалам, а помогает властям бороться с инструментами, позволяющими китайским пользователям обходить Great Firewall, то есть нарушать запреты.

Исследователи рассказали, что обнаружить Great Cannon позволил анализ DDoS-атаки (распределенной атаки типа «отказ в обслуживании»), проведенной в марте 2015 г. против ресурсов GreatFire.org и GitHub.com.

GreatFire.org – оппозиционная по отношению к правительству КНР организация, занимающаяся мониторингом ресурсов, блокируемых «Великим китайским файрволом», и публикующая список прокси-серверов, позволяющих пользователям в Китае эту блокировку обходить. В свою очередь, GitHub – популярный ресурс для обмена исходным кодом и совместной разработки приложений. Среди множества других проектов на нем размещены исходные коды приложений, предназначенных для преодоления интернет-фильтра.

Совершив DDoS-атаки на GreatFire.org и GitHub.com, Пекин попытался вывести из строя эти ресурсы и тем самым заблокировать доступ пользователей в Китае к инструментам и справочным материалам, позволяющим обходить установленный в стране интернет-фильтр. Иными словами, власти попытались ввести цензуру и за пределами государства.

«Развертывание “Великой китайской пушки” свидетельствует об усилении государственной цензуры, выходе на новый уровень», – резюмировали в Citizen Lab, добавив, что ранее стало известно об использовании подобной системы Агентством национальной безопасности АНБ в США и Центром правительственной связи в Великобритании.

Аналитики просмотрели IP-адреса, с которых осуществлялась DDoS-атака на GreatFire.org. Большинство адресов указывали на сети на Тайване и в Гонконге – 66,9 %. В обоих этих регионах Китай является официальным языком. На сам Китай же пришлось 18 % адресов.

Выбор серверов Baidu обусловлен большим числом запросов к ним из разных уголков планеты. Согласно статистике Alexa, Baidu – самый популярный китайский сайт среди всех сайтов в мире и четвертый по популярности в мире.

Система, описанная в марте 2014 г. изданием The Incertept на основе документов, предоставленных Э. Сноуденом, предназначена для инфицирования миллионов ПК по всему миру с целью слежки ***(Китай создал технологию для введения цензуры в Сети по всему миру // InternetUA (http://internetua.com/kitai-sozdal-tehnologiua-dlya-vvedeniya-cenzuri-v-seti-po-vsemu-miru). – 2015. – 12.04).***

***

Роскомнадзор получил право проверять личную переписку пользователей социальных сетей, среди которых – «Одноклассники» и «ВКонтакте», электронную почту и мессенджеры Агент.Mail.ru, ICQ, а также блог-платформы.

Соответствующее постановление подписал премьер-министр России Д. Медведев.

Отмечается, что данные меры были приняты в рамках «антитеррористического» пакета для защиты прав граждан России.

Согласно документу, ведомство в праве устанавливать факт приема, передачи, доставки и обработки сообщений, а также просматривать и анализировать ресурсы организатора распространения информации.

Также постановление дает право записывать и фиксировать действия, доступные пользователям.

Проверять переписку Роскомнадзор сможет только по запросу правоохранительных органов, ведущих оперативно-розыскные мероприятия. Сама проверка будет проходить два раза, при этом вторая – не менее чем через 60 дней.

В свою очередь в Роскомнадзоре заявили, что постановление о проверках организаторов распространения информации не делает содержимое переписки пользователей соцсетей доступным для ведомства, передает РБК.

Как заявил спикер Роскомнадзора В. Ампелонский, ведомство сможет узнавать только о фактах передачи информации пользователями, но не видеть сами сообщения.

Ранее сообщалось, что по требованию прокуратуры Роскомнадзор будет заниматься блокировкой всех найденных копий информации с ресурсов с запрещенной или экстремистской деятельностью ***(В России разрешили контролировать переписку в соцсетях и блогах // Украинская правда (http://www.pravda.com.ua/rus/news/2015/04/13/7064586/). – 2015. – 13.04).***

Проблема захисту даних. DDOS та вірусні атаки

Вредоносное ПО, перехватывающее настройки DNS в маршрутизаторах, не является чем-то новым. Тем не менее, разработанные в последнее время эксплоиты позволяют осуществлять операции перехвата с использованием одного лишь JavaScript. Специалисты компании Ara Labs обнаружили новую схему, в которой злоумышленники используют перехват DNS, после чего подменяют теги Google Analytics и встраивают в посещаемые жертвой страницы неотключаемую рекламу. Результаты своего исследования эксперты опубликовали в блоге компании.

Киберпреступники перенаправляют DNS-запросы к домену google-analytics.com на поддельный сайт, где на устройства жертв загружается вредоносный сценарий JavaScript. В дальнейшем он встраивает навязчивые рекламные сообщения (в некоторых случаях вся посещаемая страница оказывается заполненной трудноотключаемой рекламой) на веб-сайты, использующие Google Analytics для показа таргетированных объявлений своим посетителям. Отметим, что это не является уязвимостью в самом Google Analytics – киберпреступники решили использовать площадку от Google в связи с ее популярностью.

В данном случае мошенники использовали пару DNS-серверов 91.194.254.105 (основной) и 8.8.8.8 (дополнительный). Основной DNS-сервер принадлежит злоумышленникам, в то время как дополнительный используется компанией Google в качестве публичного DNS-сервера. Большинство DNS-запросов разрешаются через дополнительный сервер, но когда происходит попытка запроса DNS к google-analytics.com, основной DNS-сервер возвращает

ответный IP 195.238.181.169, который ведет на контролируемый злоумышленниками сайт.

Когда жертва посещает сайт, использующий Google Analytics, и пытается загрузить стандартные скрипты с сервера, злоумышленники передают вредоносный JavaScript, который вставляет рекламу на веб-сайт. В некоторых случаях вредоносный файл маскируется под легитимный скрипт Google Analytics.

Инъекции вредоносных рекламных сообщений производились с доменов zinzimo.info, ektezis.ru и patifill.com, которые принадлежат российской рекламной сети Popunder. Она специализируется на размещении всплывающих рекламных объявлений ***(Вредоносное ПО перехватывает DNS-запросы маршрутизаторов // InternetUA (http://internetua.com/vredonosnoe-po-perehvativaet-DNS-zaprosi-marshrutizatorov). – 2015. – 29.03).***

***

Исследователи из Университета Алабамы в Бирмингеме (США) разработали новый способ детектирования вредоносных программ на мобильных устройствах, который может существенно повысить эффективность работы антивирусных средств.

Об этом пишут Новости ИТ со ссылкой на 3D-News.

Предложенный инструмент нацелен на выявление зловредов, которые способны без ведома пользователя совершать звонки или отправлять SMS на платные номера, активировать камеру, а также NFC-соединение. Принцип работы системы основан на том, чтобы выявить различия между командами, отдаваемыми человеком и программой.

Для этого антивирусный инструмент анализирует данные от встроенных в гаджет датчиков – акселерометра, гироскопа, сенсоров освещённости и приближения. Система формирует «цифровой портрет» тех действий и жестов, которые обычно выполняет пользователь, скажем, при инициации телефонного вызова. Если при последующей попытке набора номера окажется, что такой портрет не имеет ничего общего с характером выполняемых операций, будет сделан вывод о том, что установка соединения с большой вероятностью осуществляется без ведома владельца аппарата. В этом случае вызов может быть заблокирован.

Исследователи отмечают, что предложенная технология не требует root-доступа к устройству и демонстрирует высокую аккуратность. К тому же система работает даже в том случае, если информация о зловреде не занесена в антивирусные базы данных.

В перспективе новая методика может дополнить традиционные средства обеспечения безопасности ***(Анализ данных от сенсоров смартфона поможет выявить вредоносное ПО // Новости ИТ (http://www.novostiit.net/analiz-dannyih-ot-sensorov-smartfona-pomozhet-vyiyavit-vredonosnoe-po-00018397). – 2015. – 30.03).***

***

Популярный протокол шифрования данных SSL/TLS оказался подвержен уязвимости, позволяющей поставить под угрозу конфиденциальную информацию. Специалист компании Imperva И. Мантин смог раскрыть важные данные с помощью эксплуатации бреши 13-летней давности, связанной с использованием слабозащищенного алгоритма RC4. В настоящее время RC4 используется для защиты более 30 % всего SSL/TLS-трафика в Интернете.

Результаты исследования были опубликованы в отчете «Атака на SSL с помощью RC4» (Attacking SSL when using RC4). Помимо этого, эксперт лично представил свои находки во время конференции Black Hat Asia, которая прошла в Сингапуре 26 марта.

Нападение «бар-мицва» (Bar-Mitzvah) не требует осуществления атаки «человек посередине» между клиентом и сервером. В ходе атаки эксплуатируется слабый паттерн в ключах RC4, позволяющий раскрыть важные данные, передаваемые по SSL/TLS, в текстовом виде. Соблюдая некоторые условия, хакер может получить логин и пароль жертвы, ее финансовую информацию и прочие конфиденциальные данные.

«Безопасность алгоритма RC4 многие годы вызывала сомнение у экспертов, в особенности его механизмы инициализации, – сообщается в отчете Imperva. – Тем не менее, осознание слабостей в RC4 и отказ от его использования последовал лишь в последние годы». Отметим, что «бар-мицва» стала первой практически осуществимой атакой, требующей лишь пассивного наблюдения за SSL/TLS-соединениями ***(Уязвимость 13-летней давности в SSL/TLS упрощает хищение конфиденциальных данных // InternetUA (http://internetua.com/uyazvimost-13-letnei-davnosti-v-SSL-TLS-uprosxaet-hisxenie-konfidencialnih-dannih). – 2015. – 31.03).***

***

Некоммерческие компании сомневаются, выполняет ли правительство США свои обещания по информированию производителей ПО о наличии в их продуктах уязвимостей. Об этом сообщается в блоге организации Electronic Frontier Foundation (EFF).

Как сообщили представители EFF в понедельник, 30 марта, в результате судебного разбирательства они получили ряд значительно отредактированных документов от Управления директора национальной разведки США (Office of the Director of National Intelligence, ODNI). Причиной иска стала медлительность ведомства и АНБ в обработке запроса, поданного в июле прошлого года в рамках Акта о свободе информации (Freedom of Information Act, FOIA).

EFF интересовалась документами, связанными с правительственной программой Vulnerability Equities Process (VEP). Она предусматривает, что власти США будут сотрудничать с производителями ПО и сообщать им об обнаруженных уязвимостях нулевого дня в их продуктах.

Тем не менее, специалисты некоммерческой организации опасаются, что правительство США слишком долго удерживает эту информацию. В результате существенно возрастает риск компрометации продуктов, в которых были обнаружены уязвимости, в то время как американские власти обязались защитить их от потенциальных атак со стороны других государств.

По данным правительства США, компании немедленно уведомляются об уязвимостях в их ПО, но в случае угрозы нацбезопасности эта информация временно удерживается. Как сообщил коорди. Обамы М. Дэниел в блоге Белого дома, в случаях, когда данные о брешах позволяют отразить нападение террористов, информация временно удерживается и не разглашается ***(Правозащитники сомневаются в политике разглашения уязвимостей властей США // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/31/government-says-it-has-policy-disclosing-zero-days.html). – 2015. – 31.03).***

***

Специалисты ИБ-компании Symantec сообщили о новом трояне-шпионе, получившем название Trojan.Laziok (по классификации Symantec). Вредонос действует в качестве разведывательного инструмента, позволяющего злоумышленникам собрать необходимую информацию для адаптации методов атаки на каждый скомпрометированный компьютер.

В период с января по февраль текущего года эксперты зафиксировали многоступенчатую кампанию, нацеленную на размещенные по всему миру энергетические предприятия. Под особо пристальное внимание злоумышленников попали Средневосточные компании.

По данным Symantec, самым таргетируемым регионом оказались Объединенные Арабские Эмираты (25 %), чуть меньше случаев инфицирования зарегистрировано в Саудовской Аравии, Пакистане и Кувейте (по 10 % в каждой стране), на последнем месте оказались Камерун, Колумбия, Уганда, Катар, Оман, Индия, Индонезия, США и Великобритания (по 5 %).

Как выяснилось, большинство целевых компаний были связаны с нефтяной, газовой или гелиевой промышленностью, что позволяет предположить наличие у злоумышленников стратегического интереса в бизнес-операциях данных предприятий.

Руководствуясь собранной трояном информацией, преступники принимали критические решения о дальнейшем ходе атаки – продолжать или остановить. Троян распространялся в спам-письмах, к которым прикреплялось вредоносное вложение в виде документа Excel, содержащее эксплоит для уязвимости в Microsoft Windows (CVE-2012-0158), позволяющей выполнить произвольный код на целевой системе. Открытие жертвой файла Excel приводит к исполнению кода эксплоита, после чего происходит инфицирование целевой системы. Троян скрывается в директории %SystemDrive %\Documents and Settings\All Users\Application Data\System\Oracle, где создает новые папки и переименовывает себя.

Вредонос собирал следующую информацию: имя компьютера, установленное ПО, объемы ОЗУ и жесткого диска, а также данные о процессоре и присутствующих в наличии антивирусах. Все полученные сведения троян отправлял злоумышленникам, которые затем инфицировали компьютер дополнительным вредоносным ПО ***(Новый троян-шпион атакует мировые энергетические компании // InternetUA (http://internetua.com/novii-troyan-shpion-atakuet-mirovie-energeticseskie-kompanii). – 2015. – 1.04).***

***

Check Point Software опубликовал отчет об обнаружении группы злоумышленников, которая, вероятно, происходит из Ливана и связана с его политическими силами.

Исследователи из подразделения Check Point Malware and Vulnerability Research Group обнаружили систему Volatile Cedar, которая использует для атак специально разработанное вредоносное ПО под кодовым названием Explosive. Кампания стартовала еще в начале 2012 г., в ее рамках были проведены успешные атаки на целый ряд ресурсов по всему миру. В результате этих атак злоумышленники получили возможность отслеживать действия жертв и похищать их данные.

Мы можем подтвердить, что на сегодняшний день в число жертв группировки входят организации оборонной промышленности, телекоммуникационные и медиакомпании, а также образовательные учреждения. Природа атак и их последствия говорят о том, что целью злоумышленников является получение не финансовых выгод, а доступа к конфиденциальной информации жертв атак.

Ключевые результаты исследования:

• Volatile Cedar – это целенаправленная и прекрасно организованная кампания. Она направлена на тщательно выбранные организации, при этом масштаб заражения держится под контролем, что позволяет злоумышленникам выполнять задачи с минимальным риском обнаружения.

• Первые доказательства функционирования Explosive появились в ноябре 2012 г. С тех пор было обнаружено несколько версий этого вредоносного ПО.

• Метод работы данной преступной группировки заключается в атаках на доступные извне веб-серверы, при этом поиск уязвимостей выполняется как в автоматическом, так и в ручном режиме.

• Получив доступ к серверу и контроль над ним, злоумышленник может использовать его как опорную точку для изучения, идентификации и атак на дополнительные ресурсы, находящиеся в сети организации. Мы обнаружили признаки как попыток онлайн-проникновения, так и механизма распространения вредоносного ПО через зараженные USB-носители.

«Volatile Cedar – это очень интересная вредоносная кампания. Она успешно работает на протяжении долгого времени, избегая обнаружения за счет хорошо спланированных и аккуратно управляемых процессов. Система постоянно отслеживает действия своих жертв и моментально реагирует на

инциденты обнаружения, – говорит Д. Вайли, глава подразделения Incident Response & Threat Intelligence Check Point Software Technologies. – Это один из образов целевых атак будущего: вредоносное ПО тихо наблюдает за сетью, похищает данные и может быстро сменить стратегию действий при обнаружении антивирусным приложением. Поэтому организациям нужно использовать проактивный подход к обеспечению безопасности своих сетей».

Клиенты Check Point уже защищены от Volatile Cedar за счет наличия множественных сигнатур на различных уровнях защиты, а также блейдов ThreatCloud, которые способны распознавать все варианты вредоносного ПО Explosive. Организации могут защитить себя от атак, подобных Volatile Cedar, применяя продвинутую инфраструктуру безопасности, которая включает в себя правильную сегментацию ЛВС с помощью межсетевых экранов, IPS, систему анти-бот, своевременную установку патчей и контроль использования приложений ***(Check Point обнаружил глобальную шпионскую кампанию из Ливана // ITnews (http://itnews.com.ua/news/76566-check-point-obnaruzhil-globalnuyu-shpionskuyu-kampaniyu-iz-livana). – 2015. – 2.04).***

***

Международная антивирусная компания Eset предупреждает о росте активности трояна Win32/TrojanDownloader.Waski, нацеленного на пользователей из стран Европы.

Троян-загрузчик Win32/TrojanDownloader.Waski известен с 2013 г. В настоящее время он все более активно используется киберпреступниками. Среди пострадавших преобладают пользователи из Великобритании, Ирландии, Литвы, Испании, Украины, а также Турции и Канады.

Waski распространяется в спам-рассылке, имитирующей официальные сообщения с корпоративных адресов электронной почты. По мнению экспертов Eset, некоторые отправители реально существуют, и их ПК, рассылающие спам, входят в состав ботнета. Обнаруженные сообщения написаны на английском и немецком языках, но встречаются и другие варианты, сообщили CNews в компании.

Файл Waski, замаскированный под документ pdf, содержится в приложенном к письму архиве. После установки троян обращается к удаленному серверу, направляет данные о зараженном ПК и загружает другие вредоносные программы. Выполнив эти действия, Waski передает на командный сервер информацию об успешном заражении.

С помощью Waski распространяется, в частности, троян Win32/Battdil, предназначенный для кражи данных онлайн-банкинга. Вредоносное ПО действует в популярных браузерах (Firefox, Chrome, Chromium, Internet Explorer), перехватывая аутентификационные данные пользователя, которые затем отправляются в зашифрованном виде на удаленный сервер.

Вирусная лаборатория Eset рекомендует игнорировать спам-сообщения и вложения, полученные от неизвестных отправителей ***(Троян атакует***

банковские счета пользователей // InternetUA (http://internetua.com/troyan-atakuet-bankovskie-scseta-polzovatelei). – 2015. – 3.04).

***

В базе данных Apache Cassandra была обнаружена уязвимость, позволяющая удаленному пользователю скомпрометировать систему. Брешь с идентификатором CVE-2015-0225 нашел исследователь безопасности Г. Гешев. Она затрагивает версии 1.2.x, 2.0.x и 2.1.x программного продукта.

Уязвимость существует из-за того, что в конфигурации по умолчанию Cassandra привязывает интерфейс JMX/RMI ко всем сетевым интерфейсам без предварительной аутентификации. Поскольку RMI позволяет осуществить транспортировку и удаленное выполнение сериализованного Java-кода, любой злоумышленник с доступом к интерфейсу может выполнить произвольный код с правами текущего пользователя.

Для того чтобы исправить уязвимость, следует установить исправление с сайта производителя. Поскольку линейка 1.2.x более не поддерживается, ее пользователям потребуется перейти на более новые версии Apache Cassandra ***(Уязвимость в Apache Cassandra позволяет скомпрометировать систему // InternetUA (http://internetua.com/uyazvimost-v-Apache-Cassandra-pozvolyaet-skomprometirovat-sistemu). – 2015. – 6.04).***

***

Злоумышленники используют файл .swf для осуществления инъекции скрытого iFrame. С помощью данной кампании мошенникам удалось скомпрометировать множество сайтов на базе WordPress и Joomla. Напомним, ранее подобный инжектор iFrame был обнаружен в файле .swf Adobe Flash. ИБ-специалисты Sucuri считают, что, вероятно, автор данных вредоносных программ один и тот же.

Вредоносный файл всегда находится в images/banners/, его название состоит из трех случайных символов с последующими .swf и с идентификационным параметром: xyz.swf?myid=1d57987c38051fdc93ea7393b448003e. Имена переменных и логика кодирования очень похожи на те, что использовались в Adobe Flash. Тем не менее, отличается сайт-источник загрузки вредоносного ПО.

ИБ-специалисты не могут назвать точное число инфицированных сайтов на базе WordPress и Joomla. Радует то, что половина антивирусных программ способны обнаружить данный вредонос ***(Участились атаки с использованием вредоносного инжектора iFrame // InternetUA (http://internetua.com/ucsastilis-ataki-s-ispolzovaniem-vredonosnogo-injektora-iFrame). – 2015. – 5.04).***

***

В нескольких библиотеках JSON Web Token (JWT) обнаружены уязвимости, позволяющие злоумышленнику обойти процесс верификации. Об этом сообщает канадский исследователь безопасности Т. МакЛин.

JWT представляет собой стандарт по созданию и обмену токенами между двумя сторонами. К примеру, сервер может создать администраторский токен, переданный по JSON и подписанный ключом сервера. Клиенты могут им воспользоваться для проверки того, что пользователь аутентифицирован как администратор.

По словам Т. МакЛина, уязвимость существует из-за ошибки в алгоритме асимметричной криптографии. Из-за этого возникает лавинный эффект между системами, подписанными с помощью хеш-функции HMAC и с помощью RSA.

«Если сервер ожидает получить токен, подписанный с помощью RSA, но получает токен, подписанный по HMAC, он посчитает HMAC-ключ открытым. Проблема в том, что HMAC-ключи должны быть закрытыми, но из-за этой ошибки они становятся открытыми», – объяснил Т. МакЛин в своем блоге.

В данном случае злоумышленник с доступом к открытому ключу может воспользоваться им как закрытым токеном, а вследствие вышеуказанной ошибки сервер примет его. Т. МакЛин советует всем, кто пользуется любой имплементацией JWT, не принимать токены с разными подписями с помощью механизма белых или черных списков ***(Уязвимости в библиотеках JWT позволяют обойти ограничения безопасности // InternetUA (http://internetua.com/uyazvimosti-v-bibliotekah-JWT-pozvolyauat-oboiti-ogranicseniya-bezopasnosti). – 2015. – 4.04).***

***

Во вторник, 31 марта, американский CERT опубликовал уведомление об уязвимости в системе mDNS (multicast Domain Name System). Найденная брешь может эксплуатироваться для получения доступа к важным данным внутри локальной сети и проведения DDoS-атак.

Среди уязвимых производителей называют такие компании, как Canon, HP и IBM. Продукты Cisco, D-Link и Microsoft не подвержены уязвимости, а устройства от Apple и Dell остаются под вопросом.

mDNS используется для упрощения конфигурации сети, а также для интеграции сетевых сервисов. Проблема состоит в том, что некоторые устройства с поддержкой mDNS могут отвечать на запросы, полученные из Интернета, предоставляя злоумышленникам доступ к потенциально важным данным о сетевых устройствах, присутствующих в локальной сети.

Для того, чтобы проверить наличие уязвимости, достаточно отправить стандартный DNS-запрос на порт 5353. Если ответ на такой запрос получен, то злоумышленник сможет использовать WAN-интерфейс для дальнейших действий. Масштаб возможной утечки данных зависит от особенностей конкретного устройства. Это могут быть серийные номера, информация о конфигурации локальной сети и прочее.

Для устранения уязвимости рекомендуется блокировать входящие и исходящие запросы на порт UDP 5353 ***(Обнаружена опасная уязвимость в реализации mDNS // InternetUA (http://internetua.com/obnarujena-opasnaya-uyazvimost-v-realizacii-mDNS). – 2015. – 4.04).***

***

Даже хорошо подготовленные компании не готовы к опасным кибератакам

Согласно результатам исследования IT-компании Computing Technology Industry Association (CompTIA), 54 % бизнес-организаций США осведомлены об увеличении числа кибератак на предприятия, 48 % в курсе, что злоумышленники используют для своих кампаний сложные инструменты, и 52 % не сомневаются в высокой организации кибернападений. К сожалению, большинство даже хорошо подготовленных американских компаний не готовы к опасным кибератакам.

58 % бизнес-организаций чаще всего используют инструменты для предотвращения потери данных, 57 % компаний обращаются к управлению идентификацией и доступом, 49 % предприятий эксплуатируют технологию управления информационной безопасностью и киберинцидентами. По словам ИБ-экспертов CompTIA, технологии являются только одним из многих компонентов нового подхода для борьбы с киберугрозами.

Старший управляющий по анализу технологий CompTIA С. Робинсон уверен, что бизнес-компании должны сосредоточиться на формальном анализе риска кибератак. Предприятиям необходимо удостовериться, что реализуемые ими методы обеспечения безопасности не ставят их под угрозу кибернападения.

52 % опрошенных предприятий сообщили, что межсетевые взаимодействия добавили работы системам защиты. Предприятия используют сервисы хранения данных и мобильные технологии, что увеличило риск кибернападений. С. Робинсон уверен, что бизнес-компаниям необходимо усовершенствовать подходы к обеспечению безопасности.

Специалист также добавил, что большую роль в защите предприятий играет человеческий фактор. Множество проблем безопасности компаний создают сами сотрудники. Согласно статистике, только 54 % предприятия вкладывают деньги в обучающие ИБ-тренинги и курсы для своих работников ***(Даже хорошо подготовленные компании не готовы к опасным кибератакам // InternetUA (http://internetua.com/daje-horosho-podgotovlennie-kompanii-ne-gotovi-k-opasnim-kiberatakam). – 2015. – 5.04).***

***

Як захистити розмови, SMS та чати шифруванням

Значно ускладнити шпигування за вами можна, якщо проводити всі переговори та листування по телефону в зашифрованому вигляді. Для цього не потрібно купувати дорогі гаджети з вбудованими функціями такого захисту. Можна їх додати до свого Android.

Секретні чати

Листування без сторонніх очей можна вести в програмі Wickr-Top Secret Messenger. Її створили спеціалісти з комп’ютерної безпеки, які отримали ідею

на хакерській конференції Def Con. Головна мета цієї утиліти – надати захищений від спецслужб канал зв'язку, для чого використовується шифрування військового рівня. Крім того, усі повідомлення та файли самознищуються через встановлений термін. Тому, запевняють розробники, користувачів неможливо буде визначити навіть після захоплення сервера цього чату.

Шифровані SMS

Популярна утиліта для відправлення захищених коротких повідомлень TextSecure вже не підтримується автором. Тому в неї з'явився клон SMSSecure, який надає ще надійніше шифрування. Ця програма використовує 256-бітний симетричний шифр AES (замість 128-бітного у TextSecure) та 192-бітне шифрування еліптичними кривими (замість 160-бітного). SMSSecure недоступна у PlayStore, і її потрібно завантажувати зі сторінки розробника.

Захищені телефонні розмови

Власники смартфонів Android можуть захистити не тільки текстове листування, а й голосові переговори. Їм допоможе утиліта RedPhone, яка створена на базі програмного забезпечення волонтерської групи Open Whisper Systems. Остання займається тим, що робить приватні комунікації простішими.

Скористатися RedPhone досить просто, адже вона інтегрує в себе номер телефону SIM-картки користувача. Розмови проходитимуть як звичайно та без зайвих дій, але всі дані пересилатимуться зашифрованими. Для цього необхідно, щоб співрозмовник також користувався цією програмою, а також швидкісний Інтернет ***(Як захистити розмови, SMS та чати шифруванням // InternetUA (http://internetua.com/yak-zahistiti-rozmovi--SMS-ta-csati-shifruvannyam). – 2015. – 8.04).***

***

Мошенническая сеть, обманом получающая деньги от доверчивых пользователей Skype, насчитывает более 10 офисов в России и СНГ и несколько сотен аккаунтов. Об этом анонимный участник организации рассказал пользователю «Хабрахабра» под ником MaxxArts.

По словам анонимного сотрудника сети мошенников, только в их организации насчитывается семь офисов в России и ещё четыре в странах СНГ. Работа происходит по сменам: в его команде состоит семь человек, вероятно, столько же людей и во второй смене, предположил вымогатель.

Сами участники проекта не знают, откуда берутся взломанные аккаунты Skype и номера кошельков, на которые они просят переводить деньги. В основном используются кошельки Qiwi, реже – «Яндекс.Деньги», так как их «дороже персонализировать», пояснил анонимный представитель.

Работники организации должны обладать определённой квалификацией: по словам мошенника, в офис пускают только после прочтения двух книг по психологии. Иногда в чатах злоумышленники специально читают предыдущую переписку, чтобы лучше влиться в общение, однако это не всегда возможно по причине огромного числа одновременных диалогов: от трёх до 20.

В качестве целей обычно выбираются пользователи из списка контактов, которые выглядят платёжеспособно: чем старше человек, тем лучше. Если возраст не указан в профиле, на «серьёзность» человека может указывать его ник или полностью заполненное ФИО.

В месяц один сотрудник по плану должен «зарабатывать» не менее 100 тыс. р., из которых он получает 40 %. При «переработке» выплачивается уже 50 % от полученной суммы, однако её верхний потолок ограничен 200 тыс. р.: с чем это связано, мошенник не уточнил.

С одной «жертвы» разрешается брать не больше 14 тыс. р., уточнил собеседник. Это может быть связано с ограничениями на перевод в популярных платёжных системах в 15 тыс. р. Если предположить, что в каждом из 11 офисов работает по 14 сотрудников, то годовой оборот такой компании составляет около 180 млн р.

Для обеспечения безопасности самих сотрудников используются выделенные серверы с настроенным VPN-подключением, однако сотрудников и самих запугивают компроматом, заявил интервьюируемый участник группировки.

Думаю, тех мер безопасности, которые они устраивают, хватает. В любом случае, если что – мы под давлением. Если не работаешь – на тебя что-то найдут. Или что-то сделают… Не хочу об этом сейчас. Анонимный участник мошеннической группировки

По словам анонимного мошенника, работу он нашёл через объявление, однако на вопрос, как именно оно звучало, отвечать отказался.

17 марта блогер и предприниматель С. Доля рассказал о взломе аккаунта Skype PR-директора Acronis Е. Турцевой: злоумышленники обманом просили перевести её друзей 15 тыс. р. на «Яндекс.Кошелёк». Тогда собеседник отказался давать интервью, а в Skype отказались комментировать ситуацию ***(Мошенники рассказали о международном бизнесе по обману пользователей Skype // InternetUA (http://internetua.com/moshenniki-rasskazali-o-mejdunarodnom-biznese-po-obmanu-polzovatelei-Skype). – 2015. – 9.04).***

***

Группа исследователей IT-сервиса ScrapeSentry обнаружила скрытый функционал в популярном бесплатном расширении для браузера Chrome – Webpage Screenshot. Предположительно, вредонос мог отправить данные о браузерной активности более 1,2 млн пользователей на один IP-адрес в США, сообщается в пресс-релизе компании, размещенном на портале SourceWire.

Webpage Screenshot было загружено из online-магазина Google Chrome Extension более 1,2 млн раз. Расширение позволяет делать снимки экрана и хранить их.

Как пояснил один из основателей ScrapeSentry М. Зеттерлунд, его компания занимается выявлением и блокировкой скреперов и ботов, нарушающих условия и правила пользования веб-сайтов. В ходе одной из таких проверок специалисты зарегистрировали необычную конфигурацию входящего

трафика на одном из ресурсов, что побудило их тщательно исследовать ситуацию.

При ближайшем рассмотрении оказалось, что расширение Webpage Screenshot содержало вредоносный код, отправлявший копии всех данных о браузерной активности пользователей на сервер, расположенный в США. Таким образом, вся важная информация, видимая в заглавии страницы, например, адрес электронной почты при работе с почтовым клиентом, могла быть отправлена на американский IP-адрес без ведома пользователя.

По словам аналитика ScrapeSentry К. Мариолини, последствия загрузки вредоносного расширения могут быть довольно значительными. Хотя пока не известно, кто и с какой целью собирал информацию, специалисты считают, что ни к чему хорошему это не приведет. В любое время, подчеркивает К. Мариолини, в приложение может быть добавлен новый вредоносный функционал.

Результаты анализа исследователи ScrapeSentry передали специалистам Google. Расширение Webpage Screenshot уже изъято из магазина Chrome Extension, а его разработчик пока никак не прокомментировал ситуацию ***(Вредонос в расширении Chrome отправил данные более 1 млн пользователей на один IP-адрес // InternetUA (http://internetua.com/vredonos-v-rasshirenii-Chrome-otpravil-dannie-bolee-1-mln-polzovatelei-na-odin-IP-adres). – 2015. – 8.04).***

***

Специалисты компании «Доктор Веб» исследовали образец новой вредоносной программы, способной выполнять поступающие от злоумышленников команды и похищать различную информацию на инфицированных устройствах.

Троянец-бэкдор, получивший наименование BackDoor.Hser.1, распространялся с помощью целевой почтовой рассылки на личные и служебные электронные адреса сотрудников более 10 предприятий, входящих в состав известного российского концерна, причем все эти предприятия имеют оборонный профиль или обслуживают интересы военно-промышленного комплекса. Письмо было отправлено якобы от имени сотрудника головной организации холдинга и имело заголовок «Дополнение к срочному поручению от 30.03.15 № УТ-103». В тексте сообщения получателю предлагалось ознакомиться с номенклатурой некоего оборудования, а во вложении злоумышленники разместили файл табличного редактора Microsoft Excel с именем Копия оборудование 2015.xls.

Вложенный в сообщение файл содержит эксплойт, использующий уязвимость CVE2012-0158 в некоторых версиях табличного редактора Microsoft Excel. При попытке открытия данного файла на атакуемом компьютере запускается процесс excel.exe, в который встраивается дроппер троянца.

Дроппер распаковывает из своего тела бэкдор BackDoor.Hser.1 и сохраняет его на диск под именем npkim.dll в папку C:\Windows\Tasks\,

регистрирует данную библиотеку в параметрах автозагрузки Windows и запускает командный интерпретатор cmd.exe для удаления файла процесса, в который он был встроен.

После своего запуска на инфицированном компьютере BackDoor.Hser.1 расшифровывает хранящийся в его теле адрес управляющего сервера и устанавливает с ним соединение. Троянец отправляет в принадлежащий злоумышленникам командный центр информацию об атакованном ПК (IP-адрес компьютера, его имя, версию операционной системы, наличие в сети прокси-сервера), после чего ожидает поступления команд от злоумышленников. Среди прочего, вредоносная программа способна по команде передавать на удаленный сервер список активных процессов на зараженном ПК, загрузить и запустить другое вредоносное приложение, а также открыть командную консоль и выполнить перенаправление ввода-вывода на принадлежащий киберпреступникам сервер, благодаря чему злоумышленники получают возможность дистанционного управления инфицированным компьютером.

Сигнатура троянца BackDoor.Hser.1 добавлена в вирусную базу Dr.Web, и потому эта вредоносная программа более не представляет опасности для пользователей антивирусных продуктов компании «Доктор Веб». Тем не менее, мы снова напоминаем читателям о необходимости установки современного антивирусного ПО и поддержания вирусных баз в актуальном состоянии ***(Предотвращена атака опасного троянца на оборонные предприятия // ITnews (http://itnews.com.ua/news/76635-predotvrashhena-ataka-opasnogo-troyantsa-na-oboronnye-predpriyatiya). – 2015. – 8.04).***

***

Еще один информационный сайт Севастополя подвергся хакерской атаке. Как сообщили krymr.com в редакции независимой онлайн-газеты «Меридиан Севастополь», на их сайт с 3 по 6 апреля была проведена мощная DDoS-атака. В результате большого количества запросов от ложных посетителей сервер был перегружен и посетители не могли зайти на сайт.

«Поводом стали опубликованные материалы расследований о злоупотреблениях севастопольских чиновников», – отметили в редакции.

По оценке администрации сайта, для хакерской атаки, в частности, послужили статьи: Севастополь ставит на мошенников, Когда Севастополь объявит дефолт? Социальное жилье от официального жулья. Именно после их публикации и началась атака, отметили в редакции.

После атаки сайту пришлось «переехать» на другой сервер и включить облачную защиту от DDoS.

«Сайту “Меридиан Севастополь” в декабре нынешнего года исполнится 10 лет. За это время нами были опубликованы сотни различных расследований о злоупотреблениях севастопольских властей. Но только в прошлом году на наш сайт начали организовывать заказные хакерские атаки», – сообщают в онлайн газете.

Как сообщали Крым.Реалии, в течение последних нескольких дней неизвестные организовали массированные DDOS-атаки на сайт «Новости Севастополя», вследствие чего сайт стал недоступен для интернет-пользователей ***(Из-за статьи о злоупотреблениях чиновников сайт Севастополя был атакован хакерами // МедіаБізнес (http://www.mediabusiness.com.ua/content/view/43034/118/lang,ru/). – 2015. – 8.04).***

***

Американець подав до суду на соціальну мережу Facebook за функцію розпізнавання облич. Про це повідомляє Mashable.

Мешканець штату Іллінойс К. Ліката заявляє, що через спосіб, у який здійснюється додаванна тегів, соцмережа Facebook порушила законодавство про збір персональних даних. Позивач вважає, що ресурс збирає найбільшу у світі приватну базу біометричних даних користувачів.

За словами К. Лікати, він не давав соцмережі дозволу збирати чи зберігати свої біометричні дані. Позивач також зауважив, що його не попереджали про це і не надали можливості запобігти цьому.

У своїй заяві речник Facebook заявив, що позов К. Лікати безпідставний і компанія має намір рішучо себе захищати.

Функція «поради» при тегуванні людини (коли соцмережа підказує, хто зображений на фото) була запроваджена 2010 р. Компанія пояснювала своє рішення намаганням зробити процес позначення людей на знімках простішим.

Попри те, що Facebook надає спосіб відмовитися від тегування особі самостійно, захист К. Лікати вважає, що цього недостатньо. «Якщо ви змінили налаштування приватності, це нічого не змінить, оскільки Facebook вже отримав ці дані», – каже адвокат Д. Еделсон.

Нині, як зазначає Mashable, соцмережа Facebook працює над новою технологією розпізнавання облич DeepFace ***(На Facebook подали до суду через функцію розпізнавання облич // MediaSapiens (http://osvita.mediasapiens.ua/web/social/na_facebook_podali_do_sudu_cherez_funktsiyu_rozpiznavannya_oblich/). – 2015. – 8.04).***

***

Хакеры «Шалтай-Болтай» опубликовали переговоры российских чиновников по Крыму

Активисты анонимной хакерской организации «Шалтай-Болтай» выложили в сеть расшифровку перехваченных ими записей телефонных разговоров руководящих лиц двух крупных банков РФ.

«Шалтай-Болтай» разместил расшифровку розговора, который ведут, предположительно, начальник службы безопасности Банка Москвы В. Никишаев и два члена совета директоров Российского национального коммерческого банка – А. Гостевой и Р. Арефьев.

Чиновники обсуждают кандидатуру А. Гостева на важный пост в Совете министров аннексированного Российской Федерацией Крыма. Предполагается, что он станет одним из первых лиц в оккупационном правительстве полуострова ***(Хакеры «Шалтай-Болтай» опубликовали переговоры российских чиновников по Крыму // InternetUA (http://internetua.com/hakeri--shaltai-boltai--opublikovali-peregovori-rossiiskih-csinovnikov-po-krimu). – 2015. – 10.04).***

***

В Австрии 25 тыс. пользователей подали коллективный иск к Facebook в связи с предположительными нарушениями соцсетью европейского законодательства в области конфиденциальности пользовательской информации. Рассмотрением дела займется суд в Вене. Об этом сообщает BBC News.

В частности, истцы выражают недовольство тем, как Facebook собирает и использует личные данные.

Иск, составленный инициативной группой под руководством юриста М. Шремса, специализирующегося на вопросах защиты личных данных, подан против головного офиса соцсети в Европе, который находится в Дублине. Эта штаб-квартира отвечает за регистрацию всех аккаунтов за пределами США и Канады.

Также истцы заявили, что соцсеть нарушает закон, когда следит за пользователями при использовании ими кнопки Facebook «Нравится» на сторонних сайтах. Они рассчитывают отсудить у Facebook компенсацию в размере 540 дол. на человека. Таким образом, если суд удовлетворит требования в полном объеме, общая сумма компенсаций, которую соцсети придется выплатить, может достигнуть 13,5 млн дол.

М. Шремс заявил, что данным шагом хочет остановить «массовую слежку», осуществляемую крупнейшей соцсетью в мире. Активист предполагает, что компания также сотрудничает с PRISM – системой слежения США, запущенной в 2007 г. Агентством национальной безопасности (АНБ) ***(25 тысяч пользователей подали в суд на Facebook // InternetUA (http://internetua.com/25-tisyacs-polzovatelei-podali-v-sud-na-Facebook). – 2015. – 9.04).***

***

Специалисты компании «Доктор Веб» исследовали новую вредоносную программу, способную выполнять поступающие от злоумышленников команды и передавать на удаленный сервер сделанные на инфицированном компьютере снимки экрана.

Бэкдор обладает механизмами проверки наличия на атакуемом компьютере виртуальной среды и антивирусных программ.

Троянец, получивший наименование VBS.BackDoor.DuCk.1, написан на языке Visual Basic и распространяется в виде файла ярлыка с расширением .lnk,

в содержимое которого записан запакованный VBS-сценарий. При открытии ярлыка VBS-скрипт извлекается и сохраняется в виде отдельного файла, после чего происходит его запуск.

Троянец VBS.BackDoor.DuCk.1 использует весьма примечательный способ определения адреса управляющего сервера. В начале VBS-сценария предусмотрено три ссылки: две – на страницы видеохостинга YouTube, а еще одна – на страницу облачного сервиса Dropbox.

Троянец отправляет на данные ресурсы GET-запрос и в поступившем ответе выполняет поиск с заданным вирусописателями регулярным выражением: our (.*)th psy anniversary. Полученное в результате поиска значение делится на 31 337 – итог этой математической операции представляет собой число, которое после перевода в шестнадцатеричную форму соответствует значению IP-адреса управляющего сервера. Для проверки его работоспособности троянец отправляет по указанному адресу специальный GET-запрос и проверяет в ответе наличие строки «ОКОКОК».

VBS.BackDoor.DuCk.1 обладает специальным механизмом проверки наличия на атакуемом компьютере виртуальной среды, а также работающих процессов различных приложений для мониторинга операционной системы. Также в самом бэкдоре реализовано выявление на инфицированном компьютере нескольких антивирусных программ (в случае обнаружения таковых троянец не выполняет один из своих сценариев).

В директории текущего пользователя Windows VBS.BackDoor.DuCk.1 создает вложенную папку, которую использует в качестве рабочей. В целях маскировки троянец сохраняет в папке для размещения временных файлов документ vtoroy_doc.doc и демонстрирует его пользователю:

При этом можно предположить, что изначально злоумышленники планировали использовать в качестве «приманки» презентацию PowerPoint, поскольку в коде троянца реализован алгоритм завершения процесса данного приложения (если установлен соответствующий флаг), однако по каким-то причинам передумали.

Для создания снимков экрана бэкдор использует собственную библиотеку, при этом сами скриншоты сохраняются во временную папку в виде файлов с расширением .tmp. С помощью специального REG-файла троянец отключает расширения браузера Microsoft Internet Explorer, а если вредоносная программа запущена в операционной системе Windows Vista, то с помощью другого REG-файла VBS.BackDoor.DuCk.1 отключает в данном браузере режим protected. Помимо этого, VBS.BackDoor.DuCk.1 реализует собственный автоматический запуск путем размещения в папке автозагрузки соответствующего ярлыка:

Для получения команд от управляющего сервера троянец с интервалом в одну минуту направляет на него соответствующий запрос. Среди специальных команд VBS.BackDoor.DuCk.1 может выполнить скачивание на инфицированный компьютер другого вредоносного приложения, либо с помощью запроса загрузить снимки экрана на удаленный сервер. Все

остальные команды VBS.BackDoor.DuCk.1 передает командному интерпретатору CMD или PowerShell. Также данный бэкдор способен выполнить на зараженной машине Python-сценарий, результаты работы которого в зашифрованном виде передаются на принадлежащий злоумышленникам сервер.

Сигнатура VBS.BackDoor.DuCk.1 добавлена в вирусную базу Dr.Web, и потому эта вредоносная программа более не представляет опасности для пользователей антивирусных продуктов компании «Доктор Веб» ***(Новый бэкдор угрожает пользователям Windows // ITnews (http://itnews.com.ua/news/76650-novyj-bekdor-ugrozhaet-polzovatelyam-windows). – 2015. – 10.04).***

***

9 апреля исследователи безопасности под псевдонимами MLT и PsychoMantis сообщили об XSS-уязвимостях в нескольких доменах филиалов интернет-ритейлера Amazon – amazon.ca (Канада), amazon.com.mx (Мексика), amazon.com.br (Бразилия) и amazon.de (Германия). На момент написания новости бреши все еще не были исправлены.

В текущем году исследователи безопасности обнаружили в общей сложности 18 XSS-уязвимостей на вышеуказанных веб-сайтах: amazon.ca и amazon.de – 10 (по пять на каждом), amazon.com.mx и amazon.com.br – 8 (по четыре на одном и на другом). В настоящее время ни одна из них не исправлена, что подвергает системы пользователей, посетителей и администраторов риску компрометации злоумышленниками.

Похищение cookies-фалов, персональной информации, учетных данных и истории браузера является наименее опасным последствием XSS-атак. Подобные атаки становятся все более сложными и зачастую используются вместе с точечным фишингом, техниками социальной инженерией и атаками drive-by ***(В нескольких доменах Amazon обнаружены XSS-уязвимости // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/04/10/XSS-flaws-at-amazon.html). – 2015. – 10.04).***

***

Компания ESET раскрыла кибершпионскую атаку «Операция Buhtrap», нацеленную в первую очередь на российские финансовые организации.

Об этом пишут Новости ИТ со ссылкой на 3D-News.

Сообщается, что злоумышленники действовали в течение как минимум одного года. Приоритетной целью атаки стали российские банки – на них пришлось почти 90 % всех зафиксированных случаев заражения.

Для проникновения в атакуемую систему киберпреступники рассылали фишинговые письма с прикреплённым документом в формате Microsoft Word. Такие сообщения, в частности, маскировались под счёт за оказание неких услуг и под контракт мобильного оператора «МегаФон».

При попытке открытия файла запускается эксплойт для одной из уязвимостей в Word (CVE-2012-0158), в результате чего на ПК устанавливается NSIS-загрузчик. Программа проверяет некоторые параметры Windows и затем скачивает с удалённого сервера архив 7z с вредоносными модулями. Любопытно, что многие такие компоненты подписаны действительными цифровыми сертификатами, выданными в том числе зарегистрированным в Москве юридическим лицам.

Чтобы установить контроль над заражённым ПК, в «Операции Buhtrap» используются программы с исполняемыми файлами mimi.exe и xtm.exe. Они позволяют получить или восстановить пароль от Windows, создать новый аккаунт в операционной системе, включить сервис RDP. Далее с помощью исполняемого файла impack.exe осуществляется установка бэкдора LiteManage.

На финальном этапе на инфицированный компьютер загружается банковское шпионское ПО с названием исполняемого файла pn_pack.exe. Программа специализируется на краже данных и взаимодействии с удалённым командным сервером. Шпион способен отслеживать и передавать злоумышленникам нажатия клавиш и содержимое буфера обмена, а также перечислять смарт-карты, присутствующие в системе.

Количество пострадавших в ходе «Операции Buhtrap» организаций и размер финансового ущерба не уточняются ***(Масштабная кибератака Buhtrap нацелена на российские банки // Новости ИТ (http://www.novostiit.net/masshtabnaya-kiberataka-buhtrap-natselena-na-rossiyskie-banki-00018893). – 2015. – 9.04).***

***

Специалисты по информационной безопасности компании High-Tech Bridge нашли новый тип хакерской атаки, которая получила название drive-by login».

В рамках рутинной проверки одного из своих клиентов, инженеры High-Tech Bridge обнаружили на его сервере файл ozcommerz_pwner.php.bak, который оказался программой-бэкдором.

Система внедряет вредоносный код в скрипт /includes/application_bottom.php, чтобы загружать зловред с удалённого сервера, в зависимости от IP-адреса пользователя или его адреса электронной почты, для зарегистрированных пользователей. Как выяснилось, скачивание зловреда осуществлялось после авторизации в онлайн-магазине. Подобный вредоносный код в настоящее время не определяется ни одним антивирусом в мире.

Эксперты убеждены, что атаки типа drive-by login в ближайшем будущем получат широкое распространение, поскольку являются чрезвычайно эффективными и трудными для обнаружения ***(Новый тип хакерской атаки drive-by login заражает ПК после онлайн-авторизации // Блог Imena.UA (http://www.imena.ua/blog/drive-by-login/). – 2015. – 9.04).***

***

Не только широкополосные маршрутизаторы для домашнего использования имеют ненадежную защиту. Согласно результатам исследования компании Veracode, интернет-вещи, которые автоматически синхронизируются с облачным хранилищем, также не обеспечивают защиту данных на высоком уровне.

Не изменяя стандартных настроек сетевого оборудования и не пытаясь обойти защиту ни устройств, ни облачных сервисов, эксперты Veracode обнаружили множество уязвимостей в решениях от компаний Chamberlain Group, SmartThings, Ubi и Wink, просто захватив сетевой трафик.

Специалисты протестировали контроллеры для домашней автоматизации WinkHub и Wink Relay, систему активации голосом Unified Computer Intelligence, решение для автоматизации и контроля от компании SmartThings, интернет-интерфейс системы для управления гаражными воротами MyQ Garage и ПО для управления выключателями и розетками электропитания MyQ Internet Gateway от компании Chamberlain Groups.

Эксперты проверили тестируемое ПО на соответствие ряду требований, которые разбили на категории:

– поддерживает ли устройство шифрование при подключении к облачному сервису; проверяется ли сложность пароля и подлинность TLS-сертификата. Только решение от SmartThings соответствует всем стандартам;

– взаимодействие с облачными сервисами – защита процесса аутентификации устройства; шифрования при взаимодействии с облачным хранилищем; защита от атак «человек посередине»; защита конфиденциальных данных. Снова только продукт компании SmartThings успешно прошел все тесты;

– мобильный интерфейс – защита связи между устройством и смартфоном. Устройство от SmartThings опять стало лучшим в тесте;

– отладка безопасности – открыт ли интерфейс отладки, защищен ли он, может ли злоумышленник выполнить произвольный код на устройстве. Здесь продукт SmartThings провалился – к устройству можно получить доступ через протокол Telnet. MyQ Gateway успешно прошла все тесты категории ***(Специалисты обнаружили множество брешей в защите интернет вещей // InternetUA (http://internetua.com/specialisti-obnarujili-mnojestvo-breshei-v-zasxite-internet-vesxei). – 2015. – 11.04).***

***

В iOS 8 обнаружена уязвимость, способная вывести из строя смартфоны iPhone. Об этом сообщают исследователи безопасности из компании FireEye.

Как указывается в блоге FireEye, уязвимость Phantom с идентификатором CVE-2015-1118 позволяет хакерам вызвать непрекращающееся аварийное завершение работы всех установленных приложений и самой ОС. Для этого злоумышленник должен вынудить жертву изменить настройки прокси-сервера в их iOS-устройствах.

«Хакер может распространить вредоносный профиль конфигурации, содержащий специальные настройки прокси-сервера, среди пользователей определенной точки Wi-Fi. Задействовав приемы социальной инженерии, злоумышленник может уговорить или вынудить жертву установить вредоносный профиль. После этого возникает несколько ошибок использования после высвобождения, что приводит к моментальному аварийному завершению работы большинства приложений и системных компонентов и нестабильной работе ОС», – сообщается в блоге FireEye ***(Уязвимость в iOS выводит из строя iPhone // InternetUA (http://internetua.com/uyazvimost-v-iOS-vivodit-iz-stroya-iPhone). – 2015. – 11.04).***

***

Facebook признала, что с помощью социальных плагинов, таких как кнопка Like («Нравится»), компания собирала статистику посещений сторонних веб-сайтов у тех пользователей, которые не были зарегистрированы в Facebook.

В компании сообщили, что сбор данных у таких пользователей происходил из-за ошибки в работе плагинов. В настоящее время специалисты Facebook занимаются ее устранением, сообщили представители компании в официальном блоге.

Запись в блоге Facebook в целом посвящена опровержению тезисов, сделанных исследователями Бельгийской комиссии по защите частных данных (Belgian Privacy Commission). В конце марта 2015 г. они пришли к выводу, что Facebook нарушает европейские законы о защите информации.

Исследователи выяснили, что Facebook не только отслеживает историю просмотра страниц в Facebook, которые посещает зарегистрированный в соцсети пользователь, но и историю тех интернет-пользователей, которые даже не посещали сайт Facebook.

Как выяснили специалисты, соцсеть делает это с помощью социальных плагинов, установленных на миллионах сайтов. При посещении сайта с таким плагином на диск компьютера помещаются «куки» (cookies) – специальные файлы, хранящие историю веб-серфинга. Когда пользователь повторно посещает сайт Facebook с таким плагином, Facebook через этот плагин считывает куки, записанные в память компьютера.

И хотя веб-история хранится в куках в обезличенном виде, у исследователей такое поведение соцсети вызвало негодование. Они указывают на то, что Facebook собирает данные втайне, а у пользователя нет возможности отключить этот процесс.

У Бельгийской комиссии по защите частных данных нет полномочий оштрафовать Facebook. Однако выводы исследователей сгущают тучи над социальной сетью, заставляя европейских властей задавать больше вопросов относительно того, ведет ли крупнейшая в мире социальная сеть бизнес честно.

Как отмечает Wall Street Journal, в случае если Facebook будет официально признана виновной в неправомерном использовании

пользовательских данных для отображения релевантной рекламы, ей грозит штраф в размере до 5 % от годовой выручки. В 2014 г. выручка Facebook составила 12,5 млрд дол. (таким образом, штраф может достичь 600,25 млн дол.).

Facebook далеко не в первый раз становится объектом критики вследствие небрежного отношения к персональным данным ***(Facebook заявила, что шпионила за пользователями по всему интернету из-за программной ошибки // InternetUA (http://internetua.com/Facebook-zayavila--csto-shpionila-za-polzovatelyami-po-vsemu-internetu-iz-za-programmnoi-oshibki). – 2015. – 13.04).***

***

Apple устранила опасную уязвимость в OS X, но только для пользователей Yosemite

В обновлении OS X Yosemite 10.10.3 исправлена опасная брешь безопасности, позволяющая злоумышленнику повысить свои привилегии. Данная уязвимость присутствует во всех операционных системах Apple, начиная с версии OS X 10.7.

Уязвимость обнаружил в октябре прошлого года специалист шведской фирмы Truesec Э. Кварнхаммар. «Дыра» безопасности открывает возможность повышения привилегий в нескольких версиях операционной системы. В Apple исправили баг только в обновлении OS X 10.10.3, которое вышло на этой неделе.

Из-за этой ошибки пользователь может обойти ограничения пользовательской оболочки и получить права суперпользователя, для чего в нормальных условиях ему бы понадобился пароль. В сети уже было опубликовано несколько демонстраций наличия уязвимостей в разных версиях OS X. Сам Э. Кварнхаммар представил видео, в котором он подтверждает наличие бреши, не вдаваясь в технические подробности.

Как выяснили в Engadget, компания Apple не планирует выпускать патч для пользователей Mavericks и Mountain Lion из-за технических сложностей. В компании рекомендуют пользователям переходить на последнюю версию операционной системы – OS X Yosemite.

Пользователям предыдущих версий операционных систем OS X эксперты рекомендуют использовать для рядовых задач учетные записи без прав администратора, а также шифровать данные на жестком диске при помощи технологии FileVault ***(Apple устранила опасную уязвимость в OS X, но только для пользователей Yosemite // InternetUA (http://internetua.com/Apple-ustranila-opasnuua-uyazvimost-v-OS-X--no-tolko-dlya-polzovatelei-Yosemite). – 2015. – 12.04).***