СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16–28.03)

2015 № 6

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16–28.03)
№ 6

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

Головний 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

Украинский офис международной исследовательской компании TNS огласил список самых популярных сайтов среди украинских интернет-пользователей за февраль. В рейтинге лидирует социальная сеть «ВКонтакте» с охватом 65 % среди интернет-аудитории в возрасте 16–55 лет. С незначительным отрывом второе место занимает поисковик Google, охват которого составляет 64 %. Третье место у Youtube – 61 %. Помимо общего рейтинга, TNS также представил топ новостных ресурсов уанета по охвату – в нем лидирует tsn.ua, пишет AIN.UA (http://ain.ua/2015/03/17/570232).

Среди социальных сетей вторым по популярности идет Facebook, расположившийся на седьмом месте. Он опережает «Одноклассники», которые занимают девятое место по охвату украинской аудитории. В первую десятку также вошли Mail.Ru, «Яндекс», Wikipedia, OLX и «ПриватБанк».

Напомним, в аналогичном исследовании по версии Factum Group первая тройка сайтов уанета по охвату выглядит несколько иначе: Google здесь опережает «ВКонтакте», а вместо YouTube бронзу получил Mail.ru. Также срезы популярных сайтов делает компания Gemius, однако свежего отчета за февраль аналитики еще не предоставили ***(Топ-10 сайтов уанета по версии TNS: «ВКонтакте» лидирует, «ПриватБанк» замыкает десятку // AIN.UA (http://ain.ua/2015/03/17/570232). – 2015. – 17.03).***

***

По сведениям аналитиков из Global Web Index, на днях фотохостинг Instagram стал наиболее быстрорастущей социальной сетью – за последние несколько месяцев количество активной аудитории увеличилось примерно на 23 %.

Второе место в списке занимает социальный новостной ресурс Reddit, чей показатель роста равен 13 %, и сайты Pinterest и Quora, которые продемонстрировали незначительный рост на 6 % каждый. Довольно низкий результат показала социальная сеть Twitter, которая увеличила активную аудиторию всего на 2 %.

Довольно любопытно, что гиганты YouTube, Facebook, «ВКонтакте» и «Одноклассники» и вовсе продемонстрировали сокращение активной аудитории, а не прирост, как от них все ожидали. Согласно статистике, каждая из этих социальных сетей за последние полгода потеряла примерно 3 % аудитории.

Безусловно, это является тревожным звоночком для руководства сетей ***(Социальные сети стремительно теряют активную аудиторию // Ageofcomp.info (http://ageofcomp.info/soft/32144-socialnye-seti-stremitelno-teryayut-aktivnuyu-auditoriyu.html). – 2015. – 17.03).***

***

Фотохостинг Instagram запустил свое новое приложение Layout, позволяющее собирать несколько фото в одно изображение.

С помощью Layout можно создавать различные коллажи, а поиск фотографий для них возможен, например, благодаря функции «Лица» (Faces): приложение способно найти все изображения из галереи пользователя, на которых есть люди.

Для создания своего макета пользователь может изменять порядок фото, перетаскивая их, увеличивать, регулировать размер, растягивая границы изображения. Кроме того, можно создавать зеркальные эффекты, наклоняя и поворачивая фото, чтобы получить необычную композицию.

Другая опция «Фотобудка» (Photo Booth) позволяет делать несколько кадров, которые сразу же попадут в макет.

Layout пока доступен только для iOS-устройств, версия для Android, по словам компании, планируется выпустить в ближайшие месяцы.

У Instagram, принадлежащего крупнейшей соцсети Facebook, уже есть приложения помимо основного сервиса фотохостинга. К примеру, отдельное приложение Hyperlapse способно создавать таймлапс-видео (техника, которая позволяет снять видео в замедленном режиме, а затем воспроизвести его с нормальной скоростью). Другой сервис компании – Bolt – позволяет обмениваться моментальными изображениями и видео с близкими людьми ***(Instagram запустил приложение для создания креативных коллажей // InternetUA (http://internetua.com/Instagram-zapustil-prilojenie-dlya-sozdaniya-kreativnih-kollajei). – 2015. – 24.03).***

***

В Swarm появилась возможность отправки сообщений в один клик. Теперь пользователи могут не только чекиниться, но и отправлять сообщения одному другу или группе друзей, даже если их нет в Swarm. Для удобства координации при обмене сообщениями собеседники видят местоположение друг друга.

Напомним, социальная сеть Foursquare в 2014 г. разделилась на две самостоятельные платформы – собственно Foursquare, который стал платформой персонализированного поиска, и Swarm – сервис чекинов ***(В Swarm появились личные сообщения // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_swarm_poyavilis_lichnye_soobscheniya). – 2015. – 24.03).***

***

Twitter и Foursquare объявили о своем партнерстве. Теперь пользователи смогут указывать в твитах свое точное местоположение, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-i-foursquare-objavili-o-svoem-partnerstve-43723/).

Об этом было объявлено в официальном аккаунте Twitter.

Партнерство имеет смысл для обеих компаний. Для Foursquare – это шанс восстановить свое положение после передачи чекинов Swarm и напомнить пользователям, что у сервиса все еще есть очень большая база геолокационных данных. Для Twitter – это возможность улучшить взаимодействие между пользователями. Рекламодателям Twitter это нововведение позволит улучшить локальный таргетинг.

По словам представителя Twitter, новая возможность будет выкачена в течение ближайших нескольких недель в США и Канаде ***(Twitter и Foursquare объявили о своем партнерстве // Marketing Media Review (http://mmr.ua/news/id/twitter-i-foursquare-objavili-o-svoem-partnerstve-43723/). – 2015. – 24.03).***

***

Социальная сеть Facebook ведет переговоры с The New York Times, BuzzFeed и National Geographic и рядом других СМИ о размещении их контента на страницах соцсети. Если переговоры завершатся успехом, то пользователи Facebook смогут читать статьи и новости СМИ, не покидая Facebook.

С такой инициативой, по неофициальным данным, полученным NYT, выступил вице-президент Facebook по вопросам развития продукта К. Кокс. В настоящее время новости публикуются в Facebook в виде анонса со ссылкой на сайт СМИ.

Для того чтобы прочесть новость целиком на мобильном устройстве, необходимо кликнуть на ссылку и дождаться загрузки соответствующей страницы в окне браузера, что, по данным социальной сети, требует в среднем 8 секунд, в то время как размещение текста новости целиком в Facebook позволит получить ее за доли секунды, достаточно перевести глаза на текст. Это позволит увеличить удовлетворение пользователя как от мобильного приложения социальной сети, так и от новостного контента издателей.

Чтобы предложение стало интересным для крупнейших СМИ, Facebook предлагает разделять с ними доходы от рекламы в новостях. До недавнего времени социальная сеть не практиковала такой подход и размещала у себя контент в обмен на трафик, который правообладатель получал из Facebook. Однако с конца 2014 г. компания М. Цукерберга все чаще практикует такой подход. По словам одного из анонимных источников в компании, рассматривается даже вариант, когда издатель может размещать в новость одну собственную рекламу, что для мобильного формата вполне достаточно.

Выгоды от такого партнерства для Facebook очевидны. Социальной сети необходимо как можно дольше удерживать свою 1,4-миллиардную аудиторию в рамках своего сайта и мобильного приложения для обеспечения роста своих коммерческих показателей.

Кроме того, сделка с крупнейшими СМИ позволит Facebook сделать еще один важный шаг на пути замещения Google как «точки входа в Интернет».

Для самих СМИ все не так просто. С одной стороны, трафик из социальных сетей стал одним из определяющих показателей успешности

медиа-ресурсов и те из них, кто откажется или будет не способен распространять контент за пределами своего сайта, в будущем могут потерять аудиторию и узнаваемость своего бренда. Этого мнения придерживается BuzzFeed, который уже публикует свои новости далеко не только на своем портале. Кроме того, использование механизмов социальной сети позволит распространять новости более адресно (например, такой аудитории, как «молодая жительница Нью-Йорка, любящая путешествовать»), что повысит вовлеченность читателей.

С другой стороны, публикуя свой контент за пределами своих сайтов, медиа-ресурсы теряют контроль над рекламой, своим брендом и аудиторией.

Для крупных СМИ, которые продают платную подписку на свои премиальные новости и материалы, трафик на собственном сайте – это необходимое условие монетизации, и не факт, что разделение доходов от рекламы в Facebook покроет потери. Кроме того, вместе с контентом новостные порталы теряют и данные об интересах и поведении читательской аудитории, которые достаются Facebook, и о разделении доходов от их продажи речь уже не идет.

Генеральный директор PubMobile И. Колотухин согласен с мнением представителей медиа-ресурсов: «Размещая контент на сторонней платформе, такой как Facebook, СМИ могут утратить интерес пользователей к основному каналу распространения новостей, таким как сайт издательства или мобильное приложение. Facebook не первый, кто хочет агрегатировать новостной контент, и многие это уже делают в том или ином виде. Но в рамках Facebook такая методика жизнеспособна и подойдет для сотрудничества с некоторыми СМИ. Однако если вместе с контентом предлагается подача рекламы, то только издание должно осуществлять контроль рекламных материалов, чтобы в том числе избежать курьезов и, например, в новости о рождении второго ребенка у К. Миддлтон случайно не появилась реклама презервативов».

СМИ, публикующие премиальный контент, например The Guardian, отнеслись к предложению Facebook весьма прохладно. Они предлагают коллегам из других издательств объединиться для коллективного обсуждения принципов работы отрасли и контроля над контентом и рекламой.

Однако если соглашение с Facebook все же будет заключено, это станет прорывом во взаимоотношениях интернет-медиа с крупными социальными сетями и поисковиками, которые агрегируют их контент и зарабатывают на нем. Пока эти взаимоотношения складываются непросто.

Несколько дней назад CNN International, Financial Times, The Guardian, Reuters и The Economist объединились с Programmatic-платформой Pangaea Alliance с целью отобрать рекламную аудиторию у Google и Facebook.

Programmatic-платформа – это технология, позволяющая рекламодателям покупать рекламное место на интернет-площадках.

В конце 2014 г. компания Google просто закрыла свой знаменитый агрегатор новостей Google News в Испании из-за принятия там закона, который требует от компании платить за размещение материалов испанских СМИ.

«Поскольку Google News не приносит нам денег, этот новый подход просто-напросто нежизнеспособен» – так прокомментировал это решение в своем блоге глава Google News Р. Джинграс ***(Facebook готовит сенсацию // InternetUA (http://internetua.com/Facebook-gotovit-sensaciua). – 2015. – 25.03).***

***

Российская аналитическая компания «Кибриум» установила, что ежедневно в сети появляется до 30 млн записей, однако, большинство из них – это повторные публикации чужих материалов, пишет Блог Imena.UA (http://www.imena.ua/blog/unique-texts-are-rare/).

Для анализа посещаемости и цитируемости эксперты отслеживали положение дел в самых популярных социальных сетях в РФ. Выяснилось, что в Twitter число постоянных пользователей достигает от 1,5 до 2 млн человек, каждый из которых оставляет от 8 до 12 сообщений ежедневно.

Во «ВКонтакте» данный показатель равен 12 млн записей, в LiveJornal – 14 млн блогов ведутся ежедневно, а в Instagram размещается до 2 млн фотографий за сутки. Наконец, в социальной сети Facebook ежедневно появляется от 4 до 5 млн заметок в день.

Но из миллионов опубликованных постов всего 5 % пользователей во всех социальных сетях создают хоть что-то уникальное – подавляющее большинство просто делает очередную перепубликацию чужих материалов.

Ранее аналитики компании Ericsson ConsumerLab установили, что подавляющее большинство мирового трафика создают всего пять приложений и сайтов. Первое место по генерации всемирного трафика в Интернете занимает социальная сеть Facebook. Второе место – сервис Instagram, третье – видеохостинг YouTube ***(Только 5 % пользователей социальных сетей создают уникальные материалы // Блог Imena.UA (http://www.imena.ua/blog/unique-texts-are-rare/). – 2015. – 25.03).***

***

Социальная сеть Facebook обнародовала новую функцию, которая позволит пользователям заглянуть в прошлое. Об этом говорится в пресс-релизе компании. Об этом пишут Новости ИТ со ссылкой на 3D-News.

On This Day – новая функция, призванная сыграть на ностальгии посетителей социальной сети. Она будет размещать информацию из прошлого в Хронике пользователя. Это могут быть статусы, теги, фото, посты, размещённые владельцем аккаунта в этот день в разные годы.

Разработчики On This Day явно вдохновлялись успехом Timehop – стороннего приложения с похожей функциональностью, быстро завоевавшего популярность среди пользователей крупнейших социальных сетей.

В компании заявляют, что не собираются монетизировать новый сервис и неохотно сравнивают его с приложениями от сторонних разработчиков. В рамках One This Day, Facebook разработала специальный алгоритм, призванный защитить пользователей от неприятных воспоминаний. Например, он будет

ограничивать информацию, в которой упоминаются бывшие романтические партнёры или умершие друзья.

По заверениям компании, пользователи всего мира смогут воспользоваться новой функцией в течение нескольких недель. В России On This Day пока что недоступна ***(Facebook предложит взгляд в прошлое // Новости ИТ (http://www.novostiit.net/facebook-predlozhit-vzglyad-v-proshloe-00017940). – 2015. – 25.03).***

***

Соціальна мережа Facebook працює над сервісом голосових дзвінків, що автоматично відсіюватиме спам. Про це повідомляє Mashable з посиланням на Android Police.

Про плани соцмережі створити такий додаток свідчить скріншот, надісланий виданню двома людьми. Facebook, очевидно помилково, повідомив їх про нову функцію.

Додаток має назву Phone. Він показуватиме інформацію про особу, яка телефонує користувачу, імовірно, базуючись на Facebook-профілях, та автоматично блокуватиме дзвінки, раніше ідентифіковані як спам.

У коментарі виданню Mashable речник Facebook заявив: «Ми постійно тестуємо щось». Ситуацію довкола додатка Phone коментувати відмовився.

Facebook експериментує з голосовими дзвінками не вперше. Компанія представила функцію голосових дзвінків за допомогою Messenger кілька років тому. Вона також тестує таку можливість на Android-версії WhatsApp ***(Facebook тестує додаток для телефонних дзвінків – ЗМІ // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/social/facebook_testue_dodatok_dlya_telefonnikh_dzvinkiv_zmi/). – 2015. – 24.03).***

***

Pinterest раскрыл больше деталей алгоритма машинного обучения, который обеспечивает показ релевантных пинов в лентах пользователей.

Pinterest позаимствовал алгоритм новостной ленты у Facebook, но сейчас лента визуального сервиса – не хронологическая: она организована в порядке релевантности пинов, а не даты их публикации. Это изменение было внедрено в августе 2014 г. путём запуска «умной» ленты (smart feed).

Pinterest называет новый алгоритм Pinnability. Pinnability – следующий этап усовершенствования алгоритма сервиса, призванного уменьшить количество «информационного шума», получаемого пользователями социальной сети.

В блоге компании поясняется, как инженеры компании используют модели машинного обучения для определения, с какими пинами пользователи вероятнее всего будут взаимодействовать.

Разработчики внедрили коэффициент релевантности, присваиваемый каждому отдельному пину, который будет включен в ленту пользователя. В эту

выборку входят все пины от людей, на которых пользователь подписан, а также пины, рекомендованные сервисом (Picked for You), и, возможно, продвигаемые пины, хотя они не упоминались в посте компании.

Модели машинного обучения выводят рейтинг Pinnability путём определения таких факторов, как внутреннее качество пина (популярность, актуальность и вероятность спама); пол и активность пиннера и то, как он ранее взаимодействовал с пинами этого типа.

Затем, на основании этих данных, Pinterest показывает наиболее релевантные твиты в топе ленты пользователей.

По словам представителей компании, внедрение этих изменений значительно увеличило показатель вовлечённости во взаимодействие с пинами в лентах пользователей:

«Мы продолжаем улучшать Pinnability и внедрили несколько усовершенствований алгоритма. После каждого шага мы наблюдали значительное увеличение вовлечённости пиннеров, включая увеличение числа репостов в домашней ленте на более чем 20 %. Мы также наблюдали значительное повышение других метрик, включая общее количество репинов и кликов».

Более подробная информация об алгоритме Pinnability доступна в инженерном блоге Pinterest.

Напомним, что в январе этого года Pinterest приобрёл стартап Kosei, который владеет алгоритмом машинного обучения, способным устанавливать взаимосвязь между различными сущностями. Покупка призвана улучшить рекомендации, поиск по сервису, кроме того, технологии будут использованы для повышения точности рекламных сообщений ***(Pinterest поделился информацией об алгоритме показа релевантных пинов пользователям // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_podelilsya_informatsiey_ob_algoritme_pokaza_relevantnyh_pinov_polzovatelyam). – 2015. – 24.03).***

***

Бывший главный редактор «Большого города» и один из основателей проекта Arzamas Ф. Дзядко объявил о скором запуске тестовой версии социальной сети Relikva.com, пишут «Экономические известия» (http://news.eizvestia.com/news-culture/full/825-v-internete-poyavitsya-novaya-socialnaya-set-muzej-samogo-sebya).

Создатели начинают набор людей, которые вместе с ними будут создавать «музей самого себя». Конкретная дата начала работы соцсети пока неизвестна. В настоящее время в описании проекта говорится, что это будет сайт о частной памяти. Что это значит, и для чего понадобилось создавать новую социальную сеть, мы узнали у самого Ф. Дзядко.

Для кого и чего создана Relikva?

Мы столкнулись с тем, что у каждого человека есть некоторое количество, иногда небольшое, иногда огромное, предметов, фотографий и документов, которые почему-то ему дороги. Они, как правило, пылятся где-то в ящиках стола или в коробках на антресолях. Раз в год их открывают на каких-то семейных торжествах или если хотят объяснить друзьям какие-то случаи. Они потихонечку теряются, портятся; забывается, кто изображен на фотографиях. Мы поняли, что необходимо пространство, где бы это все аккуратно складывалось и продолжало жить.

Как будет выглядеть сайт?

Поначалу в постах можно будет разместить фотографию и историю – все очень просто. Вы публикуете фотографию старого снимка, медали деда, какой-нибудь книги и рассказываете, что это фотография для вас значит, ее историю.

На какие средства будет жить проект?

В настоящее время этот сайт сделан буквально за тысячу рублей. Собралась компания друзей и почти год придумывала, как это должно выглядеть. Если окажется, что людям эта штука нужна, появятся и те, кто этим заинтересуется с точки зрения бизнеса. Сейчас эта вещь полная гипотез, которую мы будем с помощью наших пользователей проверять и совершенствовать. Что касается спонсорства, мы открыты к предложениям.

Почему не Facebook?

Для того чтобы эта вещь хорошо функционировала, должна быть отдельная площадка, где живут именно реликвии. В Facebook и других соцсетях есть множество всего интересного. Но здесь нужен несколько специальный функционал. А главное, здесь должен жить именно ваш «музей», а не новости ***(В Интернете появится новая социальная сеть – «музей самого себя» // Экономические известия (http://news.eizvestia.com/news-culture/full/825-v-internete-poyavitsya-novaya-socialnaya-set-muzej-samogo-sebya). – 2015. – 24.03).***

***

Компания Twitter выпустила сервис видеотрансляций Periscope, купленный в январе за 100 млн дол. Об этом сообщается на официальном сайте проекта, пишет gazeta.ru.

Periscope позволяет вести прямые видеотрансляции с мобильного устройства. Записи трансляций будут доступны в течение 24 часов с момента прекращения съемки, после чего автоматически удалятся. Притом что Periscope принадлежит Twitter, сервис пока не имеет синхронизации подписок с социальной сетью, как и другой видеосервис компании, Vine.

В настоящее время приложение Periscope доступно только для iOS. Версия для Android появится позднее. О поддержке Windows Phone разработчики пока не сообщают ***(Twitter выпустил сервис видеотрансляций Periscope // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42894/118/lang,ru/). – 2015. – 27.03).***

***

Twitter продолжает прилагать усилия по привлечению новых пользователей. На этот раз платформа экспериментирует с обновленной домашней страницей. Цель эксперимента – привлечь 500 млн пользователей, которые ежемесячно посещают Twitter, но не логинятся там.

В отличие от действующей домашней страницы с одним фоновым изображением и формой входа, экспериментальная страница отображает разные категории и темы, обсуждаемые в сети. По мнению команды Twitter, это вызовет у пользователей ощущение, что они пропускают что-то важное интересное, и заставит их вступить в число 288 млн активных пользователей.

Представитель Twitter подтвердил, что в настоящее время эксперимент продолжается, и обновленная домашняя страница доступна ограниченному количеству пользователей. Интересно, что незалогиненный пользователь может сколько угодно исследовать тематические области, но как только он войдет в сервис, история его «путешествий» будет потеряна.

В марте Twitter уже был замечен в эксперименте – платформа тестировала возможность просмотра аналитики отдельных твитов прямо в ленте ***(Twitter тестирует новую домашнюю страницу // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_testiruet_novuyu_domashnyuyu_stranitsu). – 2015. – 25.03).***

***

Facebook объявила о серии обновлений во время ежегодной конференции для разработчиков F8, которая прошла в Сан-Франциско 25 марта, сообщает Marketing Media Review со ссылкой на портал mashable.com (http://mmr.ua/news/id/facebook-anonsiroval-osnovnye-izmenenija-na-konferencii-f8-43749/).

Facebook Messenger становится хабом

Прежде всего, основные обновления коснутся приложения для обмена сообщениями Facebook Messenger. Мессенджер превращается в коммуникационный хаб, и пользователи смогут пересылать фото, гифки, музыку. Разработчики теперь могут добавлять кнопку мессенджера в сторонние приложения.

Facebook Messenger Business

Facebook представила на конференции растущую платформу Messenger Business, которая позволит клиентам онлайн-магазинов напрямую коммуницировать с компаниями, отправляя им сообщение или сделать заказ и проверить информацию о доставке.

Пользователи смогут лично общаться с компаниями, в частности с представителями по работе с клиентами, и задавать вопросы, быстро получать ответы.

Трехмерное видео

Вскоре социальная сеть будет поддерживать 360-градусные видео, которые будут отображаться в ленте пользователя. Видео можно будет посмотреть с помощью очков Facebook – Oculus Rift или Samsung Gear VR.

Кроме того, компания создала новый плагин, который позволит встраивать видео с Facebook на другие сайты.

Аналитика для приложений

Компания представила новую платформу Analytics для приложений, которая предоставляет данные для разработчиков и маркетологов, чтобы они лучше могли понять свою аудиторию. Рекламодатели смогут получать статистику объявлений, в рамках которой можно будет проанализировать среднюю продолжительность сессии, средний размер платежей внутри программы и количество активных пользователей.

Интернет вещей

Facebook представила новый набор инструментов для разработчиков, чтобы поддержать растущий наплыв смарт-девайсов для дома. Компания анонсировала платформу Parse для разработки мобильных приложений. С ее помощью можно будет интегрировать мобильные приложения с устройствами, подключенными к сети Интернет ***(Facebook анонсировал основные изменения на конференции F8 // Marketing Media Review (http://mmr.ua/news/id/facebook-anonsiroval-osnovnye-izmenenija-na-konferencii-f8-43749/). – 2015. – 26.03).***

***

LinkedIn выпустил приложение по поиску работы Job Search для пользователей Android-устройств.

Функционал новинки повторяет возможности аналогичного приложения для iOS. Интерфейс такой же, как и в iOS-версии, но он также включает некоторые специфические элементы Android, такие как боковые вкладки.

Основная задача нового продукта – помочь пользователям найти работу на ходу. Вакансии можно отфильтровать по названию, местоположению, компании, отрасли и уровню должности. Кроме того, пользователям будут предложены рекомендованные вакансии, основанные на их истории поиска. Сервис также уведомит пользователя об истечении сроков публикации объявлений.

Компания также предоставила несколько графиков, демонстрирующих различия между пользователями Android и iOS в рамках социальной сети в США.

Например, пользователи Android-устройств отправляют много приглашений в LinkedIn, в то время как пользователи iOS осуществляют больше поисков.

Что касается сферы деятельности, пользователи Android чаще работают в ИТ и программировании, в то время как пользователи Apple – в сфере здравоохранения и графического дизайна.

Приложение Job Search доступно в Play Store пользователям из англоязычных стран.

Напомним, что в январе этого года LinkedIn улучшил функцию поиска людей, работы и сообщений. Теперь поиск стал персонализированным ***(LinkedIn запустил приложение по поиску работы для Android // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_zapustil_prilozhenie_po_poisku_raboty_dlya_android). – 2015. – 27.03).***

***

Социальная сеть Facebook продолжает завоёвывать крайне конкурентный рынок мобильных мессенджеров. Ежемесячная аудитория приложения Facebook Messenger превзошла отметку в 600 млн пользователей.

Впечатляет не только количество пользователей, но и темпы, которыми мессенджер расширяет аудиторию. Всего четыре месяца назад – в ноябре 2014 г. – пользовательская база приложения составляла 500 млн. 100 млн дополнительных пользователей за такой короткий срок – весьма внушительное достижение.

Главным конкурентом Facebook Messenger является приложение WhatsApp, также принадлежащее Facebook, его ежемесячная аудитория – больше 700 млн человек. Социальная сеть за явным преимуществом лидирует в гонке мобильных мессенджеров. Совокупная аудитория приложений компании превышает 1,3 млрд пользователей, что позволяет оставить далеко позади всех конкурентов. Ближайший конкурент – китайский интернет-конгломерат Tencent – его приложениями WeChat и QQ Mobile пользуются около 1 млрд человек.

Несмотря на сравнимые по размеру пользовательские базы и функциональность, подход к развитию Facebook Messenger и WhatsApp кардинально различается. Если WhatsApp остаётся «чистым» мессенджером, не обременённым сторонними сервисами, то из Messenger в Facebook стараются сделать полноценную платформу. Возможно, руководство сети, таким образом, убивает двух зайцев разом: у Facebook появляется шанс полностью доминировать на рынке мобильных мессенджеров. WhatsApp будет конкурировать с приложениями вроде Kik, Viber и Telegram, в то время как Facebook Messenger вступит в борьбу с азиатскими платформами WeChat, Line и KakaoTalk ***(Аудитория Facebook Messenger превысила 600 млн // InternetUA (http://internetua.com/auditoriya-Facebook-Messenger-previsila-600-mln). – 2015. – 29.03).***

***

Facebook Messenger будет открыт для сторонних приложений. Об этом пишут Новости ИТ со ссылкой на 3D-News.

До сегодняшнего дня пользователи Facebook Messenger были полностью погружены в экосистему социальной сети. Обмен сообщениями, звонками, изображениями, файлами происходит строго в рамках системы Facebook. Единственный способ для третьей стороны поучаствовать в информационном

потоке – кнопка «Отправить» – с её помощью пользователи могут пересылать ссылки друг другу.

По сообщению TechCrunch, Facebook намерена изменить такой подход и превратить Messenger в полноценную платформу. Для этого компания откроет доступ к мессенджеру разработчикам сторонних приложений.

Как будет происходить взаимодействие, пока не ясно. Источники внутри компании сообщают, что сначала третья сторона получит возможность создавать контент и информационные потоки внутри приложения. Например, это может быть бизнес, предлагающий свои услуги напрямую пользователям, или друзья, обменивающиеся контентом, не привязанным к Facebook.

Аналитики замечают, что в данном случае Facebook явно копирует стратегию многих азиатских компаний. Разработчики мессенджеров WeChat, Line и KakaoTalk давно развивают свои приложения в формате платформ. Их пользователи могут вызвать такси, сделать платёж, заказать столик в ресторане, не покидая приложения.

Стоит отметить, что инновации компании пока обходят стороной мессенджер WhatsApp, который может похвастаться большей ежемесячной аудиторией. Трудно сказать, есть ли у социальной сети планы по преображению WhatsApp, возможно, приложение так и останется «чистым» мессенджером, а нововведения будут уделом Facebook Messenger ***(Facebook превратит Messenger в полноценную платформу // Новости ИТ (http://www.novostiit.net/facebook-prevratit-messenger-v-polnotsennuyu-platformu-00017728). – 2015. – 22.03).***

***

Twitter исполнилось девять лет. Отпраздновать очередной год сервис решил весьма своеобразно – сняв трогательное видео с детьми, которые рассказывают, чем так хорош этот возраст, и скромно благодаря своих пользователей, которые были с Twitter все эти годы. Об этом пишет likeni.ru.

Прошедший год был достаточно плодотворным для Twitter:

Согласно финотчету компании за IV квартал 2014 г., месячная активная аудитория платформы составила 288 млн, увеличившись на 4 млн по сравнению с III кварталом 2014 г. Доля мобильных месячных пользователей составила 80 % от общего числа месячных пользователей. А количество просмотров ленты увеличилось на 23 % по сравнению с прошлым годом и достигло 182 млрд в IV квартале.

В январе 2015 г. Twitter запустил собственную видеоплатформу, позволяющую мобильным пользователям загружать ролики длительностью до 30 с.

В бета-режиме были запущены продвигаемые рекламные видео.

Была запущена бета-версия новой системы оплаты за рекламу, позволяющей оплачивать конкретные действия пользователей.

Twitter добавил в список своих рекламодателей 12 новых стран, а в ноябре представил официального партнера по продаже рекламы в России.

Twitter предоставил подписчикам возможность узнать, кто и каким образом взаимодействовал с их твитами, посредством Tweet activity dashboard и открыл доступ к Twitter Analytics по всему миру ***(Twitter исполнилось 9 лет // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42849/118/lang,ru/). – 2015. – 23.03).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В обласному центрі Волині презентували пілотну версію електронного проекту «Всеукраїнська соціальна мережа “Фейсгов”». Про це повідомляє «Волинська правда».

Так, згідно зі стратегією програми розвитку Волині, до 2020 р. був розроблений окремий розділ, що стосується електронного врядування. Таким чином, робоча група створила проект, який уже презентували, проте його обговорення ще триває. Наразі створено його пілотну версію, а до 31 березня охочі можуть висловити свої пропозиції та доповнення. Після відпрацювання такої інформації, у травні цього року громадськості представлять версію продукту для тестування.

Керівник проекту Д. Гаврилов розповів, що місією є створення мережі, яка надасть можливість жителям регіонів контролювати органи державної влади та державні установи на предмет виконання їх функцій та запобігати розвитку корупції.

За словами керівника мережі, ідея розробки проекту виникла після Євромайдану. Аби зробити владу відкритішою для народу, постало питання створення подібного ресурсу. «Цей ресурс створений для того, щоби людина могла зареєструватися і подати запит. Наприклад, питання по роботі жкг, освіті, охороні здоров’я... Задати питання державному службовцю чи чиновнику», – зазначає Д. Гаврилов. На його думку, «Фейсгов» дасть змогу створити позитивний імідж влади, показати результати її роботи. У свою чергу люди зможуть проконтролювати роботу держслужбовців, пришвидшити процес розв’язання актуальних проблем населення, запобігти розвитку корупції та хабарництва.

У цій електронній системі також передбачена функція «лайк». Подібно як і в інших соцмережах, люди можуть створити рейтинг довіри до посадовців та чиновників. Підтримуючи або не підтримуючи їх, лайкаючи чи ні, державні службовці отримують рейтинг довіри населення до себе та результатів своєї роботи.

Таким чином, наразі реалізована пілотна версія продукту, внесена база даних регіональних гілок влади Волинської області та планується протестувати версію продукту з розширеним функціоналом у травні.

Зрештою, функції соціальної мережі ще обговорюються, сайт розробляється, тож виокремивши всі його недоліки та переваги, його почнуть запускати в дію ***(У Луцьку презентували пілотну версію соціальної мережі // Волинська правда (http://www.pravda.lutsk.ua/ukr/news/73099/). – 2015. – 18.03).***

***

Мешканці анексованого Росією півострова Крим викладають фотографії своїх паспортів зі зворушливими підписами.

Кримчани, для яких анексія півострова стала реальною проблемою, уже давно створювали такі патріотичні світлини, які відображують ставлення місцевих жителів до подій «російської весни». Тепер же в мережі вони вирішили організувати флеш-моб, повідомляє Еспресо.TV із посиланням на повідомлення батальйону «Азов» у Facebook.

Так само, як і жителі Сходу, вони поруч із пропискою в паспорті фотографували наклейки з текстом «Крим хоче додому!» та іншими написами ***(Крим хоче додому! – Кримчани в мережі влаштували патріотичний флеш-моб // Espreso.tv (http://espreso.tv/news/2015/03/26/krym_khoche_dodomu___krymchany_v_merezhi_vlashtuvaly_patriotychnyy_flesh_mob). – 2015. – 26.03).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Брендовые компании-рекламодатели все чаще стали публиковать свои рекламные объявления в Instagram, постепенно уходя из социальной сети Facebook. Такое исследование провела аналитическая компания L2, пишет Marketing Media Review (http://mmr.ua/news/id/brendovye-kompanii-perehodjat-iz-facebook-v-instagram-43604/).

На сегодняшний день количество брендовых постов в Instagram превышает количество постов в соцсети Facebook. Такое положение дел специалисты-аналитики связывают с новой политикой социальной сети.

Согласно вступившим в силу новым правилам Facebook, алгоритм органического охвата аудитории был снижен. Чтобы рекламу увидели как можно больше пользователей, компании должны были платить за дополнительное размещение. Если этого не сделать, то пост будет висеть некоторое время, пока не наберет определенное количество просмотров или лайков, а потом исчезает. Facebook объяснил такое нововведение тем, что

пользователи стали недовольны засильем рекламных объявлений, поэтому разработчики и решили ввести инструмент, благодаря которому каждая отдельная реклама будет нацелена на определенную аудиторию. Это должно принести большую пользу от размещения объявлений как для посетителей, так и для рекламодателей, пояснили в Facebook. Однако компании не отнеслись с особым восторгом к этому и стали искать новые средства для продвижения своей продукции.

Поскольку в последнее время ресурс Instagram имеет огромную популярность среди пользователей, число которых возросло в несколько раз за последние месяцы, рекламодатели обратили пристальное внимание на него. В отличие от Facebook, Instagram сейчас остается открытым для информации любого контента.

За IV квартал 2014 г. компания L2 исследовала деятельность 250 брендов. Каждую неделю они размещали в Instagram 9,3 постов, а в Facebook 8,8. Для сравнения, в 2013 г. эти показатели равнялись 7,5 и 11,1 соответственно

Стоит отметить, что такой переход от Facebook к Instagram является предсказуемым шагом для маркетолов, поскольку органический охват последнего выглядит намного привлекательнее. Кроме этого, аналитики выяснили, что лидером по вовлечению пользователей к постам стал автомобильный сегмент – 1,52 %. На втором месте оказались посты с напитками – 1,32 % вовлечения.

Из числа самых эффективных постов оказались посты, содержащие только рекламы – 65 %. Далее идут посты с фотографиями – 43 %, и посты с известными людьми – 29 % ***(Брендовые компании переходят из Facebook в Instagram // Marketing Media Review (http://mmr.ua/news/id/brendovye-kompanii-perehodjat-iz-facebook-v-instagram-43604/). – 2015. – 16.03).***

***

Facebook будет предоставлять агрегированную информацию о пользователях другим компаниям, которые таким образом будут получать отзывы на свою продукцию и смогут улучшить маркетинговую стратегию.

Крупнейшая социальная сеть мира запустит новый сервис под названием Topic Data. Компании смогут использовать его, чтобы читать отзывы пользователей Facebook на свои бренды, продукцию, мероприятия и деятельность в целом. Facebook уточнила, что вся информация будет сводной и анонимной, то есть не раскроет конфиденциальных данных и не позволит отследить конкретного комментатора, пишет The Wall Street Journal.

Сторонние компании уже используют данные Facebook для таргетированной рекламы. Однако теперь они впервые смогут получить уникальную информацию и использовать ее для разработки новой продукции, различных исследований и принятия решений о целевой аудитории. «Для мира сбора данных на платформах соцсетей это действительно новость. Бытовая информация такого уровня имеет неограниченную ценность не только в

маркетинге», – заявил главный специалист по маркетингу аналитической компании Brandwatch У. Макиннз.

В этом проекте помогать Facebook будет компания DataSift, которая обеспечит доступ к собираемым данным. DataSift будет извлекать информацию из соцсети и предоставлять фирмам, которые будут анализировать и продавать ее подходящим клиентам.

Использование данных с целью узнать поведение и вкусы потребителей уже практиковали компании StockTwits и DataMinr. Они отслеживали сообщения пользователей соцсети Twitter для клиентов из сферы финансов, СМИ и государственного сектора. Twitter сообщил, что за IV квартал 2014 г. заработал 47 млн дол. по статье «разрешение на пользование информацией и иные доходы» ***(Facebook продаст данные об отзывах пользователей сторонним компаниям // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/16/Facebook-to-sell-data.html). – 2015. – 16.03).***

***

Користувачі Facebook у США незабаром зможуть переводити один одному грошові кошти з банківських карт, повідомляється в блозі американської соціальної мережі.

Для того, щоб скористатися новою можливістю, потрібно буде відкрити повідомлення на сайті, розпочати діалог і, натиснувши на значок долара, вказати суму. Перед цим необхідно буде прив’язати свою карту до акаунту соцмережі, повідомляє Еспресо.TV із посиланням на Росбалт.

Facebook запевняє, що особисті дані клієнтів будуть надійно захищені, нагадуючи, що компанія і сьогодні проводить до мільйона транзакцій в день: платежі за рекламу і мережеві комп’ютерні ігри.

Нині лідером ринку інтернет-платежів є американська система PayPal, що має 162 млн активних користувачів. Світова місячна аудиторія Facebook становить близько 1,32 млрд осіб ***(Facebook надасть користувачам можливість грошових переказів // Espreso.tv (http://espreso.tv/news/2015/03/18/facebook_nadast_korystuvacham_mozhlyvist_hroshovykh_perekaziv). – 2015. – 18.03).***

***

Эксперты говорят о трех основных последствиях запуске платежной функции в своем мессенджере от Facebook – двух положительных и одном отрицательном.

1. Новый платежный функционал поможет Facebook не терять актуальность среди пользователей молодого поколения.

Около года назад компания представила свой сервис обмена сообщениями Facebook Messenger. Пользователей начали переводить из основного приложения в дополнительное для осуществления основных функций. Вскоре мессенджер завоевал популярность и остается одним из

самых часто загружаемых приложений. Тогда Facebook задумался над следующим вопросом: что еще представители молодого поколения хотят делать в социальной сети со своими друзьями? Ответ – пересылать деньги.

2. Facebook получил возможность предложить продавцам и рекламодателям новые возможности благодаря расширенной базе данных.

Facebook теперь имеет возможность создавать дополнительные преимущества: расширяя функционал сервиса отправки денежных переводов за рамки обычного списания средств с дебетовых карт, Facebook сможет привлечь большее количество пользователей, не подключенных к банкам, и предложить им такие решения, как микрокредитование, отправка подарков, групповые покупки и др. Таким образом, социальная сеть повышает свою ценность и занимает новые ниши на рынке.

3. Негативным последствием внедрения P2P-переводов является растущая уязвимость Facebook.

Собирая крупные объемы платежной информации пользователей, Facebook становится «большой рыбой» для кибермошенников. Обрабатывая более миллиона транзакций ежедневно в пользу геймеров и рекламодателей, после запуска нового платежного сервиса Facebook будет наращивать объем операций и накапливать еще больше конфиденциальной информации пользователей. Соответственно, защита информации должна быть укреплена ***(Платежи в мессенджере Facebook могут быть небезопасными // InternetUA (http://internetua.com/plateji-v-messendjere-Facebook-mogut-bit-nebezopasnimi). – 2015. – 21.03).***

***

Социальная сеть Pinterest привлекла 367 млн дол. и намерена довести размер текущего раунда инвестиций до 578 млн.

Теперь Pinterest, капитализацию которой оценивают 11 млрд дол., войдёт в лидирующую десятку рейтинга самых дорогих стартапов, составленного аналитиками CB Insights.

Казалось, что интерес Pinterest иссяк. Год назад закрылись даже российские клоны Pinterest. Однако спрос на хай-тек в настоящее время высок и подогревается не только астрономической капитализацией Apple. Дело в том, что на фондовом рынке уже давно не появлялось новых крупных интернет-компаний. После IPO компаний Facebook и Twitter, а также китайской Alibaba, сколько-либо заметным явлением стал только Lending Club, однако вся капитализация этой компании составляет лишь 7 млрд дол. Информационные технологии создали большой рынок – даже акции AT&T в индексе Доу Джонса заменяют на акции Apple, однако на фондовом рынке торгуется небольшое количество очень крупных игроков на фоне отсутствия средних компаний. В хай-тек секторе фондового рынка ощущается дефицит новых бумаг. Поэтому инвестбанкиры ищут компании, которые смогут пополнить их ИТ-компоненты портфелей наряду с Facebook и Twitter.

Самым дорогим стартапом сегодня является китайский производитель смартфонов Xiaomi (45 млрд дол.), за которым идёт приложение для вызова такси Uber, а третье место занимает уже упоминавшийся выше Shapchat. Кстати, чудовищные оценки капитализации не являются всего лишь умозрительными цифрами, которые никто не готов платить. Например, в 2014 г. Facebook предлагал за Snapchat 3 млрд дол. и в итоге получил отказ. А за поглощение мобильный мессенджер WhatsApp было предложено уже 19 млрд. Причём, поскольку платить М. Цукерберг хотел не наличными, а акциями Facebook, в итоге заплатить пришлось почти 22 млрд ***(Pinterest привлёк $367 млн и вошёл в десятку самых дорогих стартапов // ITnews (http://itnews.com.ua/news/76382-pinterest-privlyok-367-mln-i-voshyol-v-desyatku-samykh-dorogikh-startapov). – 2015. – 17.03).***

***

Видео в Facebook эффективно, даже если пользователь просматривал его менее одной секунды, сообщается в последнем исследовании Nielsen, пишет Marketing Media Review (http://mmr.ua/news/id/video-v-facebook-effektivno-dazhe-esli-polzovatel-ego-ne-smotrit-43669/).

Даже если пользователь задержал свой взгляд на ролике всего на секунду и меньше, видео все равно оказывает на него воздействие – с точки зрения запоминаемости рекламы, узнаваемости бренда и принятия решения о покупке товара. Чем дольше пользователь смотрит видео – тем выше эффект.

Как показало исследование, пользователи, которые просматривали видео менее трех секунд, составляют до 47 % общей ценности кампании, а пользователи, которые смотрели видео менее 10 секунд, – до 74 %, в зависимости от метрик. Это означает, что эффективность возрастает по мере увеличения времени просмотра, однако, пользователи вовсе не должны смотреть видео полностью, чтобы было оказано необходимое воздействие. Даже просмотры ролика менее 10 секунд эффективны в построении узнаваемости бренда и повышении намерений пользователя что-либо купить.

Что это значит для маркетологов?

Так как пользователи потребляют digital-контент по-разному, очевидно, что число просмотров видео не дает рекламодателям достаточно информации для определения ценности digital-рекламы. Маркетологи должны экспериментировать с короткими видеокреативами, чтобы приносить дополнительную ценность бренду, не забывая о том, что она растет по мере увеличения длительности просмотра видео. И как всегда, рекламодатели должны продолжать оптимизировать рекламу под цели кампании, но, и не забывать смотреть не только на число просмотров, при измерении ее эффективности.

Каждая секунда видео – от первоначального показа до полного просмотра и все, что между ними, – дает бренду ценность. Понимание этого поможет рекламодателям создавать правильный контент и добиваться успеха ***(Видео в Facebook эффективно, даже если пользователь его не смотрит // Marketing***

Media Review (http://mmr.ua/news/id/video-v-facebook-effektivno-dazhe-esli-polzovatel-ego-ne-smotrit-43669/). – 2015. – 19.03).

***

Facebook запустила новую опцию таргетинга. Теперь рекламодатели получили возможность нацеливать свои объявления на людей, проживающих за пределами их родной страны. Аудитория иностранцев в Facebook составляет 92 млн человек, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-vnedril-targeting-na-inostrancev-43644/).

Новая опция позволяет нацеливать рекламу на иностранцев, проживающих в конкретной стране, или на граждан указанной страны, проживающих за рубежом. Этот вид таргетинга уже доступен для пользователей из Индии, Бразилии, Индонезии, Китая и Южной Африки.

В официальном блоге Facebook сообщается, что этот функционал был протестирован прошлой осенью компанией Средневосточных авиалиний Etihad Airways накануне индийского праздника Дивали. По данным Facebook, в социальной сети зарегистрировано 27 млн индийцев, проживающих за пределами родной страны.

«Используя таргетинг на иностранцев, Etihad разослал им рекламные сообщения с предложением о поездке домой на праздник. В результате было достигнуто 536 индийцев, проживающих на Среднем Востоке, что привело к бронированию 700 авиабилетов и 50-кратному возврату вложенных средств».

Таргетинг на иностранцев доступен для рекламодателей во всём мире на всех рекламных интерфейсах Facebook.

Настройки таргетинга поддерживают указание следующих типов соединений: 2G, 3G и 4G ***(Facebook внедрил таргетинг на иностранцев // Marketing Media Review (http://mmr.ua/news/id/facebook-vnedril-targeting-na-inostrancev-43644/). – 2015. – 18.03).***

***

Сервис микроблогов Twitter намерен заработать на продаже пользовательских записей так называемым анализаторам данных, которые в свою очередь передают полученную информацию рекламодателям, статистическим компаниям и даже службам охраны порядка. Об этом пишет Marketing Media Review со ссылкой на газету The Guardian (http://mmr.ua/news/id/twitter-zarabotaet-na-prodazhe-tvitov-43686/).

Мгновенный анализ пользовательских данных интересен не только рекламодателям, извлекающим коммерческую выгоду, но даже ученым и полиции. Определяя настроение толпы, к примеру, футбольных болельщиков, полиция может оперативно реагировать и предупреждать массовые беспорядки.

Twitter практиковал продажу «твитов» в прошлом году, однако пока продажа данных составляет небольшую часть общего дохода сервиса микроблогов. В 2014 г. из общей прибыли в 1,3 млрд дол. только 70 млн дол. были получены в результате продажи пользовательских «твитов». Однако

компания строит большие планы относительно данного источника доходов ***(Twitter заработает на продаже твитов // Marketing Media Review (http://mmr.ua/news/id/twitter-zarabotaet-na-prodazhe-tvitov-43686/). – 2015. – 20.03).***

***

Тренды Social Media на 2015 г.

Украинская ассоциация по связям с общественностью (UAPR) и Европейская ассоциация руководителей по коммуникациям (EACD) совместно с компанией Microsoft Украина провели круглый стол на тему: «Коммуникации в digital-эру». Спикерами выступили В. Дегтярев (CEO Newsfront Agency), Т. Плешивцева (PR-директор, Microsoft) и приглашенный спикер Ф. Бореманс (Van Marcke Group (Брюссель)). На круглом столе обозначили ключевые тренды Social Media на 2015 г. и дальше, пишет Marketing Media Review (http://mmr.ua/news/id/jhg-43715/).

Будущие сети:

Ello: эксперты утверждают, что хипстерская социальная сеть, организованная дизайнерами, художниками и прочими творческими единицами, к концу года значительно увеличит количество своих пользователей. Уже сейчас площадка насчитывает более одного миллиона пользователей. Главное отличие от остальных соцмедиа – ad-free – полное отсутствие какой либо рекламы.

Facebook: стоит отметить, что охват публикаций будет падать, а вот стоимость рекламы возрастет на 10 % по сравнению с 2014 г. Тем не менее, количество пользователей сети будет увеличиваться.

Twitter: ресурс станет основным каналом коммуникации для малого и среднего бизнеса, так как их основная потребность – платить за результат, а не за узнаваемость бренда.

Google+: в начале 2014 г. этой сети предрекали стремительный рост пользователей и активное использование крупными брендами, однако же в 2015 г. прогнозы весьма плачевны – сеть закончит свое существование, так как не представляет никакой существенной ценности.

Instagram, напротив, станет лидером среди маркетологов – более чем 42 % маркетологов выбирают Instagram для публикаций своего контента, вместе с тем доля видеопубликаций также будет возрастать. По некоторым прогнозам к концу 2015 г. Instagram обойдет основного конкурента по видеоконтенту Vine.

LinkedIn: более чем 88 % маркетологов используют сеть, как основной канал коммуникаций B2B, и в этом она может обойти даже Facebook.

Так или иначе, будут появляться новые социальные сети для конкретной профессиональной аудитории, где все участники будут обмениваться опытом друг с другом.

В рамках круглого стола Ф. Бореман, PR-специалист с 20-летним опытом в области корпоративных коммуникаций и управлении репутационными рисками, а в настоящее время главный эксперт и руководитель проектов

социальных медиа компании Van Marcke Group (Брюссель), поделился европейским опытом использования социальных сетей и теми уроками, которые удалось получить.

Крупные бренды давно воспринимают социальные медиа как опорный инструмент построения маркетинг-стратегии. Потребность в качественном анализе продуктивности сетей возрастает, хотя многие продолжают строить sm-активность экспериментально и интуитивно. Чтобы получить результат, необходимо точечно использовать средства маркетинга под каждый тип транслируемого сообщения.

Шаги, которые должен сделать каждый бренд в SM.

В первую очередь, необходимо определить ключевую информацию, а затем уже канал, по которому ваша целевая аудитория её получит. Два момента, на которые важно обратить внимание – публикация и её распространение. Считают, что главное – это забавный контент на странице бренда, но это не так. Нельзя одно и то же сообщение распространить по разным каналам и ожидать одинаковый результат.

Важно научиться создавать контент, который появится в нужном месте в нужное время. Форма подачи контента зависит от диалога, который вы устанавливаете с клиентами. Время публикаций напрямую также зависит от контента, но лучше вести тематический план ведения страницы в сети.

Невозможно выделить конкретные тренды, потому что всё в тренде!

Главное для компаний – полностью интегрировать SM в PR/Маркетинг-стратегию. Невозможно выделить конкретные тренды, потому что всё в тренде! Но must have для всех без исключения:

– больше нет PR-менеджеров, есть менеджер по репутации, который занимается digital-каналами наравне с другими;

– понятный язык ваших публикаций, всегда важен качественный storytellin;

– анализ данных, инвестируйте в аналитику и профессионалов, которые помогут вам посчитать эффективность ваших digital-механизмов;

– работа с обратной связью, научитесь не просто транслировать свои месседжы, но и слушать, что отвечают ваши фолловеры.

К примеру, Facebook – первоначально общество людей, а не канал связи для брендов. Лишь 20 % людей генерируют контент в сети, остальные просто следят за метериалами. Пример, когда публичный человек активно ведет страницу профиля и набирает фолловеров, в случае страниц популярных брендов не работает. Компания должна подавать информацию о продукте таргетированно. Фокусируйтесь на одной задаче, и используйте инструменты измерений эффективности конкретно для неё ***(Тренды Social Media на 2015 год // Marketing Media Review (http://mmr.ua/news/id/jhg-43715/). – 2015. – 24.03).***

***

Twitter начал тестировать автоматическое проигрывание рекламных видеороликов в ленте. Тестирование проходит в ограниченном масштабе.

Доступ к новому функционалу получила небольшая группа пользователей iOS-устройств. Об этом пишет searchengines.ru.

По информации издания AdAge, опция автопроигрывания применяется только к продвигаемым видео, которые пользователи загружают через мобильное приложение Twitter, а также к клипам, которые являются частью программы Amplify, позволяющей таким компаниям, как ESPN и NFL публиковать в сети свои видео с рекламой в формате pre-roll.

В рамках теста, Video Vine не будут автоматически воспроизводиться в ленте Twitter.

Одна часть эксперимента Twitter предполагает, что некоторые пользователи будут видеть видео, целиком воспроизводимые в ленте. В то время как другие – 6-секундные превью, предшествующие видеоролику. Оба формата будут проигрывать видео с выключенным звуком. При нажатии на понравившийся ролик, он будет расширен на весь экран и его можно будет просмотреть со звуком ***(Twitter тестирует автопроигрывание рекламных видео в хронике // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42860/118/lang,ru/). – 2015. – 24.03).***

***

Facebook расширила возможности управления рекламой LiveRail на мобильную дисплейную рекламу. Это значит, что издатели могут использовать технологию, чтобы продавать видео- и дисплейную рекламу в своих мобильных приложениях, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-mobilnuju-reklamnuju-birzhu-na-baze-liverail-43755/).

LiveRail является сервером объявлений Facebook для видео-рекламы и представляет собой технологию, которая помогает издателям управлять их рекламным видеоинвентарем и обеспечивать правильный показ рекламы правильным пользователям.

Как в рекламной бирже, LiveRail может продать на аукционе дополнительное рекламное место по самым высоким ставкам, чтобы обеспечить заполнение всех площадок. До сих пор биржа LiveRail ограничивалась видеорекламой.

LiveRail теперь будет использовать свои анонимные данные о пользователях, чтобы помочь издателям лучше обслуживать целевую рекламу вне Facebook. Вместо того, чтобы для таргетирования посетителей полагаться на cookies, издатели, использующие LiveRail, смогут добавлять пользовательские данные Facebook, чтобы получить лучшее представление о том, кто смотрит рекламу.

Поскольку все больше издателей и рекламодателей используют данные Facebook вместо cookies для таргетинга объявлений, это увеличит преимущества LiveRail для покупки рекламы вплоть до вытеснения других рекламных бирж и сетей, по-прежнему использующих cookies.

Изменения должны встревожить Google и Twitter. Google уже предлагает DoubleClick, а Twitter – MoPub, каждая из которых действует в качестве подобных рекламных бирж.

Преимущество Facebook заключается в пользовательских данных, которые он учитывает в своих рекламных инструментах, благодаря чему и отличается от конкурентов. Twitter предлагает некое таргетирование пользователей в MoPub, но не при каждой сделке. DoubleClick от Google больше ориентирован на интент. При этом в Facebook полагают, что располагают лучшими пользовательскими данными, чем Twitter или кто-либо еще.

Целью Facebook является предоставление издателям рекламного инструмента, в котором те нуждаются, от управления и отслеживания объявлений до продажи рекламного пространства вообще и в режиме реального времени в частности.

Представители социальной сети Facebook объявили о покупке сервиса онлайн-видеорекламы LiveRail летом 2014 г. По оценкам аналитиков, сумма сделки колеблется от 400 до 500 млн дол. США ***(Facebook запускает мобильную рекламную биржу на базе LiveRail // Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-mobilnuju-reklamnuju-birzhu-na-baze-liverail-43755/). – 2015. – 26.03).***

***

В этом году Twitter займёт место Yahoo как третьего по величине продавца медийной рекламы в США, сообщается в прогнозе eMarketer. Об этом пишет searchengines.ru.

В 2015 г. доля сервиса микроблогов на рынке медийной рекламы в США достигнет 5 % , Facebook – 25,5 %, Google – 13 %.

Компания Yahoo, в течение последних четырёх лет сохраняющая позицию третьего по величине продавца медийной рекламы, сместится на четвёртое место. В 2015 г. её доля на этом рынке сократится и составит 4,6 % (в 2014 г. – 5,5 %; в 2013 г. – 7,2 %).

Позиции в рейтингах ведущих компаний в отрасли онлайн-рекламы меняются по мере сдвига затрат на рекламу в сторону мобильного сегмента. В этом аспекте Twitter уже опередил Yahoo в 2014 г.: 88 % рекламного дохода Twitter приходилось на мобильные устройства, в то время как у Yahoo – только 20 %.

Подъём Twitter в рейтинге рынка медийной рекламы отображает результаты действий CEO компании Д. Костоло, направленных на показ рекламы большему количеству пользователей, включая выход продвигаемых твитов за пределы сервиса микроблогов ***(eMarketer: Twitter обгонит Yahoo по доходу от медийной рекламы в США в 2015 году // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42890/118/lang,ru/). – 2015. – 26.03).***

***

Facebook запустила два новых образовательных ресурса, предназначенных для маркетологов. Они призваны помочь компаниям, размещающим рекламу в соцсети, найти ответы на многие интересующие их вопросы, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-dva-novyh-obrazovatelnyh-resursa-dlja-marketologov-43735/).

Инструмент, получивший название Blueprint, представляет из себя образовательную программу, позволяющую агентствам, партнерам и размещающим рекламу компаниям научиться эффективнее пользоваться Facebook для создания более совершенных кампаний и улучшения финансовых показателей своего бизнеса. Blueprint совмещает в себе онлайн-курсы, очные занятия и сертификацию. Основа ресурса – центр электронного обучения, предлагающий более 35 онлайн-курсов.

Ресурс Learn How предназначен для небольших компаний и специалистов по маркетингу, ранее не работавших с Facebook. Он поможет более эффективно использовать Pages и Ads. Маркетологи найдут ответы на часто задаваемые вопросы с помощью изображений и пошаговых инструкций. Контент ресурса организован так, что ответы на вопросы можно будет находить по мере их поступления.

Компания также обновила Facebook for Business, упростив дизайн страниц и добавив новые материалы, предоставляющие пользователям информацию о том, как Facebook помогает клиентам улучшить результаты своей деятельности. Более подробную информацию обо всех нововведениях можно найти в блоге Facebook for Business ***(Facebook запустил два новых образовательных ресурса для маркетологов // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-dva-novyh-obrazovatelnyh-resursa-dlja-marketologov-43735/). – 2015. – 25.03).***

***

Социальная сеть «ВКонтакте» приняла решение в полном объеме отказаться от возможности использования денежных переводов среди пользователей. Об этом сообщил пресс-секретарь «ВКонтакте» Г. Лобушкин.

Представитель соцсети пояснил, что подобный бизнес не только не является для «ВКонтакте» профильным, но и противоречит нормам российского законодательства, применительно к основной деятельности компании. Также Г. Лобушкин напомнил, что еще несколько лет назад пользователи «ВКонтакте» могли приобретать реальные товары за деньги, но вскоре руководство соцсети приняло решение отказаться от развития этого направления.

Сегодня «ВКонтакте» оперирует собственной внутренней валютой – голосами. С их помощью можно купить, например, виртуальные подарки, а также различные артефакты и улучшения в игровых приложениях. Голоса нельзя перевести другому пользователю соцсети или потратить на реальные материальные товары. При этом получить голоса можно за реальные деньги, и

такие операции приносят «ВКонтакте» половину от общего ежегодного дохода ***(«ВКонтакте» окончательно отказалась от идеи с p2p-переводами // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vkontakte_okonchatelno_otkazalas_ot_idei_s_p2p_perevodami). – 2015. – 26.03).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

З Інтернетом краще виходить навчатися, але він має негативний вплив на мораль. Українці, наприклад, майже всі проводять час у соціальних мережах та говорять там про що завгодно, включаючи політику, стверджується в дослідженні Інтернету від компанії Pew Research.

Україна залишається країною звичайних телефонів: їх мають 73 % співвітчизників. Тоді як смартфонами володіють лише 18 %, а 9 % взагалі залишаються без мобільного зв'язку. Для порівняння, у Китаї «розумні» мобільники мають 57 % користувачів, а звичайні телефони є в 42 % населення.

Найчастіше мобільник для українців – це спосіб обмінюватися sms. Це роблять 68 % користувачів мобільного зв'язку. Зйомка фото та відео не такі популярні – цим займаються лише 45 %.

А ось комп'ютери має більше половини населення нашої держави (56 %).

І більше 73 % користується ними та іншими гаджетами для щоденного доступу в Інтернет. З нього українці черпають новини про політику (80 %), здоров'я та медицину (64 %), інформацію про владу та її послуги (50 %). Крім того, співвітчизники використовують Інтернет для пошуку роботи (33 %), оплати товарів та послуг (32 %), купівлі продуктів (44 %), онлайн-навчання (10 %). При цьому майже всі українці (93 %) використовують мережу для того, щоб залишатися на зв'язку з друзями та близькими.

Українців у віртуальному просторі стає дедалі більше: уже 53 % співгромадян користуються Інтернетом. За цим параметром ми йдемо майже на рівні з Бразилією та Єгиптом, але відстаємо від Китаю, Чилі та Аргентини.

Ми також досить багато часу проводимо в соціальних мережах. Найбільшу популярність ці сайти мають на Філіппінах (93 %) та в Кенії (88 %). Проте українці полюбляють сидіти в соцмережах, тому наша держава потрапила до топ-15. У них проводять час близько 82 % співвітчизників.

Там вони займаються різними справами та обговорюють будь-які теми: музику та фільми (55 %), спорт (33 %), різні гаджети й продукти (36) та політику (37 %). Дискутують у соцмережах про релігію лише 8 % користувачів.

Загалом українці вважають Інтернет благом, яке має гарний вплив на освіту (60 %), персональні стосунки (59 %), економіку (39 %), політику (34 %) та мораль (20 %).

Своє опитування Pew Research проводила у квітні – травні минулого року в 10 найбільших містах України, а також 29 інших державах, що розвиваються. Експерти дослідили думку 1600 українців ***(Що українці роблять в Інтернеті // InternetUA (http://internetua.com/sxo-ukra-nc--roblyat-v--nternet). – 2015. – 27.03).***

***

Активные пользователи сети Twitter чаще сталкиваются с конфликтами со своим партнером, спровоцированными именно записями в социальной сети, сообщает Донбасс. Комментарии (http://donbass.comments.ua/news/111409-otnosheniya-partnerom-ubit.html).

Как пишет Health of India, продолжительность романтических отношений при этом не имеет никакого значения.

Исследователи из Университета Миссури провели опрос более полутысячи пользователей Twitter разных возрастов. Респондентов опрашивали на предмет активности пользования социальной сетью (учитывалось количество входов, написание твитов, просмотр сообщений по подписке, число сообщений другим пользователям и ответов подписчикам). Также ученые поинтересовались, были ли конфликты с партнером, связанные с использованием соцсети.

В итоге выяснилось, что чем более активным был пользователь, тем большим был у него риск возникновения ссоры с партнером.

Отметим, что ранее те же исследователи провели подобную работу и с пользователями Facebook. Тогда было доказано, что частота использования социальной сети может «предсказать» риск связанного с ней конфликта, который в итоге приводедет к разводу и расставанию. Однако в случае с Facebook риск расставания был высок у людей, находивших в отношениях максимум три года.

В любом случае, ученые рекомендуют сократить время пользования социальной сети, если имеются проблемы в личной жизни. Хотя бы потому, что люди, слишком активно пользующиеся социальными сетями, склонны к самоотстранению, что сопровождается ростом недоверия к партнеру ***(Отношения с партнером могут «убить» социальные сети // Донбасс. Комментарии (http://donbass.comments.ua/news/111409-otnosheniya-partnerom-ubit.html). – 2015. – 26.03).***

***

Эксперты посоветовали родителям не размещать детские фото на профилях в соцсетях

Опытные специалисты из Университета в Мичигане (США) заявили, что демонстрирование новоиспеченными родителями детских снимков их детей

приносит малышам куда как больше вреда, нежели пользы. Для такого заявления существует по крайней мере пара аргументированных причин. Во-первых, психологи советуют молодым мамам, спешащим поделиться с общественностью новыми смешными снимками своего ребенка вспомнить, как в их детстве их родители так же доставали альбомы с детскими фотоснимками и демонстрировали их гостям. Когда дети подрастут, они вряд ли смогут порадоваться тому, что их часто нелепые снимки были выставлены напоказ, скорее – это вызовет у них чувство стыда и может спровоцировать развитие комплексов.

Во-вторых, не стоит забывать о том, что Интернет – общественная сеть, где любой может получить доступ к чему угодно, и никто не будет гарантировать вам, что снимки вашего любимого ребенка не попадутся какому-либо индивидууму с нездоровой психикой ***(Эксперты посоветовали родителям не размещать детские фото на профилях в соцсетях // Одной Строкой.ru (http://odnoy-strokoy.ru/?p=49814). – 2015. – 22.03).***

Маніпулятивні технології

Днепропетровский филиал Всеукраинского объединения «Свобода» разместила на своей странице в соцсети интригующее сообщение, в котором руководство призывает быть готовым к «наступлению на Москву».

«ВО «Свобода» объявляет «Наступление на Москву»!

Необходимо хорошо подготовиться и быть сильными для достижения нашей цели!

Ждите деталей в следующих сообщениях!

Слава Нации!» – говорится в сообщении ***(«Свобода» объявила «Наступление на Москву» // Днепропетровская Панорама (http://dnpr.com.ua/content/svoboda-obyavila-nastuplenie-na-moskvu). – 2015. – 15.03).***

***

Користувачі соціальних мереж є гравцями інформаційної війни і мають замислюватися над тим, чим допомогти державі.

Таку думку в ефірі програми Радіо Свобода «Культфронт» висловив засновник інтернет-видання Watcher.com.ua М. Саваневський.

Аналізуючи ситуацію в інформаційному просторі України торік і сьогодні, експерт зауважив, що ставлення користувачів соцмереж до пропаганди змінилося.

«Якщо раніше люди вважали, що треба поширювати тільки правдиву інформацію, надавати факти, то на сьогоднішній день українці є дуже активними гравцями у війні пропагандистській, де вони самі для себе вирішують, що треба публікувати що не треба», – зазначив М. Саваневський,

додавши, що в ситуації війни не можна залишатися «благородним». Водночас він зауважив, що це не стосується засобів масової інформації.

Експерт критично оцінює роль Міністерства інформації, оскільки нині відомство не має реального штату, а для ефективної інформаційної боротьби потрібні «гігантські ресурси». Він також зауважує, що сьогодні більш важливо працювати з українською аудиторією, аби вона не була залежною від російської пропаганди, аніж намагатися впливати на пропаганду в РФ.

Торік М. Саваневський зауважував, що Євромайдан спричинив кардинальну зміну взаємодії людей з інформацією: кількість переходів із соцмереж на новинні сайти збільшилася у 8–10 разів ***(М. Саваневський: Соціальні мережі – це поле війни // MediaSapiens (http://osvita.mediasapiens.ua/web/social/maksim_savanevskiy_sotsialni_merezhi_tse_pole_viyni/). – 2015. – 16.03).***

***

16 березня після трагедії в Костянтинівці кремлівська машина пропаганди розпочала свою роботу з метою загострити до межі обстановку в Україні в місті Костянтинівка (Донецька область).

Вдалося зафіксувати створення фейкової групи «Я Костянтинівка» з 6.500 учасниками (один учасник не був ботом і його видалили) із 6499 учасників більшість просто віддалені сторінки, друга частина люди з Росії та дві особи з Костянтинівки і багато з передплатників групи з'являлися в мережі ще кілька днів тому ***(Як російська пропаганда створює фейкові групи в «ВКонтакте» // СТІНА (http://www.stina.in.ua/yak-rosiyska-propaganda-stvoryuye-feykovi-grupi-v-vkontakte-video/). – 2015. – 17.03).***

***

В соцсетях сообщают о скандале с демобилизацией

16 марта в социальных сетях обсуждалась информация, что в настоящее время ребят, которые демобилизуются с 21 батальона, буквально «обирают» и заставляют за свои средства добираться домой. Прокомментировать возможный факт журналисты издания «Херсонщина за день» обратились к областным властям.

Как прокомментировал изданию изложенную информацию губернатор А. Путилов, ситуация изучается. В настоящее время готовится обращение в военную прокуратуру с просьбой разобраться: соответствует ли ситуация действительности. Со своей стороны, глава области попросил родственников или самих военнослужащих не ограничиваться анонимными заявлениями в социальных сетях, а позвонить на горячую линию ОГА или написать заявление на имя председателя ОГА и изложить конкретные факты нарушений.

«Только в таком случае можно быть уверенными, что речь идет не о провокациях. Долг органов власти, правоохранительных органов обеспечить достойную встречу наших демобилизованных Героев, защищавших Украину», – акцентировал А. Путилов ***(В соцсетях сообщают о скандале с***

демобилизацией // ХЕРСОН Онлайн (http://khersonline.net/novosti/proisshestviya/36830-v-socsetyah-soobschayut-o-skandale-s-demobilizaciey.html). – 2015. – 16.03).

***

25 березня в соціальній мережі Facebook з'явилася нібито персональна сторінка українського олігарха І. Коломойського – fb.com/Kolomoisky. Всього за добу сторінка набрала понад 50 тис. прихильників.

Щоправда, уже 26 березня І. Коломойський спростував наявність будь-яких його акаунтів у соціальних мережах: «Усі заяви, які від мого імені будуть з'являтися найближчим часом без мого особистого контакту із засобами масової інформації, якщо вони не з'являються в агентстві УНІАН або в ТСН, прошу вважати явною провокацією або фейком.

Щоб уникнути непорозумінь також заявляю, що не веду ніяких особистих сторінок у соцмережах» ***(Фейкова сторінка Коломойського у Facebook за добу набрала 50 тис прихильників // UkrainianWatcher (http://watcher.com.ua/2015/03/26/feykova-storinka-kolomoyskoho-u-facebook-za-dobu-nabrala-50-tys-pryhylnykiv/). – 2015. – 26.03).***

***

На страницах сайтов сепаратистов «ДНР» и «ЛНР» появились публикации с соцопросом за создание «Днепропетровской республики Коломойского».

Не успел И. Коломойский забрать свои вещи из кабинета, как сайты фейковой «Новороссии» начали расшатывать ситуацию в Днепропетровске, сообщает sprotiv.org.

Большинство публикаций в соцсетях появляется в группах Луганска и Донецка.

Что касается самого Днепропетровска, то такие публикации пока не замечены ***(В соцсетях уже голосуют за «народную республику» Коломойского // Громадський спротив України (http://sprotiv.org/54432). – 2015. – 26.03).***

***

Российская пропаганда больше всего влияет на украинцев, проживающих в восточных и южных областях, а также на тех, чей уровень доходов – низкий. Об этом свидетельствуют данные социологов Киевского международного института социологии, пишет Marketing Media Review (http://mmr.ua/news/id/na-kakie-oblasti-ukrainy-bolshe-vsego-dejstvuet-rossijskaja-propaganda-43752/).

Специалисты оценивали влияние пропаганды по 100-балльной шкале. Так, меньше всего пропаганде российских СМИ верят в западных областях – 12 баллов. В центральных этот показатель больше – 19 баллов. На юге – 32 и Восточный регион с Донбассом набрал целых 48 баллов.

«Юг и Восток они в наибольшей зоне риска, наиболее подвержены, соглашаются с этими тезисами, что может в будущем стать причиной дестабилизации ситуации. Этот индекс не значит заранее что определенное количество людей, они заранее готовы предпринять определенные сепаратистские действия или антиправительственные выступления, или мероприятия для дестабилизации ситуации. Но это определенная предварительная готовность, предрасположенность, в случае эскалации ситуации», – отмечает заведующий отделом КМИС А. Грушецкий.

При этом, интересно, что более чем на Донбассе, российской лжи верят в Харьковской области. В то же время украинские социологи со ссылкой на российскую негосударственную исследовательскую организацию «Левада-Центр» говорят, что в России более 80 % доверяют своим СМИ. И убеждены, что в Украине произошел государственный переворот ***(На какие области Украины больше всего действует российская пропаганда // Marketing Media Review (http://mmr.ua/news/id/na-kakie-oblasti-ukrainy-bolshe-vsego-dejstvuet-rossijskaja-propaganda-43752/). – 2015. – 26.03).***

Зарубіжні спецслужби і технології «соціального контролю»

За что социальные сети наказывают своих пользователей

Ненастоящие имена, публикация изображений предметов искусства, спам и порнография. Основатель сервиса аналитики соцсетей «Амплифера» Н. Гаджибалаев разобрался, за что именно Facebook, Instagram, «ВКонтакте», Twitter и Pinterest блокируют своих пользователей.

Социальные сети – это отражение человеческих отношений в обществе. Большинству людей понятно, как не быть заблокированным: держать один аккаунт от своего реального имени, действовать в пределах закона (без оскорблений, угроз, распространений детского порно и прочих мерзостей), не передавать логин и пароль своего аккаунта третьим лицам и сервисам и не распространять спам.

Однако у разных социальных сетей встречаются свои особенности.

Instagram

Instagram – достаточно толерантная социальная сеть: уследи-ка за сотнями миллионов пользователей и миллиардами фотографий! Однако есть несколько вещей, которые социальная сеть не прощает ни обычным пользователям, ни мировым звёздам.

Ню-фото. Instagram придерживается нулевой терпимости к откровенным фотографиям – они удаляются, пользователю выносится предупреждение, а за повторные нарушения следует бан. Однако у правил есть немало странных исключений. К примеру, не допускаются изображения женских сосков, однако можно выкладывать фотографию кормления детей грудью.

К мужской груди нет вообще никаких ограничений. А ещё Instagram очень не любит обнажённых детишек и банит даже аккаунты их родителей за фото невинных пупков.

Самоистязание. Социальная сеть не любит фотографии тощих или чрезмерно полных тел, изображения хирургических операций, крови, порезов и другого причинения вреда здоровью.

Нарушение закона. Instagram забанит вас за фотографии, на которых вы курите марихуану или продаёте человеческие органы оптом. Кроме того, сеть сразу обратится в полицию с соответствующим заявлением. А вот оружием в Instagram торговать можно – правда, только в США.

Спам. Социальная сеть распознаёт навязчивую саморекламу в комментариях, хэштегах и тегах других аккаунтов на фотографиях.

Оскорбления. Жалобы на оскорбления в Instagram рассматриваются, аккаунты провинившихся удаляются.

Чужие фото. Если кто-то использует в Instagram ваше фото, вы можете пожаловаться, и социальная сеть накажет мерзавца. Однако не советуем делать скриншот аккаунта нарушителя и публиковать его у себя (тем более с пожеланиями гореть в аду). Это может быть расценено как окорбление, и за это забанят уже вас.

Фото не с телефона. Instagram разрешает публиковать фотографии только из мобильного приложения. Кроме того, запрещается передавать свои логин и пароль третьим лицам. Это значит, что любые сервисы для постинга в Instagram нарушают правила, и опубликованные через них фотографии могут быть удалены вместе с вашим аккаунтом.

«ВКонтакте»

Со «ВКонтакте» ситуация весьма странная. С одной стороны, в потаённых уголках социальной сети можно найти как детское порно, так и агитационные пункты исламских террористов. С другой стороны, можно лишиться аккаунта и попасть под суд просто за репост чужой записи. Есть и другие способы лишиться страницы.

Нарушение правил сайта. «ВКонтакте» блокирует за распространение спама, коммерческую деятельность, загрузку порнографических материалов. Могут наказать и за оскорбляющую аватарку или описание страницы, а также за мат. Обычно за нарушения следует временное ограничение в использовании страницы. За рецидив следует вечный бан.

Взлом. Если страница оказалась в руках злоумышленников и её регистрационные данные были изменены, её заблокируют.

Локальные баны в сообществах. Чтобы избежать блокировки в популярных группых, читайте правила сообщества в описаниях группы или прикреплённых постах. Еще полезно почитывать группу, посвящённую безопасности во «ВКонтакте».

Facebook

В отношении своих пользователей Facebook придерживается политики «как бы чего не вышло». Любые сомнения в нарушении правил сайта обычно

трактуются не в пользу пользователя. При этом Facebook не щадит никого, даже звёзд шоу-бизнеса, а целые страны в ответ не щадят Facebook.

Использование вымышленных имени и фамилии. Facebook требует указывать только настоящие персональные данные. При этом социальная сеть порой довольно свободно обходится с этим правилом (администрация удалила аккаунт однофамильца М. Цукерберга).

Впрочем, в последнем обновлении правил появились некоторые послабления – пользователям разрешили самим указывать имена, к которым они привыкли. Так, Джеки Чан может остаться Чаном, а не перерегистрироваться как Чэн Лунь.

Дети. Социальной сетью нельзя пользоваться лицам младше 13 лет.

Судимые. Facebook запрещает регистрироваться людям, которых судили по сексуальным статьям: насильникам, совращателям, педофилам.

Сексуальный подтекст. Иногда социальная сеть находит извращёнными невинные фотографии детей или банит за откровенную картину XIX в. Запрещены открытые ягодицы и грудь, но кормить ей можно, как и в Instagram.

Спам. Нежелательная реклама может стоить не только аккаунта в социальной сети, но и штрафа почти в миллиард долларов США. Facebook запрещает использовать ботов и любые способы накрутки друзей и подписчиков.

Копирайт. Facebook запрещает публиковать любые материалы, запрещённые авторским правом.

URL и юзерпик. Отдельные требования – в адресе страницы и содержимом аватарки. В URL не должно содержаться оскорблений, а на фотографии пользователя – призыва к незаконному действию.

Кроме прочего, у Facebook есть требования к проведению акций, розыгрышей и викторин. Их нельзя проводить на личной или публичной странице, призывы «ставьте лайк и расшарьте пост» запрещены – всё должно делаться в отдельном приложении.

Twitter

У Twitter есть довольно понятные и грамотно написанные правила использования: с предупреждениями, разъяснениями, всё как полагается.

Имперсонация. Twitter не любит аккаунты, которые подражают другим людям или компаниям. Социальная сеть требует отдельно указывать, что такой аккаунт не является официальным или служит пародией. Сеть также может забрать у пользователя аккаунт @vladimirputin и вручить его Владимиру Путину.

Торговля аккаунтами и подделка верификации. Twitter запрещает покупать и продавать аккаунты, а также использовать в описании или на аватарках значки верификации. За подобное нарушение – бан.

Слишком активное использование. Социальная сеть не любит, когда люди действуют подобно ботам: фолловят людей списком, бесконечно постят один и тот же твит или одну и ту же ссылку. Также не рекомендуется постить

одни ссылки, без описаний. За превышение лимита сообщений в час Twitter может на время ограничить возможность публиковать новые твиты.

Pinterest

Правила Pinterest адаптированы под социальную сеть для картинок. Кроме этого, у них есть одно основное и самое страшное отличие – Pinterest банит навечно, без права помилования.

Автоматизация. В Pinterest запрещено использовать чужеродные автоматические инструменты для пользования соцсетью. Пинить, репинить, комментировать, загружать картинки из «Пинтереста» можно только лично. Но даже если вы вручную зальёте множество картинок с одного URL, социальная сеть попросит вас подтвердить, что вы не бот.

Копирайт. Нелья загружать изображения под авторским правом, порнографические изображения. Кроме того, не стоит загружать эротические картинки в открытые разделы сайта.

Замена источника. У каждой картинки в соцсети есть URL страницы, с которой она была взята. Если отредактировать пин и заменить этот адрес на нужный себе, то за такое хулиганство последует бан ***(За что социальные сети наказывают своих пользователей // InternetUA (http://internetua.com/za-csto-socialnie-seti-nakazivauat-svoih-polzovatelei). – 2015. – 25.03).***

***

Правительство Южной Кореи одобрило использование приложений для мобильных телефонов, разработанных чтобы предупреждать родителей о том, что их ребёнок, возможно, собирается покончить с собой.

Приложения анализируют содержание сообщений, оставляемых подростками в соцсетях, и проверяют их на наличие слов, способных указывать на суицидальные настроения автора.

Если механизм срабатывает, на смартфон родителей подростка приходит тревожное уведомление.

В Южной Корее очень высокий уровень подростковых самоубийств, который нередко связывают со стрессом из-за завышенных, по мнению многих, требований в школе.

Только в прошлом году с собой покончили 118 юношей и девушек школьного возраста ***(Телефон в Южной Корее предупредит о суицидальных мыслях // InternetUA (http://internetua.com/telefon-v-uajnoi-koree-predupredit-o-suicidalnih-mislyah). – 2015. – 15.03).***

***

Більшість американців знає, що Агентство національної безпеки та Федеральне бюро розслідувань читають їхню електронну пошту, підслуховують телефонні дзвінки і відстежують їхню активність у мережі. Разом з тим не намагаються протидіяти цьому.

Про це свідчать результати опитування The Pew Research Center, пише The Huffington Post.

Майже 9 з 10 респондентів заявили: вони «щось» чули про стеження, яке здійснюють державні органи. 56 % сказали, що вони про це чули «трохи». 31 % респондентів відповів, що чув про це «чимало».

Тільки 17 % опитаних повідомили, що стеження їх «дуже турбує». 35 % – що це їх «дещо турбує». 33 % респондентів це турбує «не вельми». 13 % респондентів це не турбує «зовсім».

82 % опитаних вважають «прийнятним» те, що уряд веде моніторинг спілкування осіб, підозрюваних у терористичній діяльності.

Водночас тільки 40 % респондентів вважають «прийнятним» моніторинг за спілкуванням американських громадян.

57 % опитаних сприймають це як «неприпустиме».

Дослідний центр також окремо поцікавився у 87 % респондентів, які сказали, що їм відомо про державне стеження: чи змінилося у них ставлення до недоторканності їхнього приватного життя. Тільки 34 % з них сказали, що вони вжили заходів для протидії його порушенню.

Згідно з результатами опитування, 25 % американців, обізнаних з програмами стеження, використовують складні паролі.

На запитання, чи користувалися вони конкретними інструментами, щоб протидіяти стеженню, респонденти як правило давали негативну відповідь.

53 % сказали, що вони не використовують безпечніший пошуковий механізм і не розглядають такої можливості.

46 % опитаних не шифрували електронну пошту. 40 % не розглядали можливості використання анонімного програмного забезпечення – наприклад Tor. 39 % навіть не чули про нього.

Дані The Pew Research Center дають відповідь на запитання, чому так мало користувачів мережі вживають заходів, щоб захистити себе. Виявляється, передусім тому, що їх не обходить, чи стежать за ними.

Ще одна причина у тому, що вони самі наражаються на вразливість з остраху перед використанням анонімного інструментарію. 54 % опитаних думають, що знайти способи захисту приватного життя важко.

У рамках дослідження The Pew Research Center з листопада до січня 2014 р. було опитано 475 дорослих американців ***(Американці не переймаються стеженням з боку спецслужб – дослідження // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/amerikantsi_ne_pereymayutsya_stezhennyam_z_boku_spetssluzhb_doslidzhennya/). – 2015. – 17.03).***

***

Соціальна мережа Facebook у другій половині 2014 р. заблокувала 55 російських акаунтів на прохання російської служби з нагляду у сфері зв’язку, інформаційних технологій і масових комунікацій. Про це повідомляє bbc.co.uk, пише МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42801/118/lang,ru/).

Згідно зі звітом Facebook, був заборонений доступ до матеріалів щодо пропаганди наркотиків і самогубств, екстремістської діяльності, закликів до масових безладів.

Компанія повідомляє, що відхилила два запити, пов'язані з розкриттям інформації за порушеними в Росії кримінальними справами ***(Facebook блокував півсотні сторінок через Роскомнагляд // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42801/118/lang,ru/). – 2015. – 18.03).***

***

Колишні й нинішні співробітники «Лабораторії Касперського» співпрацюють з російськими спецслужбами, деякі працівники компанії допомагають ФСБ у розслідуванні кримінальних злочинів, використовуючи інформацію про клієнтів.

Про це повідомляє «Дождь» із посиланням на Bloomberg.

Агентство повідомляє, що засновник і керівник компанії Є. Касперський сам працював у ФСБ. У 2012 р., за даними Bloomberg, з компанії пішли високопоставлені менеджери, замість них прийшли люди, у яких були тісні зв'язки з російськими військовими або розвідувальними структурами.

Деякі з них тісно співпрацювали з ФСБ і допомагали відомству розкривати кримінальні справи, використовуючи при цьому базу, у якій були дані про 400 млн клієнтів компанії.

Є. Касперський, передає Bloomberg, щотижня ходить у лазню в групі з п'яти-десяти осіб. Серед них часто виявляються співробітники російських спецслужб. Сам він в інтерв'ю агентству розповів, що похід у лазню має виключно соціальний характер. За його словами, це допомагає співробітникам «подружитися».

І. Чекунов, заступник компанії з юридичних питань, який часто, за даними Bloomberg, ходить у лазню з Є. Касперським, і є ключовою особою по взаємодії з російським урядом. З 2013 р. він нібито керує групою з 10 осіб, які надають інформацію ФСБ і іншим російським держструктурам.

Є. Касперський розповів агентству, що представники держструктур не можуть прив'язати зібрану інформацію до окремих клієнтів.

«Я не та людина, з якою можна поговорити про російські реалії, тому що я живу в кіберпросторі», – додав він ***(Bloomberg: «Лабораторія Касперського» співпрацює з ФСБ // Espreso.tv (http://espreso.tv/news/2015/03/20/bloomberg_quotlaboratoriya_kasperskohoquot_spivpracuuye_z_fsb). – 2015. – 20.03).***

***

Генпрокуратура России требует заблокировать сообщества в соцсетях некоторых организаций, которые, по мнению российской стороны, используются для информационно-пропагандистской деятельности.

«Генеральная прокуратура направила в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) предписание о блокировке интернет-ресурсов, которые пропагандируют деятельность украинских экстремистов «Правого сектора», «Украинской национальной ассамблеи – Украинской народной самообороны» (УНА-УНСО), «Тризуба имени Степана Бандеры», «Братства», – пишет российское издание «Известия».

Всего Генпрокуратура РФ направила список из 19 ресурсов – часть из них тематические группы в соцсетях «ВКонтакте» и Facebook, другая – крупные интернет-сайты.

«Интернет-сайты, которые являются официальными ресурсами вышеуказанных организаций, на них, по данным Генпрокуратуры, содержатся сведения о результатах деструктивной деятельности националистических группировок, пропагандируется идеология известных террористов, нацистов и их пособников, формируются антироссийские установки, а также распространяются призывы к осуществлению насильственных действий по политическим, расовым, национальным и религиозным мотивам», – уточняется в сообщении.

Требование по блокировке ресурсов украинских организаций с подписью заместителя генпрокурора РФ В. Гриня было передано в Роскомнадзор.

Стоит отметить, что в Роскомнадзоре подтверждают данную информацию и уверяют, что работа по блокировке ресурсов уже ведется ***(Роскомнадзор зачистит «ВКонтакте» и Facebook от «Правого сектора» // Независимое Бюро Новостей (http://nbnews.com.ua/ru/news/145824/). – 2015. – 19.03).***

***

Twitter озаботился улучшением безопасности своих пользователей. Из-за того, что сервис позволяет вести анонимные блоги, некоторые люди сталкиваются с тем, что соцсеть используют для угроз. Новая функция позволит быстро уведомить о таких происшествиях полицию.

Ранее компания позволяла только пожаловаться в администрацию соцсети и добавить аккаунт агрессора в черный список. Теперь же появилась новая кнопка email report. После того, как пользователь нажмет на нее, Twitter отправит на электронную почту человека подробный отчет о происшествии, в котором будет присутствовать перепечатка твита, ссылка на него, имя пользователя, ссылка на аккаунт обидчика и другая информация.

Также Twitter пояснит, как правильно оформить и переправить эти данные в виде заявления в полицию. «Мы надеемся, что предоставление подобного саммари сделает процесс более простым для вас», – отмечают в Twitter. В русскоязычном сегменте социальной сети новая функция пока что не появилась. Пользователям по-прежнему предлагается только внести пользователя в черный список ***(Twitter поможет сдать обидчиков полиции //***

InternetUA (http://internetua.com/Twitter-pomojet-sdat-obidcsikov-policii). – 2015. – 20.03).

***

Українські волонтери запустили сервіс для відслідковування інтернет-тролів та протидії антиукраїнській пропаганді TrolleyBust.com.

Як повідомляють засновники ресурсу, одне з його головних завдань – блокування джерел антиукраїнської пропаганди в соцмережах, а основний метод – відправлення скарг на конкретних користувачів та їхні повідомлення.

TrolleyBust дає змогу знайти значну кількість коментарів найбільш активних користувачів соцмереж. На момент запуску в базі було понад 30 млн коментарів та 6 млн користувачів.

Окрім базових аналітичних інструментів (інформація по користувача, список друзів), сервіс надає функції, недоступні в соцмережах: вибір коментарів конкретного користувача, пошук за його повідомленнями.

Таким чином відбувається виявлення акаунтів інтернет-тролів та ботів, які не публікують власних повідомлень, але активно коментують чужі.

Уже зараз волонтери TrolleyBust заблокували сотні джерел пропаганди та акаунтів сепаратистів. Головним завданням на сьогодні засновники вважають об'єднання зусиль з іншими волонтерами, щоб масово блокувати знайдені профілі тролів, яких налічується десятки тисяч.

«В антиукраїнську пропаганду вкладаються значні кошти, тому для боротьби з нею важливо використовувати ефективні інструменти. Наочним прикладом тут може бути боротьба із так званими фейками, – розповідає координатор проекту О. Шевчук. – Якщо саме створення фейкового акаунту автоматизоване і коштує дешево, то його наповнення і розкрутка обходяться значно дорожче і займають багато часу».

За словами координатора проекту, волонтери відстежують такі акаунти, а потім скаржаться на них до соцмережі. О. Шевчук переконаний, що такі «партизанські методи» ефективні.

Нагадаємо, раніше волонтери створили «Українські кібервійська», які передали Службі безпеки України дані 1025 проросійських бойовиків, виклали у відкритий доступ документи російського Міністерства внутрішніх справ, а також домоглися блокування веб-сайтів та банківських рахунків багатьох сепаратистів ***(В Україні з'явився сервіс для відстежування інтернет-тролів // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/online_media/v_ukraini_zyavivsya_servis_dlya_vidstezhuvannya_internettroliv/). – 2015. – 24.03).***

***

Как пишет издание «Крым.Реалии», до 1 апреля оккупационные власти Крыма планируют закончить выявление и блокирование интернет-сайтов, которые содержат «террористические и экстремистские материалы», а также подобрать специалистов для «адресного профилактического воздействия» на

несогласных. К этому же сроку должна быть завершена разработка методических рекомендаций о порядке действий органов государственной власти так называемой «Республики Крым», физических и юридических лиц по документированию фактов «распространения деструктивных идей и идеологии терроризма» в Интернете и по их передаче в правоохранительные органы.

Согласно плану квалифицированные специалисты (коллективы) должны будут осуществлять «адресный профилактическое воздействие на лиц, наиболее подверженных или таких, которые уже попали под влияние идеологии терроризма».

Кроме того, «глава» оккупационной власти Крыма С. Аксенов заявляет, что «в полувоенный время» работа таких телеканалов как крымскотатарский канал ATR недопустима. Напомним, что Крымскотатарский телеканал ATR и все остальные медиа, входящие этот в медиа-холдинг, не смогли получить от оккупационной крымской власти свидетельства о регистрации средств массовой информации по российскому законодательству, что грозит прекращением их работы в Крыму.

Компания уже несколько раз подавала документы в профильные ведомства Российской Федерации, но их каждый раз возвращали назад. В итоге, телеканал может прекратить вещание 1 апреля. Под угрозой закрытия находятся и детский телеканал «Ляле», радио «Мейдан» и «Лидер», а также новостной сайт «15 минут» ***(В Крыму ужесточат цензуру в Интернете и на телевидении // «Kherson.in» (http://kherson.in/news/v_krymu_uzhestochat_tsenzuru_v_internete_i_na_televidenii). – 2015. – 23.03).***

***

Одна из высокопоставленных военных организаций Китая впервые официально признала, что в составе вооруженных сил страны и разведслужб числятся спецотряды, основной целью которых является осуществление подрывной деятельности в компьютерных сетях, сообщает издание The Daily Beast.

О хакерской деятельности Китая, в частности, направленной на похищение секретов производства американских компаний, было известно достаточно давно. Это стало источником постоянного напряжения между Вашингтоном и Пекином, хотя китайские власти и отрицали свою причастность к шпионажу за корпорациями США или осуществлению кибератак с целью повреждения критической инфраструктуры страны (сетей электропередач, газопроводов и т. д.).

Теперь Поднебесная, судя по всему, прекратила играть в шарады. По словам специалиста Центра исследований и анализа в области разведки (Center for Intelligence Research and Analysis, CIRA) Д. МакРейнолдса, впервые за все время Китай признал существование тайных кибервоенных сил.

Подтверждение проведения кибероперацій содержится в последнем издании документа «Наука военной стратегии», опубликованного научно-исследовательским институтом Народно-освободительной армии Китая.

Как отметил Д. МакРейнольдс, труд выходит «раз в поколение» и является одним из самых лучших способов ознакомления с китайской военной стратегией. По словам специалиста, Китай разделил свои кибервойска на три типа. Первый из них – «специальные военизированные компьютерные войска» – состоит из оперативных военных отделов, основная задача которых – осуществление и защита от кибератак.

Второй тип – гражданские специалисты с правом выполнения «сетевых боевых действий». И, наконец, третий тип – не относящиеся к правительству «внешние элементы», которые могут быть мобилизованы для выполнения вредительских действий в сетях.

Сейчас, когда Китай раскрывает подробности о своих кибервойсках, правительства других стран теряют уверенность в том, что смогут плодотворно и безопасно сотрудничать с Поднебесной в сфере борьбы с киберпреступлениями.

К примеру, за последнее десятилетие Министерство общественной безопасности Китая оказало помощь более 50 странам в расследовании тысяч инцидентов. Кроме того, Китай заключил двусторонние соглашения о сотрудничестве с более чем 30 государствами, в том числе США, Великобританией, Германией и Россией. Теперь эти страны будут тщательно взвешивать все риски, прежде чем обращаться за помощью в Министерство общественной безопасности, отмечает МакРейнольдс ***(Китай раскрыл подробности о своих кибервойсках // Центр Інформаційної Безпеки (http://www.bezpeka.com/ru/news/2015/03/20/china-reveals-its-cyber-war-secrets.html). – 2015. – 20.03).***

Проблема захисту даних. DDOS та вірусні атаки

Эксперты предупреждают о появлении принципиально новой угрозы – зараженных вредоносным ПО USB-накопителей, способных провоцировать скачки напряжения в электронике компьютеров старого образца. По данным независимого исследователя Dark_Purple, впервые идея о носителе информации была озвучена его знакомыми в ходе переписки в Skype.

«Как-то читал статью, как парень в метро вытянул другого парня из сетчастого кармана сумки флешку, на которой 128 было написано. Пришел домой, вставил в ноут, спалил пол компа… Написал на флешке 129 и теперь носит в наружном кармане своей сумки», – цитирует специалист и отмечает, что решил создать прототип такого устройства, поскольку он работает в компании, специализирующейся на разработке и производстве электроники.

Dark_Purple также пояснил, что в современных компьютерах USB «встроен чуть ли не в сам процессор», однако в более старых системах за этот

же функционал «отвечают североюжные мосты». При этом задача упомянутого USB-накопителя – сжечь хотя бы порт, к которому он подключается.

Выделить область практического применения подобной технологии специалист затруднился и отметил, что она схожа с атомной бомбой: «Круто иметь, только применить нельзя».

Принцип работы устройства исследователь пояснил следующим образом: «При подключении к USB-порту запускается инвертирующий DC/DC преобразователь и заряжает конденсаторы до напряжения -110 В, при достижении этого напряжения DC/DC отключается и одновременно открывается полевой транзистор через который -110 В прикладываются к сигнальным линиям USB интерфейса».

Когда напряжение опускается до -7 В, транзистор закрывается, запускается DC/DC и весь процесс повторяется циклически до достижения нужного эффекта ***(Инфицированные USB-накопители могут сжечь компьютер, провоцируя скачок напряжения // InternetUA (http://internetua.com/inficirovannie-USB-nakopiteli-mogut-sjecs-kompuater--provociruya-skacsek-napryajeniya). – 2015. – 15.03).***

***

Удручающие результаты показал анализ содержимого магазинов приложений для Apple и Android, проведенный специалистами Veracode. Было найдено до 14 тыс. сомнительных программ.

Экспертами американской компании было протестировано около 400 тыс. различных приложений, наиболее часто используемых сотрудниками ведущих финансовых, медийных и прочих корпораций. Оказалось, что бреши в безопасности имеют до 3 % всех проверенных приложений.

Так, 85 % проблемного ПО, по мнению исследователей, не сохраняют должным образом важную персональную информацию SIM карты пользователя. При их использовании под угрозой находятся данные о местоположении владельца, история звонков, контакты, логи SMS, а также ID устройства.

37 % из 14 тыс. попавших под подозрение приложений замечены в выполнении подозрительных действий. Например, они запрашивают права администратора, что в дальнейшем дает им возможность отключать программы безопасности, прослушивать разговоры абонента, устанавливать посторонние приложения. Они также способны определить джейлбрейк или оригинальная операционная система установлены на устройстве. Наиболее опасен доступ таких приложений к данным кэша, куда иногда попадают и важные пароли.

35 % признанных сомнительными приложений ориентированы на сбор и пересылку конфиденциальных данных пользователя – календарного расписания, истории браузера, путешествий. Подобного рода информация используется злоумышленниками для составления социального портрета личности с целью выявить деловые связи человека или найти на него компромат.

«Многие из мобильных приложений признаны опасными поскольку их создатели неосознанно используют некачественные библиотеки и фреймворки. Другой тип сомнительных программ целенаправленно создан для шпионажа за пользователями», – заявил технический директор Veracode К. Висопал.

По завершению исследования представители Veracode уведомили о его результатах ответственных лиц в Apple и Google. Типичным примером опасного ПО выступает, по мнению экспертов компании, программа для прослушивания аудиокниг Lazy Listen. Приложение, скаченное уже полмиллиона раз, запрашивает доступ к широкому спектру информации. Сами создатели программы объясняют это необходимостью улучшения качества обслуживания пользователей ***(Тысячи мобильных приложений шпионят за пользователями // InternetUA (http://internetua.com/tisyacsi-mobilnih-prilojenii-shpionyat-za-polzovatelyami). – 2015. – 16.03).***

***

DDoS-атака на онлайн-ресурс компании влечет за собой убытки в среднем размере от 52 до 444 тыс. дол. в зависимости от размера компании – такие данные получены в ходе исследования, проведенного Kaspersky Lab и B2B International.

К расходам по устранению последствий подобных атак добавляются также репутационные потери и издержки, вызванные недоступностью публичного онлайн-ресурса для партнеров и клиентов.

Рассчитанная экспертами сумма убытков включает в себя несколько статей. Согласно исследованию, 61 % пострадавших компаний временно теряли доступ к критичной для бизнеса информации из-за DDoS-атаки, 38 % не имели возможности осуществлять свою основную деятельность, а 33 % сообщили об упущенных бизнес-возможностях и контрактах. Кроме того, в 29 % случаев успешные атаки негативно сказались на кредитном рейтинге, а у 26 % компаний возросли страховые взносы.

Также в среднюю сумму ущерба от DDoS-атаки вошли расходы на устранение последствий инцидента. Например, 65 % компаний были вынуждены воспользоваться услугами консультантов по информационной безопасности, 49 % оплачивали работы по изменению собственной IT-инфраструктуры, 46 % обращались к юристам, а 41 % – к консультантам по риск-менеджменту. И это только самые распространенные статьи расходов.

«Успешная DDoS-атака может вывести из строя критически важные для бизнеса сервисы, что влечет за собой серьезные последствия для компании. Например, мы фиксируем случаи, когда атаки на банки приводили не только к нарушению работы онлайн-сервисов в течение нескольких дней, но и к перебоям в обслуживании банковских карт и нарушению работы банкоматов. Поэтому сегодня нужно рассматривать защиту от DDoS как неотъемлемый элемент общей информационной безопасности компании наравне с защитой от вредоносных программ, целевых атак и кражи данных», – считает А. Киселев, менеджер направления Kaspersky DDoS Prevention Kaspersky Lab.

Технологии Kaspersky Lab позволяют обеспечить непрерывность доступа к онлайн-ресурсам клиента даже во время сложных, длительных и ранее неизвестных типов DDoS-атак. Сервис Kaspersky DDoS Prevention осуществляет защиту за счет переключения на время атаки клиентского трафика на центры очистки данных. Центры расположены во многих странах и подключены к Сети по высокоскоростным каналам связи. При выявлении факта DDoS-атаки вредоносный трафик отфильтровывается, и до клиента доходят только запросы легитимных пользователей, что спасает инфраструктуру и сервисы от перегрузки. Этот подход позволяет выдержать DDoS-атаку практически любой мощности, а также избежать перегрузки онлайн-сервиса клиента ***(Kaspersky Lab оценивает, во сколько обходится устранение последствий DDoS-атак // ITnews (http://itnews.com.ua/news/76356-kaspersky-lab-otsenivaet-vo-skolko-obkhoditsya-ustranenie-posledstvij-ddos-atak). – 2015. – 16.03).***

***

Как известно, новая ОС Android 5.1 Lollipop вышла буквально на днях.

Тем не менее, эксперты уже успели обнаружить в ней немалое количество недоработок, ключевой из которых является большая утечка памяти в фоновом режиме.

Как следствие, она вызывает ошибки в приложениях, проблемы с лаунчером платформы и даже зависание всей системы. К слову, в свое время подобная проблема наблюдалась также и в Android 5.0.

Со стороны Google уже последовало заявление о том, что инженеры компании начали работу над специальным патчем, который должен «закрыть» эту брешь. О дате выхода в точности не известно, но оговорено, что это должно случиться «в ближайшее время» ***(В новой ОС Android 5.0.1 Lollipop обнаружена серьезная уязвимость // ITnews (http://itnews.com.ua/news/76373-v-novoj-os-android-501-lollipop-obnaruzhena-sereznaya-uyazvimost). – 2015. – 17.03).***

***

Британская компания MDSec, специализирующаяся на безопасности, в своем блоге рассказала о так называемом «черном ящике», с помощью которого можно взломать пароль от любого iPhone и iPad.

Устройство называется IP Box и действует только на четырехзначные пароли, но это вряд ли станет большой проблемой для злоумышленников, учитывая, что большинство пользователей пользуется именно такими паролями.

Принцип работы устройства, по сути, заключается в простом подборе чисел от 0000 до 9999. Для взлома требуется лишь подключить iPhone или iPad к «ящику» и вы получите пароль от 6 секунд до 17 часов.

Что интересно, подобная функциональность может быть доступна абсолютно каждому. Стоимость IP Box составляет всего 200 фунтов стерлингов, и и его совершенно спокойно можно найти в свободной продаже.

Защитить себя от такого взлома пока можно лишь одним способом – поставить более длинный пароль, что специалисты MDSec и рекомендуют сделать ***(Черный ящик, который сможет взломать пароль любого iPhone за 6 секунд // InternetUA (http://internetua.com/cernii-yasxik--kotorii-smojet-vzlomat-parol-luabogo-iPhone-za-6-sekund). – 2015. – 18.03).***

***

BlackBerry пополнила перечень компаний, чьи продукты затрагивает уязвимость FREAK. Согласно уведомлению, компания работает над исправлениями, которые будут выпущены уже в ближайшее время.

«BlackBerry усердно работает над изучением уязвимости и определением наилучших способов уменьшения риска для пользователей. Исследования пока продолжаются, однако мы можем подтвердить, что продукты BlackBerry содержат эту уязвимость», – говорится в сообщении компании.

Уязвимыми являются смартфоны BlackBerry, а также все версии ОС BlackBerry 10, BlackBerry 7.1 и ниже, все версии клиентов BES12 (в том числе для iOS) и BES10, все Android-версии Secure Work Space и Work Space Manager для BES10/BES12, все iOS-версии Work Browser и Work Connect для BES10/BES12, все версии BlackBerry Blend для BlackBerry 10, Android, iOS, Windows и Mac OS X, BlackBerry Link для Windows и Mac OS X и пр.

Брешь не затрагивает все версии BES5, BlackBerry Universal Device Service, все версии клиента BES12 для Windows Phone и Android, BBM и BBM Protected для Android 2.7.0.6 и выше, а также для iOS 2.7.0.32 и выше.

Напомним, что обнаруженная в начале текущего месяца уязвимость в OpenSSL и Apple SecureTransport позволяет злоумышленнику расшифровать файлы cookie и другую важную информацию, полученную через соединение HTTPS ***(BlackBerry исправит уязвимость FREAK в своих продуктах // InternetUA (http://internetua.com/BlackBerry-ispravit-uyazvimost-FREAK-v-svoih-produktah). – 2015. – 18.03).***

***

Специалисты ИБ-компании «Доктор Веб» обнаружили новый Android-троян, который по команде злоумышленников способен похищать конфиденциальные данные пользователей, отправлять sms-сообщения, совершать звонки и выполнять другие опасные действия. Вредонос, получивший название Android.Titan.1 (по классификации «Доктор Веб»), нацелен на южнокорейских пользователей и распространяется посредством рассылки нежелательных sms-сообщений.

В тексте уведомления, в котором говорится о задержке доставки некоего извещения, размещена ссылка, по которой жертве предлагается перейти для ознакомления с информацией. На самом деле ссылка ведет на один из облачных

веб-сайтов, на котором содержится троян. При посещении ресурса на устройство пользователя автоматически загрузится apk-файл вредоносной программы. Тем не менее, для того чтобы троян инфицировал систему, жертва должна сама осуществить его установку.

По словам специалистов, главная особенность вредоноса заключается в том, что его основной функционал реализован в виде отдельной Unix-библиотеки, тогда как в большинстве известных Android-троянов он, как правило, находится в стандартном исполняемом dex-файле. В данном случае dex-файл используется в качестве вспомогательного компонента, который выполняет несколько незначительных функций. Такой прием встречается достаточно редко, поэтому многие антивирусные инструменты зачастую не могут обнаружить вредоносную программу.

Предположительно, троян все еще находится на стадии разработки поскольку специалисты «Доктор Веб» отмечают наличие в нем ошибок и незадействованного функционала. По их мнению, не исключено, что в будущем может появиться более совершенная версия данного вредоноса ***(Эксперты обнаружили новый Android-троян, который «прячется» от антивирусов // InternetUA (http://internetua.com/eksperti-obnarujili-novii-Android-troyan--kotorii--pryacsetsya--ot-antivirusov). – 2015. – 19.03).***

***

D-Link вновь выпустила пакет обновлений для различных моделей своих маршрутизаторов, большей частью состоящих из исправлений безопасности. Вместе с тем, как отмечают независимые аналитики, большая часть владельцев маршрутизаторов игнорирует выпуск новых версий прошивки, в результате чего уязвимости в них остаются доступными для эксплуатации злоумышленниками.

Как следует из уведомления CERT, обновления затрагивают также и сетевые камеры серии DCS-93 (модели 930L, 931L, 932L и 933L с заводской прошивкой версии 1.04). Обнаруженные в них уязвимости позволяют удаленно выполнить произвольный код, а также загружать произвольные файлы в произвольные директории атакуемой системы.

Исследователи из Tangible Security также отмечают, что брешь существует из-за ошибки в механизме установки обновлений. Проблема актуальна для всех версий прошивки до 1.21b05.

Стоит отметить, что наличие множества критических уязвимостей характерно не только для D-Link, но и для большинства производителей устройств такого класса ***(D-Link устранила очередную порцию уязвимостей в своих маршрутизаторах // InternetUA (http://internetua.com/D-Link-ustranila-ocserednuua-porciua-uyazvimostei-v-svoih-marshrutizatorah). – 2015. – 19.03).***

***

В сети наблюдается рост числа фишинговых атак, использующих в качестве приманки «умные» часы Apple Watch. Об этом рассказали MacDigger специалисты антивирусной компании ESET.

Apple Watch были анонсированы в сентябре 2014 г., а официальный старт продаж запланирован на 24 апреля 2015 г. Пока аналитики спорят о перспективах первого носимого гаджета Apple, злоумышленники используют ажиотаж вокруг новинки в своих целях.

Эксперты обнаружили в социальных сетях множество спамерских сообщений, приглашающих принять участие в розыгрыше Apple Watch. Механика «розыгрыша» типична для фишинговых кампаний: перейти по ссылке на сторонний сайт, ответить на вопросы анкеты, поделиться ссылкой с друзьями и подписчиками.

Например, для одного из «розыгрышей» на Facebook была создана страница мероприятия. Участникам предлагалось оставить свои контактные данные и имя пользователя, а затем пригласить друзей присоединиться к мероприятию. Мошенники обещали вручить модель Apple Watch (от 549 дол.) за 100 принятых приглашений, Apple Watch Sport (от 349 дол.) – за 250 приведенных участников и премиальные Apple Watch edition (от 10 000 дол.) – за 500 новых жертв.

Еще в одной мошеннической схеме, замеченной специалистами ESET, потенциальная жертва переходила по ссылкам на сторонние площадки, также созданные для кражи персональных данных, паролей и логинов.

Спам про «Apple Watch в подарок» распространялся и в Twitter. В частности, ссылки на «розыгрыш» появлялись в твитах фальшивого аккаунта Apple Giveaways.

В ESET рекомендуют не участвовать в распространении сомнительных ссылок и не оставлять персональные данные на подозрительных площадках ***(Мошенники в сети освоили новую схему обмана // InternetUA (http://internetua.com/moshenniki-v-seti-osvoili-novuua-shemu-obmana). – 2015. – 19.03).***

***

Facebook предлагает новую функцию, посвященную безопасности пользователей. Теперь люди смогут заходить на сторонние приложения через сеть, при этом не предоставляя никаких личных данных.

Систему могут протестировать любые разработчики: Facebook приглашает всех желающих подать заявку на участие в новом проекте. Суть в том, что пользователи смогут заходить в приложения через «Анонимный вход». Человек использует специальный анонимный логин, который никак не отражает его реальных данных. А пользоваться функциями будет полноценно, как и раньше, с помощью сети.

При этом стала доступной еще одна опция: функция ограничения данных. Пользователь, входя на любой сайт, может указать, какие поля оставить публичными, а какие – скрыть от всех.

«Мы беспокоимся о безопасности людей, предпочитающих Facebook. В настоящее время, когда появилось много мошенников и вредоносных приложений, мы решили поработать над созданием большей анонимности. Теперь пользователи смогут заходить на сайты и приложения, не боясь, что кто-то получит их личные данные – это попросту невозможно при использовании “анонимного входа”», – отметили в пресс-службе сети.

При этом Facebook все равно не останется без информации. На серверах будут храниться и анонимные логины, и сведения о сайтах, которые пользователи посещали. Впрочем, представители сети заверили, что эти данные использоваться не будут ***(Анонимный вход для пользователей Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/anonimnyy_vhod_dlya_polzovateley_facebook). – 2015. – 18.03).***

***

Как только вы думаете, что знаете как обезопасить свои финансы и личные данные, и откуда ждать угрозу, мошенники придумывают все новые и новые способы получения доступа к вашей кредитной карте. На этот раз скимминговые устройства были обнаружены внутри дверного устройства, которое считывает данные карты, прежде чем запустить клиента в вестибюль к банкомату.

Как сообщает известный эксперт в сфере безопасности Б. Кребс, мошенники прячут считывающие устройства внутри замка, а также устанавливают скрытую камеру возле банкомата. Таким образом, все данные по карте перехватывает скимминговое устройство при входе клиента в помещение, а камера записывает соответствующий PIN-код, когда клиент вводит его в банкомате.

Как пишет Б. Кребс, замок, открыть который можно с помощью карты, не является слишком «умным» устройством. Поэтому чтобы обезопасить себя, эксперт советует открывать такие помещения с банкоматом с помощью любой другой ID-карты. А мы советуем всегда помнить и придерживаться основных правил защиты от мошенничества в банкомате ***(Мошенники придумали новый способ получения доступа к кредитной карте // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/20/skimmers-invented-new-way-of-grabbing-credit-card-data.html). – 2015. – 20.03).***

***

Подключение автоматической синхронизации фотографий с альбомами Facebook на iOS- и Android-устройствах позволяет злоумышленникам украсть личные фотографии пользователя.

Охотник за уязвимостями Л. Матия обнаружил серьезные бреши в функции синхронизации Facebook, а также в мобильном приложении социальной сети. Уязвимости позволяют любому стороннему приложению получить доступ к скрытому альбому.

В 2012 г. Facebook представил функцию Facebook Photo Sync для iPhone, iPad и устройств на базе Android, которая позволяет автоматически синхронизировать все фото на смартфоне с учетной записью в Facebook.

Фото, которые пользователь синхронизирует со смартфона, загружаются в фоновом режиме в альбом соцсети, который недоступен для просмотра друзьям и другим пользователям. Тем не менее, позже пользователь может поделиться выбранными фото в ленте новостей или отправить их, как вложение к сообщению.

Специалист по безопасности сказал, что уязвимость напомнила ему инцидент с украденными фотографиями знаменитостей, что было возможно из-за бреши в защите облачного сервиса iCloud.

В публикации блога Л. Матия объяснил, что уязвимость находится в механизме привилегий, недоработанность которого позволяет сторонним приложениям получить права доступа к альбому с фото при помощи интерфейса vaultimages API.

Технически, фотоальбом, в котором сохраняются фото после синхронизации, должен быть доступным только приложению Facebook, но уязвимость позволяет сторонним программам получить разрешение на чтение синхронизированных фотографий ***(Уязвимость в Facebook позволяет злоумышленникам получить фото пользователей // InternetUA (http://internetua.com/uyazvimost-v-Facebook-pozvolyaet-zloumishlennikam-polucsit-foto-polzovatelei). – 2015. – 20.03).***

***

Двадцать восемь стран ЕС прошли проверку на готовность к кибератакам

Как сообщают исследователи безопасности из международной организации Business Software Alliance (BSA), по итогам внеочередной проверки, проведенной в 28 странах Евросоюза, наибольшая степень готовности к хакерским нападениям была зафиксирована в Эстонии, Австрии и Голландии.

По словам специалистов, отчет с подобной статистикой был опубликован впервые в мире, поскольку ранее никто не изучал каждую страну в отдельности и не составлял отдельные подробные доклады по каждой из них.

Важность отчета, по данным BSA, заключается в том, что он позволит немного лучше понимать, что именно необходимо предпринять для повышения уровня информационной безопасности на международном уровне. Кроме того, статистика позволит более четко видеть, в каком состоянии находится безопасность европейских стран в настоящее время.

Стоит отметить, что оценивание проводилось, исходя из 25 критериев, определяющих эффективность киберзащиты в масштабах отдельно взятой

страны. Как выяснилось, защищенность европейских государств сильно варьируется большей частью из-за существенных различий в законодательных актах ***(28 стран ЕС прошли проверку на готовность к кибератакам // InternetUA (http://internetua.com/28-stran-es-proshli-proverku-na-gotovnost-k-kiberatakam). – 2015. – 20.03).***

***

Компания «Доктор Веб» предупреждает о появлении опасной вредоносной программы, способной причинить немало бед неосторожным пользователям персональных компьютеров.

Троян носит обозначение Encoder.514. Он распространяется посредством массовых рассылок по электронной почте: сообщения приходят якобы от имени службы по передаче факсов через Интернет под заголовком Incoming Fax Report. В приложении к письму под видом факсимильного сообщения содержится ZIP-архив, внутри которого располагается вредоносный SCR-файл, являющийся исполняемым в операционных системах семейства Microsoft Windows.

Заражение трояном происходит при попытке открытия вложения. Вредоносная программа кодирует хранящиеся на накопителях пользовательские данные и требует выкуп за их расшифровку. Пострадавшие от действия зловреда файлы не получают отдельного расширения, но в начало их имени дописывается строка «!crypted!». Шифрование происходит с созданием промежуточных файлов, имеющих расширение *.cry, которые впоследствии удаляются.

Увы, в настоящее время расшифровка файлов, закодированных вредоносной программой, не представляется возможной ***(Опасный троян-вымогатель кодирует файлы без возможности расшифровки // InternetUA (http://internetua.com/opasnii-troyan-vimogatel-kodiruet-faili-bez-vozmojnosti-rasshifrovki). – 2015. – 22.03).***

***

Популярный плагин Google Analytics для системы управления контентом WordPress, как выяснилось, содержит критическую уязвимость, эксплуатация которой позволяет потенциальному злоумышленнику удаленно захватить контроль над учетной записью администратора и выполнить произвольный код на стороне сервера.

Обнаружить брешь удалось финскому исследователю безопасности Й. Пиннонену. По его словам, для успешной атаки пользователю не нужно проходить процесс авторизации, однако необходимо, чтобы администратор уязвимой версии программы просмотрел панель ее настроек.

Отметим, что на сегодняшний день Google Analytics для WordPress был скачан свыше семи миллионов раз и является самым популярным инструментом среди тех, которые взаимодействуют с интернет-сервисом поискового гиганта.

Й. Пиннонен также сообщил, что уязвимость существует из-за отсутствия в плагине процедуры контроля доступа, что позволяет сторонним пользователям изменять его настройки ***(Обнаружена уязвимость в плагине Google Analytics для WordPress // InternetUA (http://internetua.com/obnarujena-uyazvimost-v-plagine-Google-Analytics-dlya-WordPress). – 2015. – 22.03).***

***

DDoS-атаки, как всем известно, горячо обсуждаются в СМИ. Но DDoS – лишь одно из проявлений сложных бот-атак. СМИ часто упускают из виду бот-атаки на уровне приложений, которые могут повлиять на работу почти любого сайта. Боты способны похищать данные, взламывать учетные записи и многое другое. Они часто работают скрыто, разрушая доверие пользователей к бренду компании, оставаясь при этом незамеченными.

«Более 99 % бизнес-сайтов не являются целью массированных DDoS-атак. Однако существуют две угрозы, с которыми владельцы бизнеса сталкиваются ежедневно», – считает Р. Исэд, основатель и генеральный директор Distil Networks.

Боты, которые тайно сканируют данные

Угроза исходит от ботов, которые тайно сканируют информацию, ища способ украсть бизнес-данные, контент и интеллектуальную собственность. Этот вид атак происходит на уровне приложений. Подобные боты ищут уязвимости в приложениях, имеющих доступ к Интернету.

Боты, маскирующиеся под другие приложения

Такие боты маскируют себя под пользователя сайта или обычного интернет-робота и похищают все, что могут – от паролей и контента, до информации об уязвимостях приложений или сервера. Проникнув однажды в систему жертвы, они могут оставаться в «спящем режиме», а через какое-то время изъять ценные бизнес-данные. Они могут даже вызвать огромное количество других вредоносных ботов для усиленной атаки (то есть для воровства миллионов учетных данных пользователей) ***(Атаки ботов – реальная угроза, о которой забывают упомянуть // InternetUA (http://internetua.com/ataki-botov---realnaya-ugroza--o-kotoroi-zabivauat-upomyanut). – 2015. – 21.03).***

***

Большинство BIOS беззащитны перед хакерами

Эксперты по безопасности компании LegbaCore доказали, что на сегодняшний день миллионы некорректных версий BIOS уязвимы перед хакерскими атаками , пишет Блог Imena.UA (http://www.imena.ua/blog/talk-bios-hack/).

По данным экспертов, большинство пользователей сегодня совершенно не задумываются над обновлением BIOS, из-за чего практически в каждой базовой системе присутствует уязвимость.

Например, Исследователи с помощью LightEater-атаки легко получили GPG-ключи из памяти компьютера. Так они доказали, что LightEater может использовать технологию Intel Serial Over Lan для проникновения в базу данных режима системного управления SMM без использования конкретного драйвера NIC.

Демонстрируя результаты тестов, эксперты планируют убедить производителей и пользователей заняться более серьёзной модификацией всех версий BIOS для предотвращения возможных кибератак.

Ранее Министерство обороны США выложило в сеть программный комплекс для защиты от хакерских атак Dshell. Он уже пять лет используется Министерством обороны для анализа и исследования атак из сети. Теперь он стал доступен рядовым пользователям Интернета.

Архитектура Dshell представляет собой каркас, на базе которого любой пользователь может создавать собственные аналитические модули, используя в качестве основы атаки, с которым ему пришлось столкнуться ***(Большинство BIOS беззащитны перед хакерами // Блог Imena.UA (http://www.imena.ua/blog/talk-bios-hack/). – 2015. – 23.03).***

***

23 березня здійснено несанкціоноване проникнення на офіційний сайт Національної гвардії України з метою поширення неправдивої інформації провокаційного змісту.

Про це повідомляє прес-служба Нацгвардії.

З метою відновлення роботи офіційного веб-ресурсу на сайті vv.gov.ua проводяться технічні роботи.

Крім того, як зазначається, у соціальних мережах провокатори створили фейкові сторінки відомства, які не є офіційним джерелом.

Відтак, у Нацгвардії просять бути обачними та не користуватися такими адресами:

https://vk.com/vvmvsu,

https://vk.com/club17318385.

Також просять тимчасово не користуватися інформацією зі сторінки НГУ у Twitter

https://twitter.com/ng_ukraine

та не надсилати інформаційні запити на адресу:

vvmvsu@ukr.net.

Наразі офіційна, підтверджена та перевірена інформація розміщується лише на сторінках у соціальних мережах за посиланнями на сайті видання.

«Також у мережі Інтернет зловмисники розповсюджують неправдиву інформацію провокаційного змісту про “стягування сил Нацгвардії до Дніпропетровська”. Хоча насправді, військові частини Національної гвардії, які постійно дислоковані у Дніпропетровську, діють у штатному режимі, виконуючи покладені на них завдання. Ніяких додаткових сил до несення

служи підрозділами Національної гвардії Україні у Дніпропетровську не залучається», – ідеться в повідомленні.

Крім того, провокатори опублікували заяву нібито від імені т. в. о. командувача Національної гвардії України генерал-лейтенанта М. Балана щодо визнання ним законності анексії Криму РФ та загибелі 27 892 військовослужбовців під час АТО. Повідомляємо, що ніяких заяв генерал-лейтенант М. Балан не робив, а розповсюджена інформація не відповідає дійсності ***(Невідомі «зламали» сайт Нацгвардії і створили фейкові сторінки в соцмережах // Західна інформаційна корпорація (http://zik.ua/ua/news/2015/03/24/nevidomi_zlamaly_sayt_natsgvardii_i_stvoryly_feykovi_storinky_v_sotsmerezhah_575200). – 2015. – 24.03).***

***

Российские банки столкнулись с новой угрозой – вирусом, который атакует терминалы оплаты.

Как пишут «Известия» со ссылкой на источники в МВД, у вредоносной программы достаточно забавное название: Tyupkin. Она появилась в прошлом году, но уже успела доставить беспокойство финансовым структурам Китая, США и государств Европы.

Чтобы внедрить вирус в банкомат, злоумышленники вскрывают сервисный блок. После установки троянская программа заставляет аппарат выдавать купюры без всяких ограничений. Добыча преступников может составить 10 млн р.: такую сумму обычно закладывают в банкомат ***(Преступники грабят банкоматы с помощью нового компьютерного вируса // Телекомпанія НТВ (http://www.ntv.ru/novosti/1377256/). – 2015. – 23.03).***

***

Новое программное обеспечение для атак на POS-терминалы было обнаружено Cisco. PoSeidon – вредоносная программа, создана на основе печально известного Zeus, использовавшегося для атак на Target в 2013 г.

«Вредоносное ПО повреждает память POS-терминалов, перенаправляя полученные данные на российские домены», – сообщает Cisco. PoSeidon – еще одна программа из растущего списка вредоносного ПО, атакующего системы POS. Злоумышленники по-прежнему будут нацелены на POS, используя различные методы для того, чтобы избежать обнаружения.

«Пока атаки на POS-терминалы приносят прибыль, злоумышленники будут продолжать инвестировать в разработку новых вредоносных программ. Сетевые администраторы должны придерживаться передовой практики в борьбе с этим видом вредоносного ПО», – считают в Cisco.

PoSeidon содержит загрузчик, который остается на зараженных устройствах, для того чтобы исключить чувствительность к перезагрузке и деавторизации учетной записи. Впоследствии загруженная бинарная команда FINDSTR устанавливает кейлоггер, который сканирует память для получения номеров карт. Далее комбинации проверяются с помощью алгоритма «Луна»,

шифруются и отправляются на один из десятков C&C-серверов управления ***(Cisco сообщила о новом виде вредоносного ПО для POS-терминалов // InternetUA (http://internetua.com/Cisco-soobsxila-o-novom-vide-vredonosnogo-po-dlya-POS-terminalov). – 2015. – 24.03).***

***

В браузере Internet Explorer, установленном в системе Windows Phone 8.1 по умолчанию, обнаружена серьёзная уязвимость. Так, браузер всегда маскирует пароль на веб-страницах «звёздочками». То есть, если даже скопировать набор замаскированных символов и вставить их в любой другой документ, то отображаться будут эти же «звёздочки», без непосредственного раскрытия символов самого пароля. Один из пользователей обнаружил уязвимость, которая способна отображать введённые символы в секции для ввода пароля.

Для этого нужно скопировать скрытые символы и вставить их в строку поиска Bing или Cortana и нажать на кнопку поиска. После этого сам пароль отобразится без «звёздочек». Стоит отметить, что в Windows 10 подобная проблема не наблюдается. Вполне вероятно, что Microsoft закроет данную уязвимость и в случае с Windows Phone 8.1 ***(В браузере Internet Explorer для Windows Phone 8.1 обнаружена критическая уязвимость // InternetUA (http://internetua.com/v-brauzere-Internet-Explorer-dlya-Windows-Phone-8-1-obnarujena-kriticseskaya-uyazvimost). – 2015. – 26.03).***

***

ИБ-эксперт WebSegura.net Д. Сопас обнаружил ошибку в программном интерфейсе Instagram, которая позволяет злоумышленнику рассылать ссылки на загрузку файла, инфицированного вредоносным ПО, с контролируемой им учетной записи. У пользователя даже не возникнут подозрения, так как ссылка может направлять жертву на официально зарегистрированный аккаунт в Instagram.

Специалист выявил, что с помощью маркера доступа к любой учетной записи в Instagram, вставив специальный код в поле с биографическими данными, злоумышленник способен создать ссылку на скачивание дистрибутивного файла, который может быть инфицирован вредоносным ПО. Д. Сопас обнаружил, что данный метод работает в браузерах Chrome, Opera, Chrome для Android и в некоторых случаях в Firefox.

Исследователь заявил, что не сумел убедить ИБ-специалистов компании Facebook, которая владеет Instagram, в том, что обнаруженная ошибка предельно опасна для пользователей приложения. Представители Facebook сообщили, что исправление данной находки для них не приоритетно ***(ИБ-эксперт обнаружил ошибку в программном интерфейсе Instagram // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/27/Instagram-flaw.html). – 2015. – 27.03).***

***

Мощность DDoS-атак в IV квартале 2014 г. увеличилась в 3,47 раза до 4,36 млн пакетов в секунду, сообщается в последнем отчёте компании Black Lotus. Средний объем трафика возрос в 2,45 раза до 12,1 Гбит/с.

За отчётный период самая сильная DDoS-атака зарегистрирована 1 октября 2014 г. на 41,1 Гбит/с с 36 млн пакетов в секунду. По понятным причинам, Black Lotus не называет клиента, который стал жертвой такого мощного DDoS.

Рост атак в несколько раз всего за один квартал настораживает экспертов. И хотя пиковый трафик относительно невелик по сравнению с тем, который был зарегистрирован в I квартале (421 Гбит/с), налицо явное увеличение средней силы атак. Она росла примерно на 10 % в трёх предыдущих кварталах, но подскочила в 3,47 раза в последнем квартале.

Это означает, что в этом году защитные системы должны выдерживать трафик как минимум 15 Гбит/с, чтобы обеспечивать клиенту надёжную защиту от большинства атак ***(DDoS-атаки стали втрое мощнее // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/27/ddos-threat-report.html). – 2015. – 27.03).***

***

Европейская комиссия признает, что соглашение Safe Harbour не может гарантировать конфиденциальность личных данных европейских пользователей, которые американские интернет-компании передают в США. Представители комиссии предложили жителям стран ЕС закрыть свои учетные записи в Facebook для того, чтобы сохранить персональную информацию в тайне от спецслужб США.

Подобное заявление было сделано на судебном разбирательстве по делу иска австрийского правозащитника М. Шремса против социальной сети Facebook. Напомним, что М. Шремс является участником группы активистов Europe-v-Facebook, которые считают американскую социальную сеть нарушителем гражданских прав европейских пользователей. В процессе также были поданы жалобы против таких компаний, как Apple, Microsoft и Yahoo!.

М. Шремс утверждает, что работающая в Европе компания не должна передавать личные данные пользователей в США, согласно соглашению Safe Harbour. Европейская комиссия не может гарантировать конфиденциальность переданной информации. В Европарламенте вновь призывают приостановить действие соглашения. Судебное разбирательство продолжиться 24 июня 2015 г. ***(ЕС предлагает в целях безопасности закрыть учетные записи в Facebook // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/03/27/eu-Facebook.html). – 2015. – 27.03).***

***

В мобильной ОС Google Android обнаружилась очередная брешь в системе безопасности, которая незамедлительно была использована для создания нового типа атак на портативные гаджеты. Он носит название Android Installer Hijacking, и в настоящее время ему подвержено почти 50 % всех Android-устройств в мировом масштабе.

Информацию об обнаружении новой уязвимости и Android Installer Hijacking сообщила компания Palo Alto Networks, пишет ресурс PC World. Суть взлома заключается в компрометации вполне легитимных приложений из магазина Google Play с помощью стороннего ПО из других магазинов, к примеру, Amazon Store.

Иными словами, под видом вполне безобидных приложений на ваш смартфон или планшет может быть установлена вредоносная программа, цель которой заключается в краже ваших персональных данных. Утилита будет пересылать злоумышленникам все, включая фотографии, пароли, данные кредитных карт, SMS, электронную почту и многое другое. В настоящее время, как отметили специалисты, около половины всех Android-гаджетов чувствительны к данному способу взлома.

Производители смартфонов и планшетов оперативно отреагировали на появление информации об Android Installer Hijacking. В частности, Google, Samsung и Amazon уже работают над исправлением ситуации. Как отмечается, наиболее уязвимыми являются гаджеты, работающие под управлением Android ниже версии 4.4 KitKat. Данная версия, а также более поздние 5.0 и 5.1 тоже могут быть взломаны, особенно если пользователь получил root-права на своем устройстве ***(Android-устройствам вновь грозит опасность взлома // InternetUA (http://internetua.com/Android-ustroistvam-vnov-grozit-opasnost-vzloma). – 2015. – 26.03).***

***

Некоторые модели IP-телефонов Cisco, предназначенные для малого бизнеса, оказались подвержены уязвимости, позволяющей удаленному пользователю прослушивать переговоры и осуществлять звонки от имени жертвы. Об этом сообщается в бюллетене безопасности компании, опубликованном на прошлой неделе.

Уязвимости был присвоен идентификатор CVE-2015-0670. Она затрагивает модели IP-телефонов Cisco Small Business SPA300 и SPA500, работающие под управлением прошивки версии 7.5.5 и, возможно, более поздних версий.

Брешь существует из-за некорректных настроек аутентификации в конфигурации устройств. Удаленный пользователь может с помощью специально сформированного XML-запроса проэксплуатировать уязвимость и прослушивать телефонные переговоры жертвы, а также осуществлять звонки от ее имени. Таким образом, брешь позволяет раскрыть важные данные и обойти ограничения безопасности.

Отметим, что эксплуатация уязвимости требует, чтобы злоумышленник имел доступ к внутренней сети компании, устройства которой он намеревается взломать. Это несколько сужает вектор атаки.

Производитель пока не выпустил исправление, устраняющее эту брешь. В компании не считают, что уязвимость может стать широкораспространенной. До выпуска обновления администраторам следует включить опцию аутентификации запросов на выполнение XML-кода в меню настроек, а также ограничить доступ к устройству для недоверенных пользователей ***(Уязвимость в IP-телефонах Cisco позволяет прослушивать переговоры жертв // InternetUA (http://internetua.com/uyazvimost-v-IP-telefonah-Cisco-pozvolyaet-proslushivat-peregovori-jertv). – 2015. – 25.03).***

***

Исправленная в 2011 г. брешь в комплекте средств для разработки (SDK) Adobe Flex продолжает ставить под угрозу интернет-ресурсы. Об этом сообщил специалист М. Джентиле в соответствующем бюллетене безопасности. Эксплуатация уязвимости CVE-2011-2461, которая затрагивает версии Adobe Flex SDK 3.x и 4.x, позволяет удаленному пользователю с помощью специально сформированного запроса выполнить произвольный код сценария в браузере жертвы в контексте безопасности уязвимого сайта.

По словам М. Джентиле, в том случае, если файл .SWF был создан при помощи уязвимого компилятора Flex SDK, злоумышленники по-прежнему могут эксплуатировать данную брешь против последних версий веб-браузеров и Flash-плагинов.

Уязвимость позволяет киберпреступникам похищать данные путем осуществления CSRF-атак или обманом заставляя пользователей выполнить переход на вредоносную веб-страницу. В ранних версиях Adobe Flex скомпилированные файлы .SWF некорректно проводят проверку сертификатов безопасности доменов, что может привести к потенциальному возникновению XSS-проблем.

«Поскольку HTTP-запросы содержат файлы cookie и отправляются с домена жертвы, ответы HTTP могут содержать конфиденциальную информацию», – отметил М. Джентиле.

Специалист совместно со своими коллегами провел масштабное исследование, в ходе которого эксперты определяли SWF-файлы, размещенные на популярных веб-сайтах, и анализировали их при помощи специального инструмента, предназначенного для определения уязвимых конфигураций кода. Как выяснилось, уязвимыми оказалось значительное количество интернет-ресурсов, в том числе и три домена, занимающих верхние позиции в рейтинге Alexa Top 100 ***(Исправленная уязвимость в SDK Adobe Flex продолжает представлять угрозу для веб-сайтов // InternetUA (http://internetua.com/ispravlennaya-uyazvimost-v-SDK-Adobe-Flex-prodoljaet-predstavlyat-ugrozu-dlya-web-saitov). – 2015. – 25.03).***

***

Специалисты пришли к выводу, что компьютерные сети, физически изолированные от небезопасных сетей, могут быть подвергнуты взлому. Долгое время изолированные сети считались идеальным решением в вопросах компьютерной безопасности. В банковских и военных системах на протяжении долгого времени применялась данная технология, но исследователи из Университета имени Бен-Гуриона в Израиле открыли метод получения данных с компьютеров изолированных сетей с использованием измерений тепловой эмиссии и с помощью встроенных в компьютеры датчиков температуры.

Новый метод позволяет получить доступ к паролям и ключам защиты перед непосредственной передачей данных на компьютер, находящийся под контролем атакующей стороны. Со взломанного компьютера по такому же принципу можно передавать команды на устройство, находящееся в изолированной сети. Для передачи данных вредоносное программное обеспечение должно быть установлено на обоих компьютерах. Также важно знать, что использование тепловой эмиссии не подходит для передачи больших объёмов данных. 8 бит информации, к примеру, будет передаваться больше одного часа. Но в случае с паролем или секретным кодом расчёт идёт как раз на такие единицы измерения ***(Взлом компьютеров теперь можно осуществить с применением датчиков температуры // InternetUA (http://internetua.com/vzlom-kompuaterov-teper-mojno-osusxestvit-s-primeneniem-datcsikov-temperaturi). – 2015. – 25.03).***

***

Треть крупнейших сайтов уязвимы или взломаны

Согласно новому отчёту компании Menlo Security, Интернет представляет собой очень опасное место: каждый третий среди популярных веб-сайтов уязвим или уже взломан и атакует посетителей с помощью эксплоит-паков.

Например, в конце 2014 г. сайт популярного издания Forbes в течение нескольких дней заражал пользователей, используя уязвимость нулевого дня в Adobe Flash. Именно этот случай сподвиг специалистов Menlo Security на глобальное исследование Интернета. Они проверили миллион сайтов из списка самых посещаемых, по версии Alexa. С каждого сайта был скачан весь контент, который отгружается на компьютер обычного посетителя: фреймы, встроенный контент, виджеты и т. д.

На 66 % сайтов не оказалось никакого вредоносного ПО, а вот остальные 34 % классифицированы как «рискованные». В частности, 22 % серверов работают на уязвимой инфраструктуре, в том числе на уязвимой версии PHP или на уязвимой версии веб-сервера Apache или IIS. Ещё пару процентов веб-сайтов работают на уязвимой CMS, причём они поровну поделены между WordPress и Drupal.

Кроме существующих уязвимостей, 4 % крупнейших веб-сайтов уже по-настоящему взломаны и распространяют зловреды. Ещё 3 % используются для распространения спама или работы ботнетов ***(Треть крупнейших сайтов***

уязвимы или взломаны // InternetUA (http://internetua.com/tret-krupneishih-saitov-uyazvimi-ili-vzlomani). – 2015. – 28.03).