СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(27.01–9.02)

2014 № 3

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(27.01–9.02)
№ 3

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

Головний редактор
В. Горовий, д-р іст. наук, проф.

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компания Facebook отмечает 10 лет с момента запуска – за это время ей удалось добиться статуса крупнейшего социального онлайн-ресурса мира с аудиторией в 1,23 млрд пользователей в месяц, пишет «Обозреватель» (http://tech.obozrevatel.com/news/05321-facebook-ispolnilos-10-let.htm).

Глава Facebook М. Цукерберг создавал соцсеть как сайт для общения исключительно студентов Гарвардского университета, однако скоро ее преимущества оценили – сначала студенты других вузов США, потом школьники, а впоследствии и пользователи со всего мира.

За 10 лет пользователи Facebook установили свыше 200 млрд дружеских связей – соцсеть во многом изменила понимание дружбы, которое теперь часто ассоциируется с наличием человека в списке контактов соцсети. В 2009 г. Facebook первой из социальных сетей запустила кнопку Like – в настоящее время пользователи кликают на нее в среднем по 6 млрд раз в день.

М. Цукерберг сначала не хотел, чтобы на Facebook была возможность обмениваться фотографиями – однако с момента запуска функции в октябре 2005 г. пользователи разместили в соцсети свыше 400 млрд снимков. Кроме того, лишь за последние два года пользователи Facebook обменялись 7,8 трлн сообщений на сайте.

Соцсети принадлежит важный рекорд – первичное публичное размещение ее акций в мае 2012 г., когда Facebook привлекла около 16 млрд дол., стало наиболее успешным IPO в истории США. Хотя сначала акции Facebook резко упали в цене, за последний год их стоимость более чем удвоилась.

Главным приоритетом Facebook на сегодняшний день являются мобильные сервисы. Компания не жалеет денег на их приобретение – например, Instagram обошелся ей почти в миллиард долларов, а также на их разработку.

Число пользователей мобильных сервисов Facebook приближается к миллиарду, а мобильная реклама принесла соцсети 3,15 млрд дол. или 40 % всей выручки в 2013 г. В следующее десятилетие Facebook вступает с 11,5 млрд дол. наличными и амбициозным проектом Internet.org, в рамках которого хочет снять барьеры для подключения людей к Интернету ***(Facebook исполнилось 10 лет // Обозреватель (http://tech.obozrevatel.com/news/05321-facebook-ispolnilos-10-let.htm). – 2014. – 4.02).***

***

Соцсеть Facebook внедрит новый алгоритм сортировки ленты новостей, с помощью которого будет демонстрировать больше текстовых записей от друзей пользователя и меньше – от страниц, на которые он подписан.

Facebook регулярно представляет новые функции для сортировки новостей на сайте. Так, пользователь может отдать приоритет новостям в хронологическом порядке либо самым популярным записям. Функция Pages Feed позволяет просмотреть только новости от страниц, на которые подписан пользователь. В свою очередь, недавно представленные хэштеги и тренды позволяют отследить записи по определенной тематике.

«В ходе внутреннего тестирования мы выяснили, что пользователи публикуют больше обновлений статусов, когда видят текстовые статусы в ленте новостей. Когда мы показывали пользователям больше текстовых статусов от друзей, это привело к росту обновлений статуса на 9 миллионов ежедневно», – говорят в Facebook. В то же время, отмечают разработчики, этот принцип подтвердился только для пользовательских статусов, а не для записей на публичных страницах.

Новый алгоритм ранжирования новостей в Facebook выделяет в разные категории текстовые сообщения от индивидуальных пользователей и от публичных страниц. В результате охват текстовых статусов от публичных страниц может снизиться, предупреждают разработчики.

Однако они призвали администраторов страниц активнее публиковать другие виды обновлений статуса. В частности, говорят в Facebook, если страница или сообщество делится ссылками на сторонние сайты путем нажатия кнопки «Мне нравится» на этих сайтах, то такие публикации более привлекательны для читателей, чем текстовые обновления статуса со вставленной ссылкой на сторонний сайт ***(Facebook покажет больше текстовых записей друзей и меньше – от страниц // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_pokazhet_bolshe_tekstovyh_zapisey_druzey_i_menshe_ot_stranits). – 2014. – 27.01).***

***

В приложении Twitter для Android появилась возможность редактирования фотографий внутри приложения. Кроме того, разработчики улучшили функции ленты новостей.

В последнем обновлении Twitter появился редактор фотографий. Пользователь теперь может делать нужные правки, к примеру, обрезать или поворачивать снимок.

Разработчики на этом не остановились, добавив функцию для обмена фото – пометка пользователя. Она аналогична той, что используется в настоящее время в Facebook.

Также в Twitter для Android изменили ленту новостей. Если при обновлении ленты нет новых твитов, пользователю покажут рекомендуемые твиты и актуальные темы.

В настоящее время обновление доступно только на Android. Пользователям iOS новые возможности станут доступны в ближайшее время ***(В Twitter для Android теперь можно редактировать фото внутри***

приложения // RevolverLab (http://revolverlab.com/in-twitter-for-android-can-now-edit-photos-within-the-application/). – 2014. – 28.01).

***

П. Дуров, по-видимому, покидает «ВКонтакте». И это лучшая вещь, которая могла произойти с «ВКонтакте» за последние годы.

«ВКонтакте» – самая перспективная интернет-компания России. Она смогла сформировать аудиторию с самой интересной демографической характеристикой – молодостью. «ВКонтакте» за последние годы стал основной платформой общения учащейся молодежи от 12 до 25 лет. Целое поколение выросло с «ВКонтакте», это их основная платформа общения и шеринга, причем приток новых школьников во «ВКонтакте» не прекращается. Эта аудитория в настоящее время вступает в возраст 24–35 лет; люди уже при деньгах, но еще бездетные, ценней всего для рекламодателей. У «ВКонтакте» есть все шансы иметь многолетнюю лояльную платежеспособную аудиторию, лучшую среди всех интернет-компаний России – если это поколение, вырастая, не покинет соцсеть.

Именно поэтому хорошо, что время П. Дурова приходит к концу. Аудитория «ВКонтакте» возрастает, а CEO, к сожалению, нет. В настоящее время П. Дуров во главе «ВКонтакте» уже не соответствует той роли, которая нужна компании на новом этапе ее роста. Как минимум он не понимает новых правил игры и по-прежнему ведет себя как мелкий хозяйчик лавочки, а не как глава большого общего хозяйства. Публичная компания с миллиардной капитализацией не может себе позволить руководителя, чьи эмоциональные эскапады и публичные скандалы месяцами составляют основной поток новостей о компании, а демонстративное использование топ-менеджером для личных проектов активов компании (сотрудников, кодовой базы и данных) в нормальных технологических компаниях обычно быстро кончается отставкой.

С этим можно было и смириться, если бы у П. Дурова была большая гибкая стратегия, видение дальних возможностей и вызовов и понимание инструментов, доступных крупной корпорации. Но П. Дуров по-прежнему намного более яркая личность, чем дальновидный руководитель. Пути «ВКонтакте» на новый уровень в основном лежат уже не в новых программных модулях, а в стратегии роста. Что мы знаем о стратегии П. Дурова? Ничего достоверного. Как он видит себе «ВКонтакте» через пять лет? Куда он хочет двигать «ВКонтакте»? Эти вопросы не получили ответа, и, вероятно, руководитель их и не ставит.

Нет недостатка в сторонниках П. Дурова, считающих, что между «ВКонтакте» и ним можно ставить знак равенства. Но давайте посмотрим на ситуацию трезво. Причины успеха «ВКонтакте» не только и не столько в коде. «ВКонтакте» начался как копия Facebook пятилетней давности, клонирование – далеко не самая сложная инженерная задача. Аудитория «ВКонтакте» ценит не только чат «ВКонтакте», но и то, что многие годы

«ВКонтакте» был и остается богатейшим бесплатным репозиторием музыки и фильмов. Типичный сценарий работы подростка во «ВКонтакте» – в окошке чат, а в ушах наушники, где играет плеер «ВКонтакте». Музыка и видео – очень дорогое удовольствие, и уже в первые годы работы только трафик и хостинг «ВКонтакте» обходились в миллионы долларов ежемесячно, а первая выручка у «ВКонтакте» появилась только на пятом году существования. Деньги «ВКонтакте» обеспечивал не П. Дуров, а инвесторы, все это время владевшие львиной долей акций «ВКонтакте».

Это нормальная бизнес-модель: сначала купить аудиторию, затем ее монетизировать. Мы все помним, что Facebook потратил около миллиарда долларов, прежде чем вышел на окупаемость. Только насколько велика здесь роль начинающего менеджера, получившего свое место в проекте благодаря дружеским отношениям с семьей первых инвесторов? Ненулевая, конечно, но далеко не критическая. Совпадение еще не означает причинности.

Один уважаемый деятель Рунета в разговоре со мной сравнил «ВКонтакте» с Apple, а П. Дурова – со С. Джобсом. Возможно, когда-нибудь П. Дуров и получит право на такое сравнение, но для этого необходимо сравниться по достижениям со С. Джобсом – хотя бы создать после ухода новые компании не хуже, чем NeXT или Pixar. Мессенджер, сидящий поверх «ВКонтакте», на уровень таких достижений не тянет. Да и судьба его в том будущем, где у создателя не будет служебного положения для доступа к базе пользователей «ВКонтакте», пока неочевидна.

Как могла бы выглядеть та стратегия, которую мы не слышали от П. Дурова и которая сделала бы «ВКонтакте» многолетним лидером Рунета, а возможно, и превратила бы его в глобальную компанию? Внутри России «ВКонтакте» должен создать для своих пользователей возможности эффективно пользоваться собой после окончания учебы, в профессиональной жизни и для организации досуга. Искать работу во «ВКонтакте» в настоящее время бессмысленно, сидеть во «ВКонтакте» «по работе» желающих пока мало. Потратить при участии «ВКонтакте» деньги на шопинг или развлечения можно, но на других сайтах это можно делать во много раз лучше. Все это задачи, которые «ВКонтакте» придется решить, чтоб его подросшая аудитория и дальше охотно оставалась на старом, насиженном месте. Собственными силами все эти компетенции не нарастить – «ВКонтакте» придется перейти к стратегии активного приобретения других компаний и проектов, причем не только интернетовских.

За пределами России и русскоязычного мира у «ВКонтакте» тоже есть хорошие шансы нарастить аудиторию. Тут простых рецептов нет, и рекомендовать заманивать юзеров на бесплатную музыку и кино, конечно, не стоит (хотя и может сработать). Но на сегодняшний день у «ВКонтакте» достаточно денежных ресурсов и инженерной инфраструктуры, чтобы ставить эксперименты и в конце концов найти свои рынки и пользователей в большом мире. В настоящее время «ВКонтакте» стоит 2–3 млрд дол. (оценка экспертов «Коммерсанта»), но через несколько лет капитализация

«ВКонтакте» может составить 10–12 млрд дол., а через десятилетие – 25–30 млрд дол. Если, конечно, компания преодолеет свою подростковость и местечковость, при этом не потеряв постоянной привлекательности для школьников и студентов.

Если акционеры хотят увеличить капитализацию «ВКонтакте», они должны сделать для этого несколько следующих шагов. Во-первых, сформировать совет директоров международного класса и калибра, состоящий из экспертов, профессионалов и лидеров, способных оценить перспективы компании и направить ее рост. Во-вторых, совет директоров должен найти нового лидера, который быстро нарастит возможности «ВКонтакте» и через собственные ресурсы, и через приобретения, выстроит новые отношения в коллективе, основанные не на личной преданности вождю, а на сочетании материальных стимулов и общей культуры, создаст систему открытия новых направлений и перспектив, разработает продукты для пользователей и продукты для рекламодателей. Словом, новый лидер должен создать машину роста не хуже чем у лидеров мирового интернет-рынка.

Неизвестно, смогут ли достичь такого качества роста акционеры без П. Дурова. И гарантии никто не даст. Можно и остаться на прежних позициях, и загубить то, что имеется. Но вот с П. Дуровым «ВКонтакте», пожалуй, вырастет слишком поздно, а скорее вовсе никогда. Поэтому то, что происходит в настоящее время, – еще не хорошо, но уже к лучшему ***(«ВКонтакте» вырос. Нужен ли ему Дуров? // InternetUA (http://internetua.com/vkontakte--viros--nujen-li-emu-durov). – 2014. – 28.01).***

***

Социальная сеть Facebook запустила в работу первый прототип системы хранения данных, основанной на оптических дисках Blu-ray. Новая технология, по расчётам инженеров, сократит расходы на хранение данных приблизительно вполовину, а энергопотребление – на 80 %, пишет Блог Imena.UA (http://www.imena.ua/blog/facebook-blu-ray-archive).

Система способна содержать в себе петабайты информации, и лучше всего подходит для хранения материалов, к которым не требуется регулярный доступ.

Хранилище представляет собой кластер из 10 тыс. Blu-ray дисков, разбитых на десятки секций. В среднем, одна секция может хранить в себе около 1 петабайта информации (10 в 15 степени байтов).

Первое хранилище вмещает 30 петабайт информации, а в ближайшем будущем оно будет расширено до 50 петабайт. По словам главного инженера социальной сети Д. Париха в конечном счёте хранилище на Blu-ray дисках будет расширено до 150 петабайт.

Представители Facebook уже заявили, что новое решение позволит им серьёзно сэкономить: такие системы отличаются низким

энергопотреблением. Финансовая сторона выгоды ещё не подсчитана точно, однако, речь идёт о миллионах долларов экономии.

Согласно предварительным подсчётам, проведённым инженерами Facebook, ввод в действие роботизированной системы, основанной на дисках Blu-ray, за год позволит Facebook сократить расходы на хранение данных на 50 %, а расходы на энергопотребление на 80 % ***(Facebook сэкономит миллионы, запустив в работу хранилище на дисках Blu-ray // Блог Imena.UA (http://www.imena.ua/blog/facebook-blu-ray-archive). – 2014. – 29.01).***

***

Социальная сеть Facebook в понедельник, 3 февраля, представила приложение Paper. Оно предназначено для чтения новостей и прочих записей, опубликованных в Facebook. Пока программа доступна только пользователям из США.

Paper позволяет читать записи, составленные друзьями, публичными персонами, компаниями и средствами массовой информации. Записи сортируются по тематическим категориям – например, «Спорт» или «Технологии».

Чтобы увидеть ту или иную запись, не обязательно быть подписанным на страницу лица, которое ее оставило. Программа сама выявляет интересные, с ее точки зрения, новости, и распределяет их по категориям.

Поиск и отбор записей для Paper осуществляются частично автоматически (на основе количества лайков и прочих данных), а частично «вручную» командой редакторов Facebook.

Другая особенность программы – нестандартный, в сравнении с обычными мобильными приложениями Facebook, интерфейс. В приложении нет традиционных кнопок и меню, а новости показываются в виде карточек.

Несмотря на то, что программа формально является «читалкой» новостей, она, как и мобильные клиенты Facebook, позволяет писать сообщения, просматривать уведомления и выполнять поиск.

Пока Paper доступна только на iPhone и iPod touch, работающих на базе iOS 7. Facebook не уточняет, выйдет ли версия программы для планшетов iPad и устройств под управлением Android.

Facebook уже получила претензию из-за названия приложения. Студия FiftyThree, создавшая iPad-«рисовалку» Paper, в своем блоге обратилась к представителям соцсети с просьбой переименовать программу ***(Facebook выпустила приложение для чтения новостей // InternetUA (http://internetua.com/Facebook-vipustila-prilojenie-dlya-csteniya-novostei). – 2014. – 4.02).***

***

Социальная сеть Facebook совместно с компанией SecondSync проанализирует обсуждение пользователями популярных телевизионных шоу. Сообщение об этом 31 января появилось в официальном блоге соцсети.

Как говорится в посте, в Facebook заключили партнерское соглашение с SecondSync, в рамках которого соцсеть поделится с аналитической фирмой данными о пользовательской переписке. Анализироваться будут сообщения, касающиеся программ американского, британского и австралийского ТВ.

По словам представителей соцсети, вся используемая информация будет полностью анонимной и о нарушении конфиденциальности пользователей речь не идет. Первый доклад о степени вовлеченности пользователей Facebook в обсуждение ТВ, как сообщается, Facebook и SecondSync представят в феврале.

Статистику обсуждения пользователями Facebook популярных телепрограмм шоу ранее стали получать такие американские каналы, как ABC, NBC, Fox и CBS. Кроме того, в прессе появилась информация о том, что схожие договоры о сотрудничестве подписаны Facebook с рядом французских, немецких и бразильских телеканалов. Тем не менее, все подобные сведения распространялись в закрытом режиме и нигде прежде официально не публиковались.

Собственный анализ телевизионных предпочтений пользователей проводит также и другая крупная социальная сеть – Twitter. С октября 2013 г. совместно с аналитическим агентством Nielsen компания составляет телевизионный рейтинг Twitter Nielsen TV. Рейтинг составляется на основе количества твитов, посвященных тому или иному телешоу ***(Facebook поделится перепиской пользователей с телеаналитиками // InternetUA (http://internetua.com/Facebook-podelitsya-perepiskoi-polzovatelei-s-teleanalitikami). – 2014. – 31.01).***

***

Во время своего выступления на мероприятии по подведению итогов четвертого финансового квартала прошлого года М. Цукерберг сказал, что графический поиск для мобильных устройств заработает в социальной сети Facebook уже очень скоро. Оказывается, что компания уже находится в стадии тестирования нового сервиса, а некоторые пользователи даже имели возможность его использования.

Если верить имеющейся информации, пользователи клиента социальной сети для мобильных устройств получат все те же возможности графического поиска, которые существуют в десктопной версии Facebook. Уже позже официальный представитель социальной сети подтвердил эту информацию для издания The Verge.

Напоминаем, что в 2014 г. Facebook планирует выпуск большого количества мобильных приложений. Похоже, что графический поиск с его потенциалом вполне может стать началом воплощения в жизнь амбициозных

планов руководства компании ***(Facebook тестирует графический поиск для мобильных устройств // InternetUA (http://internetua.com/Facebook-testiruet-graficseskii-poisk-dlya-mobilnih-ustroistv). – 2014. – 2.02).***

***

Facebook наконец приближается к запуску социального поиска (Graph Search) на мобильных платформах, сообщил основатель компании М. Цукерберг при оглашении финансовых результатов компании за 2013 г.

«Очень скоро мы, наконец, запустим мобильную версию социального поиска, – сказал М. Цукерберг. – Это будет важным шагом для нас, поскольку значительная часть наших пользователей выходит в соцсеть преимущественно с мобильных устройств. Мы надеемся, что запуск мобильного GraphSearch повысит вовлеченность пользователей при взаимодействии с Facebook».

Согласно финансовому отчету Facebook за IV квартал 2013 г., число мобильных юзеров соцсети стремительно возрастает. Количество ежедневных пользователей, заходящих в соцсеть с мобильных устройств, составляет 556 млн. Ежемесячная мобильная аудитория достигает 945 млн пользователей.

Напомним, анонсированный в январе 2013 г. Graph Search расширенный внутренний поиск по социальной сети позволяет пользователям осуществлять поиск открытой личной информации пользователей, которая обычно не проникает в веб.

Социальный поиск, которые изначально преподносился в качестве одного из главных продуктов Facebook, наряду с новостной лентой и Timeline, спустя год после запуска был все еще доступен только на десктопных версиях.

Другой шаг, уже сделанный в сторону развития мобильного направления – запуск фрейворка для создания мобильных приложений – Bolts.

Программное обеспечение, разработанное на базе технологий облачной платформы Parse, призвано облегчить жизнь разработчикам мобильных приложений для iOS и Android.

Разработчику достаточно загрузить «каркас» и приступить к созданию собственных программных продуктов. Напомним, что в апреле 2013 г. Facebook приобрел облачную платформу Parse, которая позволяет разработчикам использовать нативные объекты для обеспечения эластичной масштабируемости ***(Социальный поиск Facebook скоро появится в мобильных // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sotsialnyy_poisk_facebook_skoro_poyavitsya_v_mobilnyh). – 2014. – 4.02).***

***

Израильская социальная сеть для геев Moovz планирует выйти на рынок Украины. Об этом изданию Lenta.ru сообщил основатель соцсети Л. Элиаш. В настоящее время руководство собирается заняться поиском официального представителя своего бренда в Украине, который занимался бы продвижением сайта в уанете. С помощью этих шагов в Moovz надеются увеличить долю украинской аудитори, пишет AIN.UA (http://ain.ua/2014/01/30/510989).

К идее развиваться в Украине израильскую соцсеть для геев подтолкнула популярность украинского танцевального коллектива, который часто обвиняют в пропаганде гомосексуализма. «Недавно мы провели у себя на сайте трансляцию живого выступления украинской танцевальной группы Kazaky, состоящей из одних мужчин. Трансляцию смотрело более двух тысяч пользователей», – заявил Л. Элиаш.

Также Moovz будет искать представителя в России – несмотря на то что там агрессивно настроены по отношению к людям нетрадиционной ориентации. Пока, по словам Л. Элиаша, доля российских пользователей Moovz в общей аудитории соцсети «не столь велика», но это планируют исправить активным локальным промоушеном.

Moovz был запущен в середине января и позиционируется как «соцсеть для геев по всему миру, объединяющая людей со схожими взглядами и интересами». По данным компании, с момента запуска пользователи отправили более 5,5 млн сообщений и создали около 8,5 млн «событий». На сегодняшний день сайт работает на девяти языках и доступен как на десктопе, так и на мобильных платформах iOS и Android. Пока русской и украинской версий сайта нет. Вероятно, они появятся с официальным выходом Moovz на локальные рынки ***(Израильская социальная сеть для геев Moovz ищет представителя в Украине // AIN.UA (http://ain.ua/2014/01/30/510989). – 2014. – 30.01).***

***

Соціальна мережа Twitter разом із стартапом Dataminr запустять новий проект, що допомагатиме журналістам шукати в потоці користувацької інформації потенційно важливі новини. Про це повідомляє jourdom.ru з посиланням на Dataminr.

Новий сервіс Dataminr for News відправлятиме журналістам сповіщення на комп'ютер чи мобільний пристрій про потенційні гарячі новини. За даними TechCrunch, Dataminr for News стане доступним для журналістів уже цього року. Проте вартість передплати не розголошують.

Компанія CNN наразі тестує сервіс. Упродовж кількох місяців вона активно використовує Dataminr у своїй роботі: щодня публікує щонайменше дві історії на основі згенерованого сервісом сюжету. За словами керівника CNN Digital К. Естенсон, сервіс допомагає бачити історії раніше за конкурентів.

Новий ресурс базуватиметься на технологіях стартапу Dataminr. За допомогою спеціальних алгоритмів він аналізуватиме потік публічних повідомлень у Twitter. Сервіс також виявлятиме важливі факти та спалахи зацікавлення до певних тем у всьому світі.

Dataminr існує п'ять років. Дотепер його технології використовували інвестори. Зокрема, ресурс допомагав їм приймати рішення щодо капіталовкладень на основі обговорень у соціальних мережах ***(Twitter повідомлятиме журналістів про важливі новини // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/27279). – 2014. – 30.01).***

***

Российская социальная сеть «Мой Мир» значительно изменила дизайн сайта, сообщает IT Expert.

Базовая палитра оформления осталась прежней, при этом изменилась локализация основных элементов. По просьбам пользователей было изменено расположение блоков меню. Поменялся вид заголовков, превью фотографий и видео. Также изменилась структура меню под аватаром. Кроме того, в «Моем Мире» появилась возможность удалять события сразу из ленты.

«За последние годы в соцсети появилось много новых функций, и иногда они с трудом вписывались в старое оформление. Пришло время переосмыслить эргономику», – комментирует руководитель соцсети «Мой Мир» Д. Алаев.

Изменения коснулись не только оформления главной страницы проекта и ленты новостей, но и отдельных элементов. Например, фильтры по типам новостей теперь расположены рядом, а ссылка на гостевую книгу вынесена отдельно. «Мой Мир» заявила, что изменения затронули и технические характеристики – значительно возросла скорость работы сайта.

Как пояснили в компании, обновление было протестировано на некотором количестве пользователей, после чего, при отсутствии технических сбоев, масштабировалось до полного охвата аудитории. На момент публикации обновленный дизайн должен быть доступен 100 % пользователей.

«Мой мир» – проект компании Mail.Ru Group. В настоящее время аудитория ресурса в России, по данным TNS, насчитывает 31,5 млн человек в месяц ***(Соцсеть «Мой Мир» изменила дизайн и функционал сайта // IT Expert (http://itexpert.in.ua/rubrikator/item/33700-sotsset-moj-mir-izmenila-dizajn-i-funktsional-sajta.html). – 2014. – 4.02).***

***

Компания Gemius измеряет Интернет в более чем 30 странах Европы, Среднего Востока и Северной Африки. В 11 странах, таких как Саудовская Аравия, Беларусь, Дания, Египет, Иордания, Польша, Турция, Россия, Украина, Венгрия и ОАЭ, компания также измеряет популярность Facebook

среди местной аудитории, пишет Marketing Media Review (http://mmr.ua/news/id/gemius-kto-polzuetsja-facebook-38186/).

Наибольшая доля интернет-пользователей, посещающих Facebook.com, отмечается в Венгрии и в Турции: приблизительно девять пользователей из десяти (86 %); за ними следует Египет – 82 %. Самый низкий показатель популярности Facebook в Беларуси (19 %), Украине (28 %) и России (30 %).

«Установлено, что более 48 % активных пользователей Facebook заходят туда ежедневно, будь то праздник или будний день. Более 40 % пользователей с утра, в первую очередь, просматривают последние новости на Facebook, – говорит Л. Летаветис, эксперт компании Gemius на рынке онлайн. – Ну и конечно, интенсивность интеграции портала и мобильных устройств только набирает обороты. Приблизительно половина, а именно 680 млн пользователей, заходят на сайт с их помощью».

Кто пользуется Facebook?

В Дании, адрес www.facebook.com посещает 72 % интернет-пользователей в месяц. Наибольшей популярностью он пользуется среди лиц в возрасте от 46 лет и старше, доля которых составляет приблизительно половину (44 %) всех пользователей социальных сетей. Другой большой группой пользователей являются лица в возрасте от 15 до 25 лет (21 %).

Оказывается, в Польше Facebook имеет почти такой же уровень популярности. Им пользуются 75 % всей интернет-аудитории. Наиболее популярен Facebook среди молодых пользователей в возрасте от 19 до 25 лет. Из данной целевой аудитории целых 80 % пользуются этой популярной социальной сетью. Следующими группами являются пользователи в возрасте 26–35 (76 %) и 7–18 лет (75 %), соответственно.

А вот в Беларуси, например, Facebook не очень популярен. Его посещают всего 19 % интернет-пользователей в месяц. При этом распределение пользователей по возрасту более похоже на то, которое наблюдается скорее в Польше, чем в Дании – целых 40 % из них это пользователи возрасте от 26 до 35 лет. Следующая группа пользователей в возрасте 15–25 лет составляет 35 %.

Главной задачей данного исследования является изучение количества и демографического профиля интернет-пользователей, а также того, как они пользуются Интернетом. Исследование проводится на основе разработанной компанией Gemius собственной гибридной методологии в соответствии с Международным кодексом ICC/ESOMAR ***(Gemius: кто пользуется Facebook? // Marketing Media Review (http://mmr.ua/news/id/gemius-kto-polzuetsja-facebook-38186/). – 2014. – 4.02).***

***

Благодаря закрытости доступа, микроблог Twitter объявил о старте масштабного исследования: избранным установам дадут бесплатный доступ к базе 140-символьным микро-постам. Twitter пошла на это в рамках своей программы Data Grants.

Если вам показалось, что недавно в Интернете произошло нечто подобное, то вы не ошибаетесь. Foursquare поступила подобным образом, использовав при этом ту же компанию что и Twitter. Gnip, выполняет всю работу связанную с исследованием, но лавры достаются социальной сети, которую та изучает.

Исследуемые данные дадут ученым информацию о том, откуда берутся тренды или как начинают появлятся твиты об одном и том же событии во всем мире.

Дедлайн для желающих поучаствовать в проекте – 15 марта ***(Twitter откроет доступ к вашим лентам во благо науки // Vido.com.ua (http://vido.com.ua/article/7939/tvittier-otkroiet-dostup-k-vashim-lientam-vo-blagho-nauki/). – 2014. – 6.02).***

***

В рамках своего 10-летия Facebook запустила видеофункцию Look Back – автоматически генерируемые уникальные видеоролики для каждого пользователя социальной сети. Многим идея пришлась по душе, но немалое количество пользователей осталось недовольно своими автоматическими социальными воспоминаниями.

Как сообщает ресурс TechCrunch, ссылаясь на представителей Facebook, в перспективе (точная дата пока не называется) компания представит инструмент для редактирования этих видео. Инструмент позволит выбрать альтернативные фотографии и материалы, если подобранные автоматически не пришлись по душе.

Журналисты утверждают, что Facebook изначально собиралась представить Look Back вместе с инструментами редактирования, но не успела к сроку. Это косвенно подтверждает тот факт, что страница поддержки Look Back уже включает информацию о редактировании последовательности при помощи специальной кнопки (которой пока нет).

Кстати, вполне вероятно, Look Back является первым шагом Facebook к внедрению некоего штатного веб-инструмента для простого и быстрого создания пользователями видеороликов на основе загруженных ранее материалов в социальную сеть. Например, к Новому году, какому-либо празднику или событию ***(Facebook позволит пользователям редактировать свои видеоролики Look Back // InternetUA (http://internetua.com/Facebook-pozvolit-polzovatelyam-redaktirovat-svoi-videoroliki-Look-Back). – 2014. – 7.02).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Уперше за весь час існування Twitter хештег, пов’язаний з Україною, вийшов на перше місце у світових трендах Twitter. 27 січня о 17:00 за Києвом

активісти розпочали Twitter-шторм на підтримку Євромайдану з хештегом #digitalmaidan. Twitter-storm – це публікація у Twitter великої кількості повідомлень з однаковим хештегом.

На момент написання статті інтенсивність постів з хештегом #digitalmaidan становить 5–6 твітів за секунду.

Організатори Twitter-шторму підготували близько 100 твітів, які були націлені на телеканали, газети, чиновників, знаменитостей за кордоном.

Організатори вважають, що, «об'єднавшись разом у Twitter-storm за допомогою повідомлень, можна підвищити обізнаність користувачів Twitter про тяжке становище протестувальників і про те, що поставлено на карту» ***(#digitalmaidan вийшов на 1-ше місце в світових трендах Твітера // UkrainianWatcher (http://watcher.com.ua/2014/01/27/digitalmaidan-vyyshov-na-1-she-mistse-v-svitovyh-trendah-tvitera/). – 2014. – 27.01).***

***

Активные украинцы все чаще выражают свою политическую позицию в соцсетях. Как показал подсчет тематических групп на разных платформах, в «Одноклассниках» явно больше симпатизируют Антимайдану, а вот в Facebook и «ВКонтакте» наоборот поддерживают митингующих.

Эксперты объясняют: в последних соцсетях моложе аудитория, кроме того, информация распространяется вирусным способом и быстрее доходит до пользователей.

«В Facebook больше офисных работников, которые легче поддаются на что-то новое, они готовы к изменениям. А в "Одноклассниках" – представители реального сектора экономики. Они предпочитают стабильность. Для усредненного "одноклассника" принцип: чтобы не было войны», – говорит PR-стратег «Ашманов и Партнеры Украина» С. Дидковский.

Facebook считается рупором Майдана. Именно с призыва журналиста М. Найема в этой соцсети начался первый митинг в столице. По сути, Facebook – большая штаб-квартира Евромайдана. Здесь собирают деньги на лечение пострадавших, организовываются участники Автомайдана, а лидеры ведут свои странички.

За последние три месяца интерес к страничкам политиков возрос: в среднем они получили на 30 % больше подписчиков.

«ВКонтакте» сидит разношерстная аудитория (более 10 млн) и охватывает всю страну, считает эксперт по соцсетям А. Мишин: «Здесь находится основная страничка радикальной организации "Правый сектор", именно в этой соцсети распространилось видео, на котором силовики издеваются над активистом. Но в то же время во "ВКонтакте" больше всего групп, поддерживающих действия беркутовцев».

А вот «Одноклассники» четко антимайдановские – здесь самые активные борцы против евромайдановцев. «Они проводят рейды по соцсети и тролят странички ярых евромайдановцев, – говорит А. Мишин. – Здесь,

пожалуй, с большей частотой размещают видео и фото в поддержку своих идей».

Создатель Одноклассники.ru А. Попков считает, что просто в его соцсети люди постарше. «Они больше думают о последствиях митингов и ценят стабильность», – сказал он.

Эксперты считают, что дело не только в возрастном контингенте соцсети, но и в вирусной системе распространения информации.

«В Facebook в основном городские жители, много представителей интеллигенции, творческих профессий. Кстати, в этой соцсети почти треть – жители Киева и области. И тут самый молодой контингент. Как известно, на Майдане большинство – это молодежь, студенты, – говорит эксперт по социальным сетям А. Калинкин. – В то же время функциональность Facebook (распространение информации самими пользователями) – вирусная. К примеру, если один пользователь лайкнул пост или новость, это видят его друзья. В других соцсетях этот принцип развит хуже» ***(Эксперты выяснили, какая соцсеть является рупором Антимайдана // From-UA. Новости Украины (http://www.from-ua.com/news/f058900147002.html). – 2014. – 5.02).***

***

Украинские политики не остались чужды общемировому тренду – все больше государственных деятелей обзаводится своим представительством в социальной сети.

Вопрос о том, кто ведет страницы политиков – они сами или их помощники, – обычно остается за кадром. «Наиболее распространенный вариант – комбинированный, когда страницу в соцсети ведет и политик, и его пресс-служба, – поясняет директор Института глобальных стратегий В. Карасев. – Как правило, у политика мало времени на то, чтобы постоянно следить за своим профилем в Facebook, но, думаю, он не забывает про него».

Рекордсменом по количеству подписчиков на свою страницу является В. Кличко – более 60 тыс. человек. На втором месте остается теперь уже бывший премьер-министр Н. Азаров, на чью страницу остаются подписанными более 54 тыс. человек. Замыкает тройку лидеров народный депутат С. Тигипко. Несмотря на то, что политик честно указал, что страница сопровождается его пресс-службой, на нее подписаны более 51 тыс. человек.

Среди популярных в социальных сетях политиков многие уже утратили статус, которому они в значительной степени обязаны количеством подписчиков. Например, на странице А. Костусева до сих пор написано – «мэр Одессы», хотя он не является таковым уже несколько месяцев.

За последние три месяца – с момента начала активных гражданских протестов в Украине – интерес к страницам украинского истеблишмента значительно возрос. Количество читателей Н. Азарова в Facebook увеличилось на 45 %. Мэр Львова А. Садовый увеличил показатель с 15 тыс. до 19,4 тыс. читателей. В. Балога – с 10 тыс. до 14,85 тыс. Также возрос интерес к странице В. Януковича-младшего: количество его читателей

достигло более 14 тыс. против 1635 подписчиков официальной страницы в социальной сети его отца ***(ТОП-10 украинских политиков по версии Facebook // Городской Дозор (http://dozor.kharkov.ua/news/social/1147394.html). – 2014. – 4.02).***

***

25 февраля Крыму пройдет первая встреча модераторов крымскотатарских групп в социальных сетях. Об этом информационному агентству QHA председатель общественной организации «Къардашлыкъ» А. Эмирсалиев.

Цель встречи модераторов – знакомство, обмен опытом и проблемами, обсуждение дальнейшего плана развития сферы сообществ в социальных сетях.

«Мы встретимся, чтобы друг с другом познакомиться, поделиться опытом и историей успеха, обсудить проблемы, которые стоят перед крымскотатарским народом, наметить перспективы развития сообщества, а также обсудить редакционную политику крымскотатарских групп в соцсетях».

Как отметил А. Эмирсалиев, в наше время существует разрыв между представителями крымскотатарской молодежи.

«Сообщество крымских татар в социальных сетях очень разрознено. В настоящее время существует огромное количество групп в социальных сетях, которые не имеют согласованной информационной политики и разрывают крымскотатарскую молодежь, использующую социальные сети, на отдельные группы», – пояснил он.

«Мы приглашаем каждого активного пользователя социальных сетей, а также людей, у которых есть видение касательно того, какие задачи стоят перед крымскотатарским онлайн-сообществом, к обсуждению взаимодействия Новых Медиа на благо просвещения и объединения крымских татар», – сообщает пресс-служба организации «Къардашлыкъ».

Напомним, общественная организация «Къардашлыкъ» является инициатором многих проектов, среди которых – перевод интерфейса социальной сети «ВКонтакте» на крымскотатарский язык ***(Впервые в Крыму соберутся крымскотатарские модераторы // QHA (http://qha.com.ua/v-krimu-sozdana-edinaya-sistema-ekstrennoi-meditsinskoi-pomoschi-132976.html). – 2014. – 4.02).***

***

Пользователи Twitter опубликовали более миллиона сообщений в этой соцсети с хэштегом #Sochi2014 в субботу, 8 февраля, сообщает Digit.ru по результатам мониторинга сервиса Socialbakers.

Из десятки субботних российских трендов Twitter пять посвящены Олимпиаде: #Olympics2014, #ЦеремонияОткрытия, #открытиеолимпиады, #Sochi2014, #Russia.

В пятницу в первый час после открытия Олимпиады было написано более 290 тыс. постов с хэштегом #Sochi2014, во второй – более 390 тыс., но общее количество таких сообщений за день не достигло миллиона.

По данным сервиса Socialbakers, самая популярная тройка языков сообщений в Twitter об Олимпиаде – это английский, испанский и русский, около 84, 5 и 4 % от всех сообщений соответственно. Самые упоминаемые виды спорта – фигурное катание, керлинг и сноуборд ***(В Twitter за день написано более миллиона сообщений об Олимпиаде // InternetUA (http://internetua.com/v-Twitter-za-den-napisano-bolee-milliona-soobsxenii-ob-olimpiade). – 2014. – 8.02).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Как социальные сети изменятся в 2014 году

Mashable опросил девять успешных предпринимателей на предмет того, как они планируют изменять свои SMM стратегии в течение последующих шести месяцев, исходя из своих прогнозов на новый год, пишет Marketing Media Review (http://mmr.ua/news/id/kak-socialnye-seti-izmenjatsja-v-2014-godu-38089/). Вот что они ответили:

1. Рост популярности графического программного обеспечения.

Посты в Facebook с фото получают на 53 % больше лайков, на 104 % больше комментариев, и на 84 % больше кликов, чем текстовые посты, согласно данным Kissmetrics. С ростом Pinterest и Tumblr станет еще более важным создание контента в визуальной форме, либо в виде инфографики, фото с текстовой надписью на нем, или иллюстрации к цитатам. Мы будем больше использовать программного обеспечения для решения графических задач, чтобы превратить текстовый контент в визуальный для увеличения его расшаривания в социальных медиа.

Лаура Пеппер Ву, 30 Day Books

2. Социальные сети не будут использоваться для продаж.

Пользователям нравится покупать, но им не нравится, когда им продают. Компании, которые в настоящее время, наиболее популярны в социальных сетях, сосредоточены на вовлечении, формированию отношений и предоставлению ценностей с помощью социального охвата. Потребители и потенциальные покупатели будут искать компании, которые предлагают ценность, развлечения, скидки, помощь и вовлечение.

Чарльз Годет, Predictable Profits

3. Взрыв автоматизации.

Специалистам по работе в социальных сетях в настоящее время приходится многое нести на своих плечах. Они должны быть голосом

бренда, во главе любых промо-кампаний или маркетинговых кампаний бренда, инструментов, которыми они измеряют социальные медиа, разных сообществ на платформах, и т. д. Это много, и настолько разнообразно, что с этим трудно справиться. В 2014 г. появится больше автоматизации тактик (платформы, структуры), чтобы специалисты могли сфокусироваться на контенте и на социальном взаимодействии.

Бреннан Уайт, Watchtower

4. LinkedIn станет самым важным издателем.

Представьте издание с более чем 100 млн читателей и писателями, такими как Б. Гейтс и Р. Брэнсон, все из которых подключены и нацелены на социальную сеть. LinkedIn станет основным источником отраслевых новостей, и следует принять участие в этой экосистеме, и чем раньше, тем лучше. Размещайте оригинальный контент, устанавливайте связи с коллегами в группах.

Тревор Саммер, LocalVox

5. Контент будет больше и лучше.

Простых сообщений и простых вопросов уже недостаточно. Чтобы достичь более глубокой связи с потребителями, компаниям нужно взаимодействовать на более глубоком и интеллектуальном уровне. Короткие видео, инфографика, качественные фотографии, и опросы помогут вовлекать глубоко. Компаниям необходимо взглянуть на свой контент и задать себе вопрос: «Этим будут делиться?» Пример крупной компании, которая преуспевает в настоящее время, это Wal-Mart. Ее контент умный и вовлекающий, а вовлечение фанатов намного выше, чем у конкурентов. Также компаниям необходимо посмотреть на фанатов, которые у них есть, а не на фанатов, которых им хочется заполучить. Если ваши сообщения всегда направлены на установление контакта, они наведут скуку на ваших фанатов, которые уже следуют за вами.

Эндрю Хаулетт, Rain

6. Социальные сети должны будут выделиться.

Социальные сети начали взрослеть. Поэтому, в них сложнее будет выделиться. Чтобы быть победителем в социальных сетях, вам необходимо креативно мыслить и находить способы выделять свой контент из толпы.

Уейд Фостер, Zapier

7. Кампании в социальных сетях должны быть платными.

Я предполагаю, что наиболее эффективные SMM кампании 2014 г. будут оплаченными. Необходимо сейчас уже узнать, как использовать платные инструменты Facebook и Twitter, чтобы иметь преимущество перед конкурентами. Например, вы используете улучшенный инструмент Facebook по работе с аудиторией? Он позволяет загружать базу данных е-мейлов и рассылать специальные сообщения напрямую вашей целевой аудитории. Twitter также ввел платную рекламу. Если вы бренд и хотите быть успешным в Twitter в 2014 г., будьте готовы платить за нее.

Кристофер Джонс, ReferLocal.com

8. Интерактивный контент перевесит статический контент

Создавать статический контент очень легко. В 2014 г. будет поднята планка для типа контента, с которым пользователи захотят взаимодействовать. Ожидайте увидеть более интерактивный контент. 2013 г. был годом «топ-10» списков. Чтобы вовлечь пользователей в 2014 г. и последующих годах, компании должны предложить вовлекающий контент, а сделать это можно с помощью интерактива.

Чак Кон, Varsity Tutors

9. Google+ появится на сцене

Google становится все более важным в ландшафте социальных медиа. Google+ обладает рядом преимуществ. Он создает сильное сообщество, которое позволяет использовать бренд и определяет потребителей, которые заинтересованы вашими продуктами. Он также позволяет бренду стать более социальным с потребителями-единомышленниками. Предоставляет потребителям-единомышленникам платформу для связи друг с другом. Все это позволяет создать сильное сообщество, а это прекрасный способ получить отклик о новых и старых продуктах от потребителей в режиме реального времени.

Николас Гремион, Free-eBooks.net ***(Как социальные сети изменятся в 2014 году // Marketing Media Review (http://mmr.ua/news/id/kak-socialnye-seti-izmenjatsja-v-2014-godu-38089/). – 2014. – 28.01).***

***

Сколько трафика приводят на сайты социальные сети? Западная платформа аналитики Shareaholic провела исследование, пишет Marketing Media Review (http://mmr.ua/news/id/issledovanie-trafik-na-sajty-iz-socialnyh-setej-38071/).

Данные 200 тыс. сайтов с количеством уникальных посетителей свыше 250 млн человек ежемесячно показали: в IV квартале 2013 г. трафик на сайты из Facebook, Pinterest и StumbleUpon увеличился на 30 %. Впрочем, другие социальные сети с точки зрения направления посетителей оказались практически бесполезны.

Доля трафика на сайты из Facebook возросла на 48,85 % (5,07 процентных пунктов по сравнению с III кварталом 2013 г.). Рост посещений из Pinterest в общей доле трафика составил 30,06 % (1,11 процентных пункта). Такой не очень популярный у нас сервис как StumbleUpon в IV квартале возрос на 54,36 % (0,3 процентных пункта). Доля социального трафика из Twitter немного упала. Заметно снизилась доля трафика из YouTube (-34,97 %).

Самыми бесполезными с точки зрения трафика социальными сетями оказались LinkedIn и Google+. Доля трафика на сайты с LinkedIn упала на 26,96 %. Доля Google+, напротив, возросла до 18,98 %. Но так как вклад в общий трафик этой соцсети остается ничтожно мал, в процентных пунктах прирост составил всего 0,01.

В целом исследование показывает интересную тенденцию. Использование в маркетинговых целях даже популярных социальных сетей не может гарантировать прирост посещаемости сайта компании. Поэтому если одна из ваших задач – получение посетителей, не стоит всецело полагаться на SMM. Необходимо использовать комплексный маркетинг, не скидывая со счетов и SEO ***(Исследование: трафик на сайты из социальных сетей // Marketing Media Review (http://mmr.ua/news/id/issledovanie-trafik-na-sajty-iz-socialnyh-setej-38071/). – 2014. – 27.01).***

***

Сервис микроблоггинга Twitter запустил интерфейс аналитической системы для работы с форматом Twitter Cards, который позволяет показывать медийный контент в твитах. Аналитический сервис Twitter Card покажет пути шеринга контента на Twitter.

Основные показатели, которые можно будет видеть в отчете: клики по URL, установки приложений и ретвиты.

- Your Snapshot – показатель привлекательности контента Twitter, показывает количество твитов со ссылкой на сайт или приложение.
- Tweets – сводные данные твитов, показов, кликов, установок и ретвитов всех сообщений со ссылкой на сайт или приложение на Twitter.
- Your Tweets – твиты со ссылкой на веб-сайт из собственных Twitter аккаунтов.
- Типы карт – ведущие по кликам Twitter Cards, параметр позволяет понять, какие именно типы контента больше всего привлекают пользователей. Также в этой секции содержится показатель CTR для других сайтов.
- Links – демонстрирует страницы с наибольшим количеством кликов.
- Influencers – показывают аккаунты с наибольшим количеством ссылок на контент
- Devices – показывает распространенные типы устройств и приложений, с которых пользователи просматривают Twitter Card.
- В качестве мер по улучшению эффективности работы с картами, создатели советуют тестировать различные типы карт и контента; сравнивать свои метрики со средними метриками по разным типам карточек; отслеживать клики и ретвиты для повышения степени вовлеченности пользователей и максимально эффективного общения с аудиторией; использовать правильные метатеги и взаимодействовать с наиболее активными подписчиками ***(Twitter запустил аналитику для Twitter Cards // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapustil_analitiku_dlya_twitter_cards). – 2014. – 28.01).***

***

Facebook мечтает вырасти из просто социальной сети и стать влиятельнее. Более того, компания серьезно настроена стать вездесущей онлайн «электростанцией», влияние которой будет как минимум на уровне с Google.

Шр. Кришнан, работающий над мобильной платформой рекламных объявлений Facebook, пишет, что он и его команда работают над небольшими тестами, чтобы определить, могут ли сторонние мобильные приложения показывать рекламу с Facebook. Если тестирование покажет хорошие результаты, то досягаемость Facebook в мире мобильной рекламы значительно увеличится.

Wired пишут, что Facebook давно мечтала о запуске комплексной сети онлайн-рекламы, которая сможет составить конкуренцию AdSense от Google. Новый проект нацелен на создание аналогичной сети для мобильных устройств. Также Facebook впервые будет обеспечивать мобильные приложения рекламными объявлениями напрямую, при этом не используя чужие рекламные сети.

Если планы Facebook увенчаются успехом, то у Facebook появится реальный шанс поравняться с Google, чье доминирование в данной области неоспоримо.

Последнее исследование eMarketer показывает, что Google получает 53,3 % прибыли от общего показателя за рекламные объявления на мобильных платформах. Пока Facebook получает лишь 15,8 %. Создание собственной сети для мобильной рекламы увеличит прибыль Facebook в несколько раз ***(Как Facebook планирует уничтожить империю Google // Vido.com.ua (http://vido.com.ua/article/7851/kak-facebook-planiruiet-unichtozhit-impieriiu-google/). – 2014. – 27.01).***

***

Чистая прибыль компании Facebook Inc. в IV квартале 2013 г. возросла в 8,17 раза – до 523 млн дол., или до 20 центов на одну акцию, в сравнении с 64 млн дол., или 3 центами на одну акцию, годом ранее. Об этом говорится в опубликованном квартальном отчете компании, пишет «Кореспондент» (http://korrespondent.net/business/companies/3298953-chystaia-prybyl-Facebook-v-IV-kvartale-2013-hoda-vyrosla-v-8-raz).

Выручка Facebook Inc. в IV квартале возросла на 63 %, превысив прогноз аналитиков с Уолл-стрит. Показатель составил 2,585 млрд дол. (годом ранее – 1,585 млрд дол.). Аналитики прогнозировали доход около 2,33 млрд дол. Компания объясняет рост доходов увеличением объема продаж объявлений, предназначенных для показа на мобильных устройствах. Так, доходы от мобильных объявлений в IV квартале 2013 г. составили 53 % от общего квартального объема рекламных доходов (1,24 млрд дол.). В

III квартале этот показатель находился на уровне 49 % от общего объема рекламы.

Крупнейшая в мире социальная сеть объявила, что число зарегистрированных учетных записей достигло 1,23 млрд, при этом 945 млн человек пользуются услугами Facebook посредством планшетов или смартфонов.

В ходе торгов на Нью-Йоркской фондовой бирже 29 января 2013г. цена акций Facebook Inc. возросла на 7 %, составив 57,36 дол. за одну акцию ***(Чистая прибыль Facebook в IV квартале 2013 года выросла в 8 раз // Кореспондент (http://korrespondent.net/business/companies/3298953-chystaia-prybyl-Facebook-v-IV-kvartale-2013-hoda-vyrosla-v-8-raz). – 2014. – 30.01).***

***

Компания Simply Measured проанализировала ТОП-100 крупных мировых брендов и обнаружила, что 92 % из них размещают твиты в среднем 12 раз в день. 58 % брендов имеют свыше 100 тыс. фолловеров. При этом среднее число фолловеров для ТОП-100 брендов – 870 тыс. В целом, за последний квартал 2013 г. число подписчиков у компаний возросло на 20 %.

Исследование показало, что наибольшее вовлечение (ретвиты, ответы, избранное, упоминания) получают твиты с изображениями и ссылками. Впрочем, это не удивительно для SMM-специалистов. Поражают цифры! Твиты, содержащие ссылки и картинки, имеют на 150 % выше уровень вовлечения, чем твиты брендов в среднем. Но только 36 % твитов имеют ссылки, показало исследование.

Значительную часть вовлекающих твитов составляют ответы пользователям. 61 % твитов бренды отправили, отвечая фолловерам.

60 % вовлечения приходится на ТОП-10 крупнейших брендов.

Большое значение на вовлечение оказывает размер аудитории, заявляют исследователи. Так для брендов с числом фолловеров 500–749 тыс. среднее значение вовлечения на один твит составляет 94. Для компаний с количеством подписчиков 750–999 тыс. эта цифра значительно выше – 289. Поэтому если вы хотите, чтобы вас чаще ретвитили и комментировали ваши твиты, наращивайте аудиторию ***(Большинство крупнейших компаний размещают в среднем 12 твитов в день // ProstoWeb http://www.prostoweb.com.ua/internet_marketing/pr_v_internete/novosti/bolshinstvo_krupneyshih_kompaniy_razmeschayut_v_srednem_12_tvitov_v_den). – 2014. – 27.01).***

***

Десять рекламных средств Facebook на замену Sponsored Stories

Как известно, тем, кто хочет заказать на Facebook рекламу в формате Sponsored Stories стоит поторопиться, т. к. уже весной этого года сервис будет закрыт.

В июне 2013 г. Facebook объявил о намерении упростить свои рекламные продукты, чтобы облегчить рекламодателям процесс траты рекламных бюджетов. Логичным продолжением этого стало заявление о том, что количество рекламных сервисов в соцсети сократится с 27 более чем вдвое.

Главным плюсом Sponsored Stories был так называемый «социальный контекст» – такая реклама показывалась в том случае, когда друг пользователя на Facebook как-то взаимодействовал с брендом в этой соцсети. Теперь же этот социальный контекст, по заверениям Facebook, будет встроен практически во все рекламные продукты компании, так что необходимость в поддержке отдельного типа рекламы Sponsored Stories просто отпадает.

В настоящее время существует 10 типов Sponsored Stories, но уже 9 апреля все они трансформируются в другие рекламные форматы. К примеру, Sponsored Story, появляющаяся при лайке на страницу бренда, станет называться Page Like ad.

Тем не менее, и помимо Sponsored Stories на Facebook все еще есть несколько типов таргетированных рекламных объявлений, которыми вполне можно успешно пользоваться.

Desktop App (реклама десктоп-приложения)

Данный тип рекламы – лучший для увеличения числа установок десктопного приложения и вовлеченности. Для того чтобы такое объявление лучше всего отображалось во всех местах, где показывается реклама на Facebook, соцсеть рекомендует следующие параметры: 90 символов текста, формат изображения 1:91, размер изображения 1200 x 627 пикселей.

Domain ad (доменная реклама)

Лучшее средство для увеличения трафика на вебсайт и повышения продаж в онлайне. Рекомендуемые параметры: 25 символов в заголовке, 90 в поле для текста, формат изображения 1.39:1, размер изображения 1200 x 864 пикселя.

Event ad (реклама события)

Суть данного типа рекламы также ясна из ее названия. Если вам нужно привлечь больше аудитории к своему событию – это то, что нужно. Рекомендуемые параметры объявления: 25 символов для заголовка, 90 для текста, формат изображения 8:3, размер картинки – 1200 x 450 пикселей. Event ad может отображаться в ньюсфиде как на десктопе, так и на мобильных устройствах, а также в правой колонке рекламы на десктопе.

MobileAppad (реклама мобильного приложения)

Если ваша задача заключается в увеличении числа установок приложения, вовлеченности и конверсии, то выбор очевиден. Facebook рекомендует придерживаться следующих параметров при создании такой рекламы: 90 символов текста, формат изображения 1:91, размер изображения 1200 x 627. При работе с видео, лучше следовать ограничениям в 15 секунд по времени, формату – MP4 и размеру в 55 мегабайт.

Если у вас нет картинки подходящего размера, то при создании объявления вы увидите предупреждения. Также стоит отметить, что в том случае, если у вашего приложения есть хотя бы 250 оценок в App Center, то на рекламе появятся звездочки рейтинга. Социальный контекст будет проявляться, когда друзья будут играть/использовать игру или приложение, будучи залогиненными в Facebook.

Offer ad (реклама предложения)

Лучший способ стимулировать имеющихся и будущих покупателей – приобрести что-то в офлайн-магазине. Рекомендуемые параметры: 90 символов текста, 25 в заголовке, формат изображения 1.91:1, размер изображения 1200 x 627 пикселей.

Реклама предложений появляется в ньюсфиде на десктопах и мобильных устройствах, а также в правой части страницы. Если загруженное изображение велико, то оно будет уменьшено до размера 100x100 на мобильных устройствах, если заголовок достаточно короткий, то в ленте новостей даты завершения акции могут быть указаны в одну строчку.

Page Like ad (реклама лайка страницы)

Отличный путь увеличения количества лайков вашей страницы. Рекомендуемые параметры: 90 символов текста, формат изображения 8:3, размер изображения 1200x450 пикселей.

Такая реклама показывается в правой колонке, а также в ньюсфидах десктопной и мобильной версии Facebook. На дексктопе, если загруженное изображение больше чем 400x150 пикселей, то оно будет уменьшено до 100x72. На мобильных устройствах, если картинка меньше чем 560x210 пикселей, то она будет сжата до размера 200x144.

Page Post Link ad (реклама ссылки на пост)

Данный вид рекламы используется, когда стоит задача по увеличению конверсий на сайте, включая генерацию лидов и продажи. Рекомендуемые параметры: 90 символов текста, 25 для заголовка, размер изображения 1200x627 пикселей.

Рекламный блок показывается в ньюсфиде на десктопах и мобильных устройствах, а также в правой рекламной колонке. Для ссылок на внешние видео-сайты вроде YouTube ограничение размера изображения на десктопе составляет 90x90 пикселей, для мобильных устройств – 100x100 пикселей.

Page Post Photo Ad (реклама фото на странице)

Используется для повышения узнаваемости бренда и увеличения вовлеченности текущих и будущих клиентов. Отлично подходит и для того, чтобы стимулировать людей взаимодействовать с вашей страницей или конкретной публикацией. Рекомендуемые параметры: 90 символов текста, формат картинки 1:1, размер изображения 1200x1200.

Рекламный блок показывается в ньюсфиде на десктопах и мобильных устройствах, а также в правой рекламной колонке. Если объявление создается для нескольких картинок, то параметры изображений для десктопов должны соответствовать 196x196 пикселей для числа картинок от

двух до четырех, а для трех и более – 129х129 пикселей. Формат изображения для таких объявлений на мобильных устройствах составит 1:1 вне зависимости от размера изображения.

Page Post Text Ad (реклама текстового поста на странице)

Как и предыдущий формат рекламы, Page Post Text Ad лучше всего использовать для увеличения узнаваемости бренда среди текущих и возможных клиентов. Также такие объявления отлично подходят для того, чтобы стимулировать людей взаимодействовать с вашей страницей и постами на ней. Рекомендуемые параметры: 90 символов текста.

Рекламный блок показывается в ньюсфиде на десктопах и мобильных устройствах, а также в правой рекламной колонке на главной странице. На мобильных устройствах и в правой колонке на десктопе текст урезается до 90 символов, но в целом на десктопе можно писать до 500 символов текста.

Page Post Video Ad (реклама видео-поста на странице)

Лучше всего подходит для повышения узнаваемости бренда, показателей вовлечения поста, а также для получения «эффективных» просмотров. Рекомендуемые параметры: 90 символов текста, формат изображения 16:9, размер изображения 1200х675 пикселей.

Рекламный блок показывается в ньюсфиде на десктопах и мобильных устройствах, а также в правой рекламной колонке на главной странице соцсети. Для правой колонки и ленты новостей мобильных устройств максимальный размер видео составляет 1 гигабайт, а длительность – 20 минут ***(10 рекламных средств Facebook на замену Sponsored Stories // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/10_reklamnyh_sredstv_facebook_na_zamenu_sponsored_stories). – 2014. – 28.01).***

***

Акции крупнейшей в мире соцсети Facebook подскочили на 16 % на открытии биржи Nasdaq, впервые пробили психологическую отметку в 60 дол. и обновили исторический рекорд стоимости после оглашения финансовых результатов и анонса мобильного приложения Paper, сообщает IT Expert.

На закрытии торгов Nasdaq 29 января акции Facebook стоили 53,53 дол. – на 2,92 % ниже уровня предыдущего дня, капитализация компании оценивалась в 130,36 млрд дол. За 2013 г. стоимость акций Facebook более чем удвоилась. На электронных торгах после закрытия биржи цена акций подскочила на 12 % сразу после оглашения финотчета.

На открытии Nasdaq 30 января акции Facebook стоили уже 62,1 дол. – на 16 % выше уровня предыдущего дня. В первые минуты торгов они достигли нового рекорда в 62,28 дол. До 30 января историческим максимумом для Facebook во время основной торговой сессии была отметка в 59,31 дол.

Главной причиной позитивной динамики акций Facebook послужили данные о росте мобильной рекламы и аудитории мобильных сервисов ***(Акции Facebook обновили исторический рекорд, превысив отметку в $60 // IT Expert (http://itexpert.in.ua/rubrikator/item/33608-aktsii-facebook-obnovili-istoricheskij-rekord-prevysiv-otmetku-v-60.html). – 2014. – 31.01).***

***

Facebook представил новый функционал для маркетологов, расширяющий возможность достучаться до мобильных и веб-пользователей, чтобы побудить их к активным действиям. Соцсеть теперь позволяет рекламодателям отправлять целенаправленные сообщения людям, которые побывали на их сайте или мобильном приложении, появилась отдельная кнопка с помощью которой маркетологи могут взаимодействовать с пользователями.

Впервые об этом расширении Facebook заявил еще в октябре, и до недавнего времени этой рекламной функцией могли воспользоваться только тестовые партнеры.

В результате анализа трафика с рекламного объявления в Facebook на мобильный или веб-сайт маркетологи получают возможность добавить призыв к действию для своих посетителей. Рекламодатели могут выбрать одну из пяти кнопок: Купить сейчас, Узнать больше, Зарегистрироваться, В закладки или Скачать.

Рекламодатели получили мощный инструмент, позволяющий многократно возвращать трафик на сайт.

В СНГ новый функционал пока не доступен, ожидаем обновление в ближайшие дни ***(Facebook предоставил новый функционал для маркетологов – кнопку «Купить сейчас» // IT Expert (http://itexpert.in.ua/rubrikator/item/33630-facebook-predostavil-novyj-funktsional-dlya-marketologov-knopku-kupit-sejchas.html). – 2014. – 1.02).***

***

Социальная сеть Twitter решила обезопасить себя от патентных исков путем подписания лицензионного соглашения с IBM. В рамках этого договора «голубой гигант» предоставит компании несколько сотен патентов, сообщает IT Expert.

Незадолго до выхода на биржу в ноябре 2013 г. Twitter получила обвинение от IBM в нарушении прав на интеллектуальную собственность по трем патентам, зарегистрированным в США. В настоящее время IBM отозвала свои претензии, поскольку подписала соглашение с Twitter о лицензировании более 900 патентов. Финансовая сторона этой сделки не разглашается.

«Покупка патентов IBM и лицензионное соглашение позволят нам лучше защищать свою интеллектуальную собственность и обеспечивает

свободу действий для создания инновационных решений для пользователей нашего сервиса», – отметил юридический директор Twitter Б. Ли.

По состоянию на 30 сентября прошлого года в распоряжении Twitter было лишь девять патентов и 95 заявок на регистрацию. Для сравнения, перед своим IPO в 2012 г. Facebook владела 774 патентами. В марте 2013 г. крупнейшая мира социальная сеть выкупила у IBM около 750 патентов для борьбы с исками Yahoo!

В 2013 г. IBM подала максимальное среди всех компаний количество заявок на регистрацию патентов – 6508. Для сравнения, показатель Samsung составил 4683 заявки ***(IBM продала Twitter более 900 патентов // IT Expert (http://itexpert.in.ua/rubrikator/item/33682-ibm-prodala-twitter-bolee-900-patentov.html). – 2014. – 4.02).***

***

Наверняка лента новостей вашего Twitter-аккаунта уже переполнена большим количеством бесполезной информации. Похоже, что в недалеком будущем в социальной сети появится еще один новый элемент – кнопка «купить».

Документы, обнаруженные на сайте Fancy.com, указывают на новый способ продажи товаров прямо в социальной сети Twitter. В скором времени появится возможность добавления спонсорских твитов с рекламным изображением продуктов, их ценой и кнопкой «купить через Fancy». Не исключено, что подобной возможностью обзаведется и мобильный клиент Twitter.

Пока остается не ясным, является ли данный документ предложением к сервису микроблогов, или он уже запущен в производство. Впрочем, новость о появлении возможности покупок прямо из Twitter, уже не первый день блуждает по Интернету ***(В Twitter появится кнопка «купить» // InternetUA (http://internetua.com/v-tvittere-poyavitsya-knopka--kupit). – 2014. – 1.02).***

***

Twitter опубликовала свой первый финансовый отчет. Аналитиков беспокоит снижение темпов роста месячной аудитории сервиса. Глава компании Д. Костоло сказал, что знает, в чем кроется причина, и обещает исправить ситуацию, сообщает CNews.RU.

Выручка Twitter в 2013 г. возросла на 110 % до 664,9 млн дол. по сравнению с 316,9 млн дол. в 2012 г., при этом убыток увеличился в 8,1 раза – с 79,4 млн дол. до 645,3 млн дол.

По итогам IV квартала 2013 г. выручка компании возросла на 116 % до 242,7 млн дол., тогда как убыток составил 511,5 млн дол. по сравнению с 8,7 млн дол. годом ранее. В указанный период компания потратила 521 млн дол. на выплату вознаграждений акциями и опционами, отмечается в отчете. Кроме того, компания потратила некоторые средства на расширение штата, отмечает Reuters.

По словам генерального директора Twitter Д. Костоло, последний квартал прошлого года стал лучшим в истории Twitter с точки зрения финансовых показателей (выручки). Он добавил, что Twitter – единственная платформа микроблогов, которая присутствует на бирже.

Напомним, что на биржу Twitter вышла в ноябре 2013 г. И отчет за IV квартал 2013 г. и весь прошлый год стал первым финансовым отчетом, который компания опубликовала открыто.

Между тем аналитиков смущает тот факт, что темп роста месячной аудитории Twitter замедляется. В IV квартале число пользователей возросло на 3,8 % по сравнению с III кварталом (до 241 млн человек). Для справки, в первые три квартала 2013 г. рост составил 10 , 7 и 6 % соответственно. При этом число просмотров Tweets Timeline (домашних страниц) упало со 159 млн в III квартале до 148 млн в IV квартале.

Аналитики опасаются, что месячная аудитория Twitter уже преодолела максимальное значение, но Д. Костоло с таким мнением не согласен. Проблема заключается в том, что сервису не удается заставить новых пользователей остаться в нем. Д. Костоло считает, что причина заключается в неудобстве и обещает исправить ситуацию.

«Мы можем многое сделать для того, чтобы существенно улучшить опыт пользовательского взаимодействия. И я верю, что наша работа, которой мы сейчас занимаемся, повысит степень удовлетворения наших пользователей», – заявил глава компании.

Некоторые аналитики остались под впечатлением того факта, что Д. Костоло признал наличие в Twitter проблем. Многие высокотехнологичные компании отказываются признаться в их существовании до последнего момента.

После публикации отчета стоимость акций Twitter упала на 18 % в период расширенной торговой сессии на Нью-Йоркской фондовой бирже до 54 дол. за штуку ***(Убыток Twitter вырос в 8 раз // proIT (http://proit.com.ua/news/telecom/2014/02/06/130544.html). – 2014. – 6.02).***

***

Стартап 300 Entertainment, возглавляемый ветераном музыкальной индустрии Л. Коэном, решил с помощью Интернета и при партнерстве сервиса микроблогов Twitter начать поиск новых звезд эстрады.

Л. Коэн, ранее возглавлявший Warner Music Group, объявил на музыкальном фестивале Midem в Каннах о заключении соглашения о сотрудничестве с Twitter. В рамках соглашения компания 300 Entertainment получит доступ к базе данных Twitter, касающейся обсуждения различных тем, связанных с музыкой. Как утверждает ресурс New York Times, специалистам 300 Entertainment будет предоставлена и закрытая информация, касающаяся местонахождения пользователей, отправивших твиты.

В свою очередь сервис микроблогов рассчитывает систематизировать с помощью программного обеспечения нового партнера имеющийся массив

данных, которые в дальнейшем смогут использовать для своей работы исполнители, звукозаписывающие лейблы и различные потребительские бренды ***(Twitter предоставил доступ к музыкальным данным стартапу 300 Entertainment // InternetUA (http://internetua.com/Twitter-predostavil-dostup-k-muzikalnim-dannim-startapu-300-Entertainment). – 2014. – 5.02).***

***

Специалисты IBM продолжают экспериментировать с искусственным интеллектом суперкомпьютера Watson. На этот раз систему обучают основам психоанализа в социальных сетях. «Талант» Watson найдёт своё применение в рекламной отрасли, пишет Блог Imena.UA (http://www.imena.ua/blog/ibm-watson-psycho).

В рамках проекта для бизнес-консалтинга инженеры IBM хотят добиться, чтобы их суперкомпьютер, анализируя записи пользователя в социальных сетях, мог безошибочно определять тип личности человека и предугадывать его действия и предпочтения в будущем.

В основе психоанализа лежат протоколы и алгоритмы, которые сверяют тысячи деталей текста и изображений пользователя с запрограммированными нормами поведения и допущениями, и позволяют создавать максимально точный психологический портрет.

Например, суперкомпьютер может самостоятельно выбрать и предложить пользователю рекламу от компаний, которые занимаются ремонтом помещений, если «увидит» на странице человека фото его новой квартиры.

Представители IBM считают, что такой навык суперкомпьютера непременно пригодится маркетологам, которые смогут получить в своё распоряжение огромную базу данных, содержащую массу актуальной информации о потенциальных клиентах.

Используя её, продавцы смогут в нужное время предложить клиенту товар с необходимыми ему характеристиками, дизайном, который по душе пользователю, и по той цене, которую он сможет себе позволить ***(Специалисты IBM обучают суперкомпьютер работе маркетолога в социальных сетях // Блог Imena.UA (http://www.imena.ua/blog/ibm-watson-psycho). – 2014. – 6.02).***

***

Корпорация Microsoft заключила лицензионное соглашение с геолокационной соцсетью Foursquare и инвестировала в компанию. Об этом сообщается в блоге Foursquare.

«В рамках лицензионного соглашения Microsoft будет использовать данные о местах, полученные от Foursquare, в своих продуктах. Эта информация позволит устройствам на базе Windows Phone и Windows и другим сервисам корпорации (например, поисковику Bing) повысить уровень

рекомендаций для своих пользователей», – отметил гендиректор Foursquare Д. Краули.

Как пишет издание Fast Company, Microsoft вложит в Foursquare 15 млн дол. Эти средства станут дополнением к привлечённым сервисом в декабре инвестициям в 35 млн дол.

Foursquare уже сотрудничает с рядом стартапов, например, фотосервисом Instagram и приложением для заказа такси Uber. Сервис предоставляет им доступ к своему API, чтобы пользователи могли отмечать конкретные места, взятые из базы данных Foursquare.

Но сотрудничество с Microsoft идёт глубже, чем просто предоставление доступа к API, рассказал гендиректор Foursquare Д. Краули. По его словам, речь будет идти о механизме пассивных рекомендаций, который предлагает пользователям отмечаться в тех или иных точках, ориентируясь на их интересы. В блоге Foursquare говорится, что нововведение увеличило активность использования приложения на 30 %.

Объявление о сделке появилось практически одновременно со вступлением С. Наделлы на пост генерального директора Microsoft. Но партнёрство с Foursquare не может считаться первым шагом С. Наделлы в новой должности: переговоры о сделке велись последние несколько месяцев, рассказал Д. Краули ***(Сулейманов С. Microsoft вложила 15 миллионов долларов в Foursquare // Tjournal.ru (http://tjournal.ru/paper/microsoft-foursquare). – 2014. – 5.02).***

***

Чистая прибыль социальной сети для делового общения LinkedIn в 2013 г. составила 26,77 млн дол. – на 24 % выше показателя предыдущего года, говорится в сообщении LinkedIn.

Как сообщает IT Expert со ссылкой на Digit.ru, в расчете на одну акцию прибыль LinkedIn за год составила 0,23 дол. по сравнению с 0,19 дол. в 2012 г. Годовая выручка соцсети увеличилась на 57 % до 1,528 млрд дол. «Двигаясь дальше, мы инвестируем значительные суммы в долгосрочные инициативы, которые позволят нам создать экономические возможности для работников по всему миру», – отметил гендиректор LinkedIn Д. Вейнер.

В IV квартале 2013 г. прибыль сервиса снизилась на 67 % до 3,78 млн дол. или 0,03 дол. на акцию, что LinkedIn связывает с выплатой компенсаций в виде акций и амортизацией нематериальных активов. Квартальная выручка LinkedIn возросла на 47 % до 447 млн дол. относительно аналогичного периода прошлого года, что превысило ожидания аналитиков.

Аудитория LinkedIn насчитывает в настоящее время 277 млн пользователей, ежемесячно заходящих на сайт, однако темпы прироста снижаются. Мобильными сервисами соцсети пользуются около 41 % владельцев аккаунтов в LinkedIn. Напомним, что эксперты высказывали опасения относительно способности LinkedIn генерировать выручку на

мобильных продуктах. Однако в прошлом году соцсеть запустила первый формат мобильной рекламы Sponsored Updates.

Помимо финотчета, LinkedIn объявила о планах покупки рекрутингового онлайн-сервиса Bright за 120 млн дол., чьи технологии должны усилить главный генератор выручки LinkedIn – платные объявления от работодателей и соискателей вакансий.

В то же время прогноз LinkedIn на I квартал 2014 г., когда компания ожидает выручки в 455–460 млн дол., разочаровал аналитиков, прогнозировавших в среднем 470 млн дол. Акции компании закрылись 6 февраля на уровне 223,45 дол., но на электронных торгах после закрытия нью-йоркской фондовой биржи упали на фоне финотчета почти на 8 % до 205,99 дол. ***(Лобовко С. Чистая прибыль LinkedIn в 2013 году возросла на 24 %, до $26,77 млн // IT Expert (http://itexpert.org.ua/rubrikator/item/33799-chistaya-pribyl-linkedin-v-2013-godu-vyrosla-na-24-do-2677-mln.html). – 2014. – 7.02).***

***

Агентство Nielsen в своем последнем отчете сообщило о росте рынка интернет-рекламы по итогам 2013 г. (+32,4 %). В 2014 г. этот показатель значительно увеличится, особенно в России – эксперты eMarketer и Starcom MediaVest Group прогнозируют 18-процентный рост (2,370 млрд дол.). Что именно станет причиной такого роста? Cossa.ru публикует прогнозы по социальным сетям, пишет Marketing Media Review (http://mmr.ua/news/id/reklama-i-socialnye-seti-v-2014-godu-prognozy-38258/).

Instagram: рекламные сообщения станут мейнстримом

В 2014 г. Instagram, скорее всего, продемонстрирует свою силу на рынке. Почва для этого подготовлена, и маркетологи наконец начинают понимать, что могут использовать Instagram, чтобы показать себя в более привлекательном свете, считают эксперты Social Media Today.

Instagram: от селфи к историям

В статье, опубликованной на Social Media Today, Instagram называется королем соцмедиа 2014 г. Автор материала Р. Симондс говорит о том, что Instagram уже не просто приложение для фоток, это инструмент для рассказывания историй – а мы все в душе дети, мы обожаем истории. По прогнозам Р. Симондса, в 2014 г. у Instagram есть реальный шанс стать серьезным инструментом для маркетологов. Р. Симондс обращает внимание на то, что соцсети становятся «более визуальными»: взять только последний год – это же год фотографий. Посмотрите: Snapchat, Instagram, Twitter и Facebook – фотографии выходят на передний план. И у Instagram в этом явное преимущество.

Кроме того, ожидается, что с брендами начнут сотрудничать звезды и популярные пользователи Instagram. Напомним, что платформа стала самой быстрорастущей на рынке социальных сетей. В России Instagram заслужил звание «самого популярного приложения» наряду с «ВКонтакте».

Facebook: реклама на блюдечке

В 2014 г. Facebook станет лучше определять, какую рекламу нужно показывать каждому отдельному пользователю. Для этого создается специальный алгоритм, способный собрать наиболее подробную информацию, которая будет состоять из фотографий, лайков, чекинов и постов, что должно существенно увеличить результаты продаж рекламы. Кроме того, социальная сеть научится определять средний доход пользователя, что пригодится для продажи таргетированной рекламы.

В этом году Facebook наконец-то понял, как важно сообщать пользователю о самых значимых событиях в мире, а также о самых популярных темах, которые обсуждают его друзья. В результате справа от News Feed в виде списка тем появятся тренды, которые будут ранжироваться по популярности. Кроме того, каждому пользователю этот список будет подбираться персонально с учетом его интересов и друзей. На тренд можно будет нажать и посмотреть, кто из друзей на него отреагировал и о чем они говорят.

«ВКонтакте»

Что касается выхода П. Дурова из доли во «ВКонтакте», пользователи связывают опасения с тем, что начнется резкий рост рекламы и это сделает некомфортным присутствие в соцсети. (На будущее: один из способов избежать нежелательной рекламы – сменить язык профиля с русского на английский). Однако эксперты считают опасения преувеличенными. Во-первых, «ВКонтакте» сегодня занят легализацией видео, а значит, реклама появится при просмотре роликов. В частности, «ВКонтакте» предоставит возможность правообладателям самостоятельно загружать свои видео и при этом зарабатывать на рекламе в них. Защита лицензионных файлов от пиратства будет происходить с помощью специальных программных решений. Заниматься размещением рекламы будет Gazprom-Media Digital, а «ВКонтакте» предоставит все необходимые данные для таргетирования аудитории соцсети.

Расходы на рекламу во «ВКонтакте» будут только увеличиваться, рекламодатели станут здесь более активными. Причиной для этого послужит взросление аудитории – те, кто бы 15-летним пять лет назад, сегодня уже 20-летний, а значит, представляет больший интерес для рекламодателя. Каждый год рост расходов на рекламу в соцсети будет составлять 20 %, считает Д. Терехов, генеральный директор агентства «Социальные сети».

«Одноклассники»

Известно, что аудитория в «Одноклассниках» старше, чем в других соцсетях, и, как правило, это пользователи из регионов.

В Sociate мы давно пришли к формуле: соцсети – это новый телевизор. А рекламодатель должен быть в телевизоре! И если «ВКонтакте» собирает аудиторию, которая уже частично отказалась от ТВ, то «Одноклассники» собирают более консервативную публику, говорит А. Новосельский, руководитель биржи Sociate, которая в январе 2014 г. начала работать с

соцсетью. Он также добавил, что новые рекламодатели продолжат прибывать в «Одноклассники». Более того, соцсеть стала более лояльна к сообществам: в этом месяце соцсеть начала тестирование сервиса платных подарков в группах (один подарок – 20 р.).

Время, которое проводят пользователи в «Одноклассниках», также увеличится: в декабре соцсеть запустила бесплатный онлайн-кинотеатр. В настоящее время в кинотеатре доступны 30 сериалов (это 10 тыс. серий), до конца года появится еще ряд новых фильмов.

Twitter

Twitter становится похожим на Instagram и другие мессенджеры: прикрепленные к твиту изображения стали показываться автоматически и появилась возможность отправлять личные сообщения. Twitter немного сменил дизайн страницы профилей, стал более упорядоченным. В последние месяцы руководство компании заключило партнерские контракты с телеканалами CBS, BBC и A&E. Twitter также начинает сотрудничать с Comcast и Time Warner Cable. Благодаря этому, вероятно, пользователи смогут смотреть телепередачи и фильмы непосредственно через сам сервис.

Также Twitter работает над стратегией торговли, которая позволила бы пользователям непосредственно через микроблог приобретать товары. Рекламный продукт будет встраиваться в поток твитов с указанием цены и краткого описания.

Twitter все активнее работает с рекламной платформой для бизнеса. Компаниям из Канады, Великобритании и Ирландии она уже стала доступна. С ее помощью они могут самостоятельно размещать рекламные твиты. Платформа (Twitter’s self-serve advertising platform) была запущена еще в апреле 2013 г., но лишь для пользователей США. Тогда же было сделано объявление, что со временем будут подключаться и другие страны, включая Россию. Размещение рекламы теперь занимает несколько минут – все, что нужно, это учетная запись в Twitter и банковская карта. Предприниматели могут контролировать свои расходы и количество рекламных публикаций и наблюдать за статистикой.

Twitter: что ожидать в 2014 году

Бизнес-корреспондент Mashable С. Фиджэрмен изучил историю сервиса Twitter, провел исследования и сделал прогнозы о том, каким он будет в 2014 г.

В настоящее время Twitter имеет более 53 млн активных пользователей в США ежемесячно, что составляет лишь приблизительно одну пятую от общего числа интернет-пользователей в стране. Глобальный рост числа пользователей резко замедлился, причем на четверть по сравнению с результатами за прошлый год. Компания сообщила об убытках в 79 млн дол. в 2012 г. и потерю почти 134 млн за первые девять месяцев прошлого года.

Совсем недавно были предприняты попытки исправить ситуацию: в Twitter появились существенные изменения, связанные с увеличением визуального контента. Twitter, скорее всего, все же станет более наглядным и

интерактивным в этом году: больше внимания будет уделяться фотографиям, статьям, клипам и т. д. Страницы профиля меняются: теперь будет выделяться больше полезной информации. Такие меры должны привлечь рекламодателей и увеличить число пользователей и их взаимодействия друг с другом. Для этих же целей Twitter планирует масштабное расширение некоторых своих рекламных инструментов.

Тем не менее, многие из нововведений были подвергнуты критике со стороны давних и наиболее активных пользователей сервиса. Автор Mashable пишет, что «за кулисами поговаривают, что руководству очень тяжело даются решения об утверждении новых функций» и некоторые из последних свернули почти сразу же после их релиза именно в связи с негативной реакцией.

Основываясь на различных интервью с банкирами и аналитиками, автор делает предположения, что расходы Twitter будут продолжать расти в 2014 г. Есть вероятность, что получения прибыли не будет аж до следующего, 2015 г.

В декабре 2013 г. Twitter запустил редирект для малого бизнеса. Теперь онлайн-магазины смогут показывать свои рекламные сообщения тем пользователям Twitter, которые когда-либо заходили на их сайт. Таким образом компании смогут охватить и мобильную аудиторию в 2014 г. (75 % пользователей Twitter пользуются микроблогом с мобильных устройств) ***(Реклама и социальные сети в 2014 году. Прогнозы // Marketing Media Review (http://mmr.ua/news/id/reklama-i-socialnye-seti-v-2014-godu-prognozy-38258/). – 2014. – 7.02).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Социальные сети оказались бесполезны для развития аналитического мышления

Возможность использовать чужое аналитическое мышление в социальных сетях помогает давать правильные ответы, но не стимулирует собственные когнитивные способности. К такому выводу пришли ученые из США, Франции, Великобритании и Арабских Эмиратов, которые моделировали процесс принятия решений в лабораторных условиях на добровольцах. Статья с результатами опубликована в журнале Journal of the Royal Society Interface.

Исследование проходили в форме тестов на аналитическое мышление, которое добровольцы выполняли в группах. Всего в эксперименте

участвовало пять групп по 20 человек. При этом каждая из групп обладала различной социальной структурой. В контрольной группе каждый из участников был изолирован и давал ответы совершенно самостоятельно, в наиболее объединенной сети каждый из добровольцев имел возможность узнать ответы всех своих коллег. В трех остальных группах связность социальной сети была промежуточной.

Добровольцам давали пять попыток на каждый из вопросов теста, поэтому они могли скорректировать свой ответ, проанализировав ответы своих соседей по социальной сети. Оказалось, что такая возможность значительно увеличивает количество правильных ответов с каждой попыткой, так как добровольцы на основе чужих ответов понимают причины своих ошибок.

Поскольку авторы основывались на том, что аналитический подход к вопросам могут стимулировать даже слабые стимулы (это было показано ранее в серии психологических экспериментов), ученые ожидали, что консультация с соседями увеличит процент последующих правильных ответов. Это, однако, оказалось не так – тщательнее к последующим размышлениям участники подходить не стали. Другими словами, добровольцы продолжали списывать и давать правильные ответы, но это не делало их умнее.

Ранее психологи показывали, что способности к аналитическому мышлению могут быть связаны с самыми разными факторами. Так, недавно была обнаружена отрицательная корреляция интеллектуальных способностей с уровнем религиозности. В другом исследовании ученые продемонстрировали, что даже в арифметике политическая окраска вопросов способна сбивать с толку и притуплять аналитические способности ***(Социальные сети оказались бесполезны для развития аналитического мышления // InternetUA (http://internetua.com/socialnie-seti-okazalis-bespolezni-dlya-razvitiya-analiticseskogo-mishleniya). – 2014. – 8.02).***

***

Как ваша депрессия и Twitter помогают науке

В Twitter в настоящее время уже более 230 млн активных пользователей – раньше там обменивались новостными заголовками и короткими ссылками, а теперь это непрерывный поток личных переживаний миллионов людей, и серьезные исследователи вовсю используют этот поток для серьезной аналитики в области массовой психологии.

Хотите верьте, хотите нет, но на ваш утренний твит про то, какой вкусный сендвич вы только что заточили теперь плевать не всем. Точнее, на него плевать всем, кроме психологов-бихевиористов из Microsoft Research, делающих на основании бессмысленных твитов про бутерброды точные выводы о поведенческих паттернах всего прогрессивного человечества.

Как вам, например, модель искусственного интеллекта, которая предупредила бы вас о риске словить депрессию, просканировав вашу

Twitter-ленту? Или предложения психологической помощи от третьих лиц, основанные на изучении ваших твитов? Э. Хорвиц, заместитель директора редмондского отделения Microsoft Research – первопроходец научного психологического изучения Twitter, и он считает, что в ближайшем будущем подобные истории действительно могут возникнуть.

«Мы подумали – а что если создать механизм, определяющий чью-либо депрессию на основании исключительно постов в социальные сети? – говорит Э. Хорвиц. – Значительная часть людей выливает в соцсети буквально всю свою душу, и вполне легко можно представить себе систему, чувствующую перемены в настроении таких пользователей еще даже до того, как они почувствуют их сами».

По словам Э. Хорвица, они с командой разработали полностью рабочую и готовую подобную историю для Twitter, и она распознает депрессию с поразительной 70-процентной точностью. Конечно, это очень далеко от идеала – 30 % людей с депрессией система не распознает; вдобавок к этому, есть и обратная погрешность – в 10 % случаев система диагностировала депрессию у совершенно счастливых людей.

Всего исследовательская команда занималась 476 пользователями Twitter, и у 171 из них они нашли депрессию. Каждый аккаунт исследовался со всех сторон – все твиты за прошедший год, лексика твитов, их частота, упоминания медикаментов, стимуляторов, алкоголя; всего компьютер изучил более чем 2 млн твитов. Далее все было уже проще – достаточно было сравнить твиты «депрессивных» пользователей со здоровыми и понять, какие именно твиты выдают первых, и вот машина уже раздавала диагнозы с неплохой точностью.

Вот, например, самые очевидные такие депрессивные твиты:

«Хорошо снова выйти на работу – меньше времени останется на депрессию, булимию и печальные фильмы»

«Хочу, чтобы кто-нибудь обнимал меня и не отпускал, когда мне становится грустно»

«“Ты ок?” Я? Да. Я понимаю, что я безнадежно расстроена, разбита, и ничто мне уже не поможет, и это ок. Я ок. Но я не в порядке!»

Разумеется, не у всех пользователей все так уж на ладони. В таких случаях нужно смотреть на множество факторов – количество твитов в день, время отправления твитов, частота ретвитов других пользователей и лексическая составляющая твитов. Например, пользователь постящий что-то в промежутке между 2 ночи и 6 утра очевидно не может уснуть, и очевидно что это из-за депрессии – здоровые люди при бессоннице не открывают Интернет, а считают овец.

Особо интересен лексический момент – о депрессии могут свидетельствовать как и очевидные слова вроде «озабоченность», «жесткий», «аппетит», «суицид», «тошнота», «сонливость», «усталость», «невроз», «зависимость», «атака», «проявление» и «сон», так и неочевидные: «она», «он», «девушка», «игра», «мужчины», «дом», «радость», «любимый»,

«желание», «терпимость», «борьба», «удивительный», «любовь», «забота», «песня» и «фильм».

«Громкость» твитов тоже немаловажна, как и количество взаимодействий – в депрессии человек пишет меньше твитов и реже ретвитит других пользователей, подсознательно обозначая свою социальную дезинтеграцию. Конечно, это не значит, что любой человек, пишущий в 4 часа ночи твит со словами «дом» и «усталость» непременно находится в подавленном состоянии – рассматривать такие случаи всегда надо с учетом общей картины за год.

Команда Э. Хорвица заметила еще одну интересную деталь – многие твиты-индикаторы депрессии были написаны как твиты-реакции на определенные шокирующие и печальные мировые или местные события. Из этого единичного наблюдения вполне может вырасти отдельное большое исследование, если не целая наука – как именно происходящие не с нами глобальные события отправляют нас в глубокую и затяжную печаль, что с этим делать и как с этим бороться ***(Как ваша депрессия и Twitter помогают науке // Advertology.Ru (http://www.advertology.ru/article120579.htm). – 2014. – 28.01).***

***

Популярность «мемов» в социальных сетях сравнили с распространением эпидемий

Исследователи установили, что соревнование «мемов» и их борьба за внимание пользователей создаёт в социальных сетях критическое состояние, что, в свою очередь, объясняет природу лавинообразного роста популярности «мемов», пишет Блог Imena.UA (http://www.imena.ua/blog/web-users-like-financial-players).

Чтобы разобраться, почему одна картинка, фотография или шутка становится популярной, а десятки других – нет, исследователи из Американского физического общества смоделировали обобщённую социальную сеть, напоминающую сервис микроблогов Twitter.

В модели искусственной сети каждый из пользователей может создать новый «мем» или передать увиденное на чьей-то другой странице изображение тем, кто является его подписчиком.

Исследователи установили, что при наличии достаточно большого количества «мемов» между ними возникает конкуренция за внимание пользователя, и эта конкуренция сильно влияет на то, как дальше развивается «жизнь» определённого поста.

За счёт усиления конкуренции достигается критическое состояние во всей сети, в котором любая случайность провоцирует лавинообразный поток популярности. После прохода «лавины» система самостоятельно опять возвращается в критическое состояние.

Подобные системы были предсказаны ещё в 1987 г. физиками из Брукхейвенской лаборатории, США. Системы функционируют и в других

сферах: на финансовых рынках, при распространении эпидемий, в некоторых видах электрической активности в головном мозгу человека ***(Популярность «мемов» в социальных сетях сравнили с распространением эпидемий // Блог Imena.UA (http://www.imena.ua/blog/web-users-like-financial-players). – 2014. – 4.02).***

Маніпулятивні технології

В Facebook в группе «УПА» появилось сообщение, в котором говорится, что некая Украинская повстанческая армия берет на себя ответственность за убийство милиционера 24 января 2014 г. и предупреждает других милиционеров о последствиях, если те не примут условия митингующих.

«УПА берет на себя ответственность за убийство милиционера 24.01.2014 г. рядом с общежитием “Беркута”. Этот поступок является местью за убийства протестующих, пытки заключенных и издевательства над ними», – сказано в тексте.

Это же сообщение дублируется в группе Повстанческой армии в сети «ВКонтакте».

Повстанцы УПА требуют от милиции «сложить оружие или перейти в подчинение Революционного Майдана, освободить всех политзаключенных (В. Запорожец, “Васильковские террористы”, А. Билецкий, защитники Рымарской, В. Применко, семья Павличенко, “мелитопольские поджигатели”, “нежинские робингуды”, “сумские художники”, Я. Притуленко, А. Дзиндзя, В. Смалий, В. Кадура, А. Онороженко и другие, задержанные в январе 2014 г., список которых ежедневно пополняется)».

Также авторы сообщения требуют арестовать или позволить митингующим арестовать В. Януковича, Н. Азарова, В. Захарченко, В. Пшонку, О. Якименко, А. Клюева, О. Лукаш и др.

В случае невыполнения требований авторы сообщения грозятся убивать по несколько милиционеров в неделю.

«В случае невыполнения нашего ультиматума мы будем вынуждены продолжить повстанческо-партизанскую борьбу, убивая по несколько работников милиции еженедельно. Мы не будем принимать участие в открытом противостоянии, мы будем вести борьбу подпольно».

«Если наш ультиматум останется без внимания со следующей недели каждый милиционер, в форме или без нее станет потенциальной целью для УПА… Мы будем убивать милиционеров в случае продолжения ими преступной деятельности (служение преступному режиму в любой форме само по себе уже является преступлением перед украинским народом)».

Также автор текста подчеркнул, что даже в случае разгона Евромайдана их деятельность не прекратится.

Напомним, 24 января в Голосеевском районе Киева огнестрельным ранением был убил 28-летний старший сержант ГСО. Следствие

рассматривает версию мести правоохранителю со стороны протестующих ***(В группе УПА в Facebook неизвестные опубликовали прямую угрозу в адрес милиционеров // Robinzon.TV (http://robinzon.tv/news/v_gruppe_upa_v_facebook_neizvestnie_opublikovali_pryamuyu_ugrozu_v_adres_militsionerov_0). – 2014. – 27.01).***

***

Абоненты провайдера «Воля» в Киеве и Львове сообщают о временном ограничении доступа к социальной сети Facebook. Зафиксировано десятки обращений, ряд которых проверены журналистами «Комментариев».

С редакцией proIT также связались несколько киевских абонентов «Воли», которые подтвердили трудности с доступом к соцсетям.

Так, 29 января в период с 15:00 до 18:00 Facebook и LiveJournal у абонентов «Воли» открывались с трудностями или не открывались вовсе. Абоненты подчеркивают, что сбой носил избирательный характер – к соцсетям доступ был ограничен, в то время как другие сайты открывались без проблем ***(Абоненты «Воли» не могут зайти в Facebook // proIT (http://proit.com.ua/news/telecom/2014/01/30/094142.html). – 2014. – 30.01).***

***

Соціальна мережа «ВКонтакте» блокуватиме спільноти, які цілеспрямовано спекулюють на темі Євромайдану.

Як повідомив прес-секретар українського офісу «ВКонтакте» В. Леготкін, у першу чергу це стосується спільнот, які змінили свою тематику та назву, додавши в них слова, повязані з революційними подіями в Україні. «Це серйозне порушення зі сторони адміністраторів сторінок. Такі речі є нечесними по відношенню до користувачів, які підписувались на одну групу, а опинилися читачами зовсім іншої», – пише В. Леготкін.

У російській спільноті SMM-спеціалістів наводиться цікавий випадок, де паблік для жінок змінив тематику на майданівську з метою швидкого приросту кількості підписників та змінив адресу на http://vk.com/euromaiidan. Техпідтримка ж, у свою чергу, пообіцяла втручатись лише у випадку грубих порушень правил – наприклад, під час поширення персональної інформації учасників протестів ***(«ВКонтакте» блокуватиме спільноти, які спекулюють на темі Євромайдану // UkrainianWatcher (http://watcher.com.ua/2014/01/31/vkontakti-blokuvatyme-spilnoty-yaki-spekulyuyut-na-temi-yevromaydanu/). – 2014. – 31.01).***

***

В Інтернеті з’явився черговий клон інтернет-видання «Українська правда». Сайт з аналогічною назвою, розташований за адресою pravda.biz.ua.

На сайті pravda.biz.ua розміщено реальні новини з «Української правди» та відверті повідомлення з дезінформацією. Дизайни сайтів

ідентичні, на клонованому ресурсі навіть відображається та сама реклама, як і на справжній «Українській правді».

Як повідомила «Телекритиці» головний редактор «Української правди» О. Притула, видання в черговий раз поскаржиться на клон у Google своєму хостинг-провайдеру та проситиме читачів бути уважними, переходячи за посиланнями на ресурси з назвою «Українська правда».

Як повідомлялося, наприкінці серпня з'явився сайт «Українська кривда», що повністю копіює дизайн інтернет-видання «Українська правда». Контент «Української кривди» здебільшого включає повідомлення, які стосуються ЗМІ, піару та політичних технологій та ніби мають на меті боротись із замовними матеріалами.

Також з кінця серпня в різних регіонах України почала поширюватися газета з назвою та логотипом інтернет-видання «Українська правда».

На початку вересня редакція інтернет-видання «Українська правда» звернулася до правоохоронних органів з приводу випуску фальшивої газети з логотипом видання та запуску онлайн-двійника «Українська кривда». Представники видання розцінюють такі дії як такі, що спрямовані на дискредитацію «Української правди»: «Розрахунок – неуважний або непоінформований читач має сприймати за чисту монету будь-які нісенітниці, які виходять на цих ресурсах або під нашим брендом, або в нашому дизайні».

18 листопада почав оновлюватися ще один клон інтернет-видання «Українська правда», сайт з аналогічною назвою, розташований на домені ukrpravda.ua ***(В Інтернеті знову з'явився клон «Української правди» // Західна інформаційна корпорація (http://zik.ua/ua/news/2014/01/31/v_interneti_znovu_zyavyvsya_klon_ukrainskoi_pravdy_457426). – 2014. – 31.01).***

***

Фальшива сторінка в соцмережі Twitter виконуючого обов'язки прем'єра України С. Арбузова була створена італійським журналістом Т. Дебенедетті, який у грудні минулого року поширив фейкову новину про смерть М. Горбачова, пише «Кореспондент» (http://ua.korrespondent.net/ukraine/politics/3300744-feikovu-storinku-arbuzova-u-Twitter-stvoryv-zhurnalist-yakyi-pokhovav-horbachova).

Раніше в соцмережі з'явився акаунт С. Арбузова. В одному з твітів користувач під ніком @ArbuzovUA повідомив про те, що Президент В. Янукович готується подати у відставку через проблеми зі здоров'ям. Проте прес-секретар С. Арбузова повідомив, що акаунт у Twitter не належить в. о. прем'єра.

Про те, що сторінка є фальшивою, журналіст написав в одному з твітів акаунта @ArbuzovUA. «Цей обліковий запис обман, створений італійським журналістом Т. Дебенедетті», – написав автор твіту.

У грудні минулого року Т. Дебенедетті поширив фейкову новину про смерть М. Горбачова. Тоді італієць зареєстрував фальшивий акаунт міністра закордонних справ Німеччини Франка-Вальтера Штайнмаєра, у якому і повідомив «новину».

Нагадаємо, у січні в Інтернеті з'явилася фейкова відповідь співачки Руслани на звинувачення нардепа від Свободи І. Фаріон ***(Фейкову сторінку Арбузова у Twitter створив журналіст, який «поховав» Горбачова // Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3300744-feikovu-storinku-arbuzova-u-Twitter-stvoryv-zhurnalist-yakyi-pokhovav-horbachova). – 2014. – 3.02).***

***

Українські бренди активно накручують лайки та інші види активностей у Facebook через спеціалізовані біржі. Інформацію про дослідження однієї з таких бірж виклав у себе у Facebook І. Давидюк, фахівець із SMM.

За його інформацією, на біржі smmok-fb.ru користувачам за гроші пропонують лайкнути сторінки брендів чи окремі пости таких брендів. Вартість дії коливається в межах 0,15–0,3 російських рублів – близько 4–6 українських копійок.

«До переліку увійшли сторінки/профілі відомих компаній та особистостей», – пише І. Давидюк. Зокрема, life, King's Bridge, Cider Somersby Ukraine, – накручують лайки до постів. В. Медведчук та «Кияни за Віктора Пилипишина» – додають друзів. Бренди Neséaf3in1, Ukraine Смартфони LG, LG Electronics Blog, Вий 3D / VIY 3D, Life, Чудо-Чадо, Chio.Ukraine, ARGO, Alfa-Bank Ukraine – накручують шанувальників до своїх сторінок ***(Українські бренди активно накручують лайки у Facebook через спеціалізовані біржі // UkrainianWatcher (http://watcher.com.ua/2014/02/03/ukrayinski-brendy-aktyvno-nakruchuyut-layky-u-facebook-cherez-spetsializovani-birzhi/). – 2014. – 3.02).***

***

Интернет-троллинг превратился в индустрию

Тема Евромайдана уже несколько месяцев не сходит с главных страниц большинства украинских интернет-ресурсов. И если основными инструментами власти для борьбы с несогласными на центральных улицах Киева и многих украинских городов были бойцы «Беркута», внутренних войск, «титушки», то в Интернете основной атакующей провластной силой стали профессиональные тролли. В результате десятки крупнейших порталов были вынуждены существенно ужесточить политику публикации комментариев к своим статьям и новостям, в частности, была включена премодерация, а на некоторых ресурсах возможность комментариев была и вовсе отключена.

Углубление политического кризиса в стране внезапно спровоцировало повышенный спрос на услуги политтехнологических «агентств», которые

давно и успешно используют такой инструмент черного пиара, как интернет-троллинг.

Как сообщил proIT бывший сотрудник крупного маркетингового агентства, пожелавший остаться инкогнито, львиная доля всего негативного политического троллинга проходит через так называемые «агентства». Работа таких агентств давно налажена и обкатана, они обладают огромными прокачанными ботнетами, фейковыми аккаунтами в наиболее популярных соцсетях, а также базой контактов троллей-фрилансеров, выполняющих механическую часть работы. Такие агентства работают годами, «у руля» стоят те же люди, что и по время прошлых президентских выборов.

Несмотря на то, что с началом Евромайдана «агентства» наняли дополнительные руки для механической работы, не существует постоянного «набора в ряды троллей», подобно тому, как через Facebook приглашают «титушек» в Мариинский парк. Рынок услуг интернет-троллей невелик, там нет сотен и тысяч рабочих мест. Поэтому профессиональным сетевым троллингом в Украине занимаются не тысячи человек, как это может показаться исходя из создаваемого «информационного фона», а всего несколько десятков.

Но все-таки наём новых «контент-менеджеров» иногда происходит, их нанимают либо непрофессионалы, либо те, кто хочет сэкономить. Дело в том, что львиную долю в цене «агентства» составляет профессиональный политтехнолог, услуги которого стоят иногда дороже, чем целая армия троллей, выполняющих механическую часть работы. Те, кто не могут его себе позволить, ищут «контент-менеджеров» в обход агентств и сами формулируют им задачи. Результат такой «самодеятельности» выглядит грубо, топорно и узнаваемо.

По словам О. Хаврука, технического директора интернет-портала Comments.ua, на полупрофессиональном уровне в качестве исполнителей ручной работы привлекают студентов. «Им дается разнарядка – список сайтов, тем, месседжей, которые необходимо “вкидывать” и они работают. Как правило, они тратят 3–5 часов в день. Обычно они направлены не на дискуссию, а на прямой “вброс” нужной информации. На Comments.ua троллей мы отслеживаем по IP-адресу: если несколько пользователей под разными именами постят провокационные тексты в одном ключе, понятно, что это один и тот же человек».

О. Хаврук говорит, что заказчик ведет учет объема и качества выполненной работы. Самый простой способ – исполнитель ведет таблицу в Excel, где отображен адрес страницы, на которой сделан пост и имя автора или сам текст сообщения. Заказчик выборочно проверяет, соответствует ли представленная информация действительности.

В роли заказчика выступают PR-структуры, нанятые для сопровождения определенной политической партии, депутата или политика, а интернет-троллинг выступает в роли дополнительной услуги. «Хотя заказчик может обратиться к исполнителю практически напрямую. Если это

какой-то мелкий депутат, и он хочет отработать конкретно по себе, то он может заказать такие услуги через своего помощника», – говорит О. Хаврук.

При этом он отмечает, что в любых крупных информационных кампаниях, будь-то евромайдан, президентские или парламентские выборы, всегда работает несколько параллельных команд интернет-троллей. По словам техдиректора портала Comments.ua, в случае с Евромайданом явно видно, что действует несколько команд: «Есть явная засветка России. Мы это видим на страницах ресурса Comments.ua, там стараются отписаться люди, у которых даже в профилях указано, что они из Москвы, Санкт-Петербурга и они рассуждают о том, “как эти западенцы всех задолбали, сколько можно бандеровцев кормить”. Хотя, казалось бы, о чем они могут говорить, если даже не в этой стране живут».

Между тем, несмотря на пафосность и важность основной задачи интернет-троллей – формирования общественного мнения – работа исполнителей не считается квалифицированной и платят за нее не так уж и много. Дневной заработок может колебаться в пределах 10–30 дол., и это при том, что всегда существует большая вероятность «кидка» со стороны заказчика. Впрочем, исполнители перестраховываются и требуют предоплаты в размере 50 %.

Если же речь идет об услугах интернет-троллинга на профессиональном уровне – создание и сопровождение имиджа организации, или поддежание заданного градуса общественного мнения по определенному вопросу – заказчик должен быть готов раскошелиться уже не на сотни долларов, а на десятки тысяч. Впрочем, и эффективность будет несопоставимо выше – «агентства», обеспечивающие выполнение крупного заказа, обладают сформированной структурой и профессиональной командой с четким распределением обязанностей. По словам «ветерана» одного из «агентств», которое стартовало еще в 2008 г. под президетские выборы, иерархия исполнения выглядит в общих чертах так:

• Представитель заказчика. Формулирует «заказ» и обеспечивает финансирование. Как правило, аппаратчик уровня помощника нардепа или пресс-секретаря.

• Политтехнолог. Декомпилирует и «переваривает» задание, зачастую сформулированное «по понятиям» («чтоб все было в шоколаде»), определяет болевые точки целевой аудитории. Как правило, профессионал высокого уровня. Один политтехнолог может готовить стратегию, которая затем используется одновременно несколькими «агентствами». Именно с подачи политтехнологов в массы был вброшен термин «майдауны», постулат о том, что жители западных областей – все поголовно «бандеровцы», а также раскрутка идеи федерализации. Зарплата – десятки тысяч долларов.

• Координатор. Самая трудоёмкая профессия в цепочке. Его задача – распределить работу между исполнителями механической части, проконтролировать её исполнение, раздать гонорары и отчитаться перед заказчиком. Как ни странно, чаще всего эту работу выполняют люди, не

связанные с высокими технологиями. Здесь в первую очередь требуются навыки организатора производства и умение истребовать результат. Фиксированной ставки нет, кормится комиссионными от армии подчиненных, фактический заработок – несколько тысяч долларов.

• Программист. Создает интерфейс для автоматизированной рассылки шаблонных комментариев по соцсетям и Twitter, а также под статьями в онлайн-СМИ, где комментирование возможно без авторизации и проверки подлинности. Кроме этого, интерфейс в онлайн-режиме (через RSS) уведомляет контент-менеджеров о появлении новых публикаций в ключевых СМИ и автоматически «накручивает» рейтинги негативных комментариев, используя подконтрольные аккаунты в соцсетях. За создание постинг-интерфейса с нуля получает 2–3 тыс. дол. разово, за поддержку – около 1 тыс. дол. в мес.

• Копирайтер. Отталкиваясь от стратегии политтехнолога, пишет шаблоны универсальных «речёвок», подходящих для комментирования любой статьи, независимо от содержания. Должен обладать навыками психолога. Как правило, сотрудник рекламного или маркетингового агентства, не брезгующий подобной «халтурой». Получка разовая, около 1 тыс. дол. за пакет темников.

• Контент-менеджеры – собственно тролли. Исполнители механической части работы – подбирают из темника и вручную публикуют шаблонные комментарии там, где это невозможно сделать автоматически, поддерживают «дискуссию» где требуется, накручивают рейтинги, делают скриншоты о выполненной работе. Зарплата в среднем 300–400 грн в день. Одновременно работает 2–3 человека на раскрутку 1 персоны, и 10–15 под специальную «долгоиграющую» тему.

• Ботнет. Покупается на хакерском черном рынке. Предложение состоит из двух раздельных частей: 1) пакет угнанных или специально созданных аккаунтов в соцсетях, от имени которых публикуются комментарии;

2) армия инфицированных компьютеров, с IP-адресов которых происходит скрытая рассылка комментариев, с целью обхода спам-фильтров и бана на атакуемых ресурсах. Цены очень разные: от нескольких центов за свежесозданный пустой аккаунт (100 % бот), до 10 дол. за угнанный «прокачанный» аккаунт с живыми друзьями/фолловерами.

Итого, поддержка уже налаженного троллинг-ботнета, раскручивающего конкретную персону/организацию, обходится в 50–60 тыс. грн в месяц. Крупный ботнет, работающий на специальную тему или на формирование и поддержание заданного общественного мнения, обходится в несколько сотен тысяч гривен ежемесячно. Для крупных акций может быть привлечено несколько «агентств» (независимых ботнетов).

Таким образом, интернет-троллинг уже давно перестал быть просто забавой отдельных личностей, заинтересованных в большей узнаваемости, публичности и эпатаже. Благодаря современным технологиям массовый

постинг провокационных комментариев превратился в вид бизнес с оборотами в десятки и сотни тысяч долларов. И этот инструмент пользуется стабильным спросом как со стороны рядовых депутатов и чиновников, так и со стороны тайных и влиятельных сил соседних стран ***(Интернет-троллинг превратился в индустрию // proIT (http://proit.com.ua/article/internet/2014/02/05/210333.html). – 2014. – 5.02).***

***

Мошенники создают в «ВКонтакте» контакты-двойники, с которых просят «друзей» перевести денег электронным платежом, по результатам проведенного Digit.ru мониторинга соцсетей.

В социальных сетях заметен всплеск жалоб пользователей на попытки мошенников взять в долг у сетевых друзей с аккаунтов-двойников пострадавшего. Сам способ довольно старый: создается страница, на которую копируется фотография, имя и личная информация какого-либо пользователя. Затем его друзьям рассылается просьба о переводе денег, например на карту или Qiwi-кошелек.

«Да, мы фиксируем всплеск подобного мошенничества в последние дни. Поддержка завалена вопросами. Есть даже просьбы об удалении подобных страниц в других социальных сетях. Пока единственный совет пользователям – проводить профилактическую работу с друзьями», – сообщил Digit.ru пресс-секретарь «ВКонтакте» Г. Лобушкин ***(«ВКонтакте» фиксирует всплеск мошенничества с аккаунтами-двойниками // InternetUA (http://internetua.com/vkontakte--fiksiruet-vsplesk-moshennicsestva-s-akkauntami-dvoinikami). – 2014. – 5.02).***

Зарубіжні спецслужби і технології «соціального контролю»

Популярнейшая в мире игра для мобильных телефонов и планшетов Angry Birds используется спецслужбами США и Британии для сбора персональных данных, утверждает бывший сотрудник американских спецслужб Э. Сноуден.

Речь также идет о целом ряде других популярных мобильных приложений.

Американское Агентство национальной безопасности (АНБ) по-прежнему настаивает на том, что не интересуется личными данными, за исключением особо оговоренных случаев, когда это необходимо в интересах внешней разведки. «Любое утверждение, что деятельность АНБ в области внешней разведки ориентирована на сбор информации о рядовых американцах через их смартфоны и социальные сети, не соответствуют истине», – говорится в заявлении АНБ.

Несмотря на это, материалы, опубликованные изданиями New York Times, ProPublica и Guardian, свидетельствуют о том, что АНБ и британский Центр правительственной связи (ЦПС) с 2007 г. совместно разрабатывают

способы получения доступа к информации из приложений для мобильных телефонов и планшетов.

Масштабы сбора данных пока неясны.

Данные о пользователях собираются из разнообразных картографических приложений, игр и социальных сетей приблизительно теми же методами, какие используются для перехвата мобильного трафика в Интернете и текстовых сообщений SMS.

Более того, опубликованные документы свидетельствуют о том, что спецслужбы США и Великобритании все больше убеждаются в важности информации, которую можно получить от мобильных приложений. «Фактически речь идет о том, что любой человек, включающий у себя на смартфоне Google Maps, автоматически начинает работать на ЦПС», – говорится в одном из секретных документов, датируемых 2008 г.

Еще в одном докладе ЦПС 2012 г. излагаются принципы использования информации, которую можно получить от приложения Angry Birds на платформе Android. В настоящее время эта видеоигрушка о птицах и свиньях является, вероятно, самым популярным мобильным приложением – его скачивали 1,7 млрд раз.

Британская спецслужба заявила, что не комментирует вопросы внешней разведки, но настаивает на том, что ее деятельность не выходит за рамки ее полномочий.

Другой документ – уже американской АНБ – описывает так называемый «золотой слиток» – идеальный сценарий получения информации аналитиками АНБ из всех возможных источников, включая социальные и прочие сети, к которым подключается мобильное устройство, загружаемые в него документы, посещаемые пользователем интернет-сайты и списки контактов, друзей, «френдов» и «фолловеров».

Помимо уже упомянутых приложений, спецслужбы активно интересуются также фотосайтом Flickr, социальной сетью для любителей кино Flixster и, естественно, мобильным приложением Facebook ***(Angry Birds сливает персональные данные // Главное™ (http://glavnoe.ua/news/n163046). – 2014. – 29.01).***

***

В то время как сотрудники АНБ прослушивали телефоны, читали почту и отслеживали данные игроков в Angry Birds, их британские коллеги также не сидели без дела. Центр правительственной связи, одна из спецслужб Великобритании, отслеживал пользовательские данные с сервиса YouTube, а также просматривал данные о пользователях, размещавших контент с видео-сервиса на своих страницах в Facebook, Blogger или Blogspot.

Агенты ЦПС могли физически подключаться к глобальным линиям связи, по которым шли данные YouTube, и выделять из общего потока информацию о нужном контенте или пользователе. Об этом говорится в документах, которые предоставил NBC News Э. Сноуден. Данная программа

получила название Squeaky Dolphin, что в дословном переводе означает «Скрипучий Дельфин». Это словосочетание имеет несколько значений.

Цель программы заключалась в том, чтобы отслеживать изменения в социальных сетях в контексте мировых событий, чтобы дать возможность спецслужбам спрогнозировать вероятные антиправительственные акции. В последнее время посредством социальных сетей радикально настроенные граждане координировали свои акции, которые нередко заканчивались погромами. Руководство же сервисов далеко не всегда соглашалось сотрудничать с правительствами.

Что касается Великобритании, то местные чиновники уже выступили с заявлением, в котором говорится, что сбор данных осуществлялся в соответствии с законодательством. Впрочем, как заявили представители Google и Facebook, сбор незашифрованных данных происходил без их ведома, и разрешения на проведения подобных операций они никому не давали ***(Британское правительство отслеживало пользователей в соцсетях с помощью «Скрипучего дельфина» // IT Expert (http://itexpert.in.ua/rubrikator/item/33544-britanskoe-pravitelstvo-otslezhivalo-polzovatelej-v-sotssetyakh-s-pomoshchyu-skripuchego-delfina.html). – 2014. – 29.01).***

***

Суд по контролю за внешней разведкой США (U.S. Foreign Intelligence Surveillance Court) разрешил крупным IT-компаниям обнародовать информацию о правительственных запросах, касающихся персональных данных. Об этом 27 января сообщает Agence France-Presse.

Согласно решению суда, ряд крупнейших IT-компаний теперь сможет публиковать приблизительные данные о количестве запросов со стороны американских спецслужб, а также о количестве аккаунтов, по которым правительство запрашивало информацию.

Кроме того, компании получили возможность информировать общественность о количестве критериев, по которым запрашивается информация. Сами критерии обнародованы не будут.

О том, что компании получат больше возможностей по обнародованию фактов запросов данных со стороны спецслужб, 17 января 2014 г. заявил президент США Б. Обама.

Компании Microsoft, Google, Yahoo, Facebook и LinkedIn обратились в суд по контролю за внешней разведкой США после публикаций о деятельности Агентства национальной безопасности (АНБ). Целью иска было получение права на публикацию подробной статистики запросов пользовательской информации со стороны спецслужб. Право на публикацию общей статистики компании получили летом 2013 г. Информация о слежке за пользователями Интернета появилась в СМИ в июне 2013 г. благодаря бывшему сотруднику АНБ Э. Сноудену, передавшему журналистам секретные документы агентства ***(IT-компаниям позволили раскрывать***

данные о запросах спецслужб // InternetUA (http://internetua.com/IT-kompaniyam-pozvolili-raskrivat-dannie-o-zaprosah-specslujb). – 2014. – 28.01).

***

За первые шесть месяцев 2013 г. компании Microsoft, Google, Facebook, а также Yahoo! предоставляют данные десятков тысяч пользователей по запросам спецслужб. Об этом говорится в материалах, опубликованных компаниями 3 февраля.

С января по июнь 2013 г. спецслужбы обращались к Microsoft от 15 до 16 тысяч раз, в Google – от 9 до 10 тыс., Facebook – от 5 до 6 тыс. Самое большое количество обращений, – более 30 тыс., – было направлено в Yahoo!.

В статистику попали только секретные запросы ФБР и Агентства национальной безопасности (АНБ) США, одобренные судом на основании закона «О контроле за деятельностью служб внешней разведки» (Foreign Intelligence Surveillance Act, FISA).

Американские IT-компании смогли обнародовать информацию о запросах спецслужб в результате договоренности с министерством юстиции. Эти сведения компаниям разрешили разглашать только с задержкой в полгода, при этом имена пользователей и ведомств, направивших обращение, сообщать было запрещено.

Компании отметили, что такого уровня раскрытия информации недостаточно. Так, в Google подчеркнули, что деятельность систем наблюдения должна быть более прозрачной, чтобы каждый мог увидеть, как функционируют законы, разрешающие слежку за интернет-пользователями, и служат ли они общественным интересам ***(Microsoft, Google и Facebook рассказали о запросах спецслужб США // DailyUA (http://www.daily.com.ua/news/10/2014-02-187351.html). – 2014. – 4.02).***

***

Руководство Twitter раскритиковало соглашение о раскрытии статистики сотрудничества со спецслужбами, заключенное крупнейшими американскими IT-компаниями с правительством страны. Сообщение об этом 6 февраля появилось в официальном блоге соцсети. Представители Twitter заявили, что будут добиваться от властей права публикации более подробной статистики запросов со стороны разведывательных ведомств.

В Twitter отметили, что новые договоренности с правительством США дают интернет-компаниям возможность публиковать лишь общие сведения о количестве запросов пользовательской информации. «С одной стороны, это безусловно шаг в правильном направлении. С другой, обнародование итогового количества таких запросов не дает пользователям реального представления относительно того, какие сведения и в каких объемах мы раскрываем», – отметили в компании.

Руководство социальной сети заявило, что планирует в ближайшее добиться права публикации конкретных цифр по запросам, касающимся национальной безопасности, а также по запросам, связанным с деятельностью разведывательных служб (в частности, Агентства национальной безопасности США, АНБ). Кроме того, в Twitter сообщили, что будут просить власти о праве сообщать об отсутствии запросов определенного типа.

Ранее администрация Twitter также завела отдельный официальный микроблог @policy, посвященный политике конфиденциальности сервиса. Предполагается, что аккаунт будет использоваться для более подробного и оперативного освещения политики компании в области защиты персональных данных ***(Twitter пообещал добиться большей прозрачности в отношениях со спецслужбами // InternetUA (http://internetua.com/Twitter-poobesxal-dobitsya-bolshei-prozracsnosti-v-otnosheniyah-so-specslujbami). – 2014. – 7.02).***

***

Компания Facebook выпустила обновление мобильного клиента под Android. Новая версия требует дополнительные разрешения, в том числе разрешение читать текстовые сообщения SMS или MMS.

Зачастую пользователи просто нажимают «Принять» и соглашаются предоставить необходимые разрешения, даже не читая текст. В случае с приложением Facebook, пожалуй, лучше воздержаться от обновления.

Как и другие социальные сети, Facebook зарабатывает деньги на показе таргетированной рекламы. Например, рекламу фототехники Nikon можно продавать дороже, если показывать ее только пользователям, которые увлекаются фотографией. Сканирование текста SMS позволяет извлекать ключевые слова, по которым можно еще эффективнее подбирать целевую рекламу.

Кроме текста SMS мобильное приложение Facebook имеет доступ к адресной книге, информации о звонках, списку установленных приложений и проч. Программа может скачивать файлы без уведомления, добавлять новые контакты в адресную книгу и изменять информацию в ежедневнике. Компания заверяет, что доступ к SMS нужен только для подтверждения телефонного номера, привязанного к аккаунту Facebook, с помощью автоматического считывания кода, который присылают по SMS ***(Facebook теперь читает ваши SMS // InternetUA (http://internetua.com/Facebook-teper-csitaet-vashi-SMS). – 2014. – 29.01).***

***

В России говорят, что ресурсов, призывающих к насилию над русскими, достаточно много не только в Украине, но и в самой РФ, причем, большая часть из них расположена на страницах Livejournal, Facebook и «ВКонтакте».

Член Общественной палаты РФ, президент Фонда исследования проблем демократии М. Григорьев направил письмо в Генпрокуратуру России с просьбой ограничить доступ к интернет-ресурсам, содержащим «человеконенавистнические идеи нацистского характера», исходящие с Майдана, пишет «Зеркало недели».

«По Майдану и в украинской сети распространяется множество русофобских материалов с плакатами Степана Бандеры и т. д. Идет большая кампания, информационно поддержки его идей», – заявил он.

Эксперт обратил внимание на то, что часть подобной информации находится в Livejournal, Facebook и «ВКонтакте». «Это не только русофобские, но совершенно неприкрытые человеконенавистнические идеи нацистского характера, – тексты, коллажи и карикатуры. Например, под знаменем украинской партии "Свободы", националистической, если не пронацистской организации, красуется надпись "Мы идем на Москву! "», – пояснил политолог.

Собеседник указал, что среди популярных изображений на русоненавистнических, но при этом российских страничках – свинья на фоне триколора РФ, с которой призывают расправиться, а также любые коллажи с пропагандой насилия и ненависти к нашей стране.

Кроме того, на других источниках, помимо призывов к массовым беспорядкам и осуществлению экстремистской деятельности, отмечаются яркие выражения симпатии некоторых украинцев к НАТОвским войскам и заявления о поддержке.

«Вся эта информация абсолютно противоречит ФЗ от 28 декабря 2013 г. № 398-Ф «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации", поэтому я направил письмо в Генпрокуратуру с просьбой ограничить доступ к данным источникам», – заявил М. Григорьев ***(В России из-за Майдана могут ограничить доступ к Livejournal, Facebook и «ВКонтакте» // Новости Донбасса (http://novosti.dn.ua/details/217580/). – 2014. – 5.02).***

***

Крупнейшая социальная сеть РФ может стать на путь усиления ментального железного занавеса

Продажа П. Дуровым своей части акций «ВКонтакте» неожиданностью, мягко говоря, не стала – об этом говорили целый год. Назывались даже ориентировочные сроки сего события – к примеру, сразу после Олимпиады. И вот, ожидаемое свершилось. 12 % акций П. Дурова ушли к И. Таврину из «Мегафона» (читай – к А. Усманову), превратившись вместе с ранее накопленными в 52-процентный контрольный пакет.

Сам П. Дуров утверждает, что, даже оказавшись без акций, все равно останется на руководящих постах в компании и к его слову новые акционеры будут по-прежнему внимательно прислушиваться, поскольку он понимает «глубинные процессы».

Впрочем, судя по широкому и бурному потоку откровенно заказных публикаций даже в весьма уважаемых российских СМИ на тему «Дуров – психически неуравновешенный кодоваятель мелкого масштаба», сбыться этим надеждам творца «ВКонтакте» вряд ли суждено – что продано, то продано.

О крупных переменах в управленческих структурах косвенно свидетельствует и тот факт, что следом за П. Дуровым «ВКонтакте» покинул и вице-президент компании И. Перекопский. На его место прибыла «усмановская гвардия» в лице бывшего руководителя ИД «Коммерсант» Д. Сергеева. Причины рокировки назывались разные – то ли проблемы с разделом выручки, то ли подчиненность дата-центров компании «неправильным» офшоркам. Но все это выглядело скорее поводом.

По-видимому, никто не заинтересован в каких-либо коренных изменениях в работе соцсети. Резать курицу, несущую не только золотые яйца, но и стяг одной из наиболее успешных российских IT-компаний и может похвастаться 60 миллионами ежедневной аудитории, естественно, никто не хочет.

Очевидно, суть произошедшего сводится всего лишь к консолидации всех медийных активов страны близким к российскому руководству бизнесом.

При этом сам П. Дуров в ярые оппозиционеры отнюдь не собирался – «золотой мальчик» со шлейфом громких скандалов, одним росчерком пера конвертируемых в уголовные дела, не хочет и, по большому счету, не может позволить себе оппозиционный эскапад. Но хороший хозяин носит все ключи в своем кармане, и потому «ВКонтакте» была обречена на «надежные руки».

Особенно если учесть то, что серьезные люди в Кремле очень серьезно относятся к роли социальных сетей в протестных движениях, и доверять управление подобным инструментом «первым попавшимся» отнюдь не намерены. Российские власти давно разрабатывают комплекс мер противодействия технологиям ненасильственной смены власти, показавшим свою эффективность во время восточноевропейских бархатных, цветных и особенно арабских революций. Социальные сети оказались очень эффективным средством мобилизации и координации протестов, каналом связи с внешним миром, а также мощной альтернативой официальным СМИ.

В Москве прекрасно осознают: потеря советским руководством монополии на информацию стала одним из факторов, приведших к коллапсу СССР. И российские власти стараются этот опыт учесть. Инакомыслящие СМИ собраны в некое подобие интеллектуального гетто, на базе РИА «Новости» создано подобие министерства пропаганды. Стада троллей пасутся на интернет-ресурсах. Но их усилий явно недостаточно: учитывая, что Россия вошла в число стран победившего капитализма, в условиях глобализации экономики и относительной свободы перемещений единственный более-менее надежный железный занавес – ментальный. И строится он путем не самых сложных манипуляций с контентом.

Конечно, «ВКонтакте» никогда не была и, по-видимому, вряд ли станет местом серьезного обмена мнениями – вроде давно покойного российского сектора LiveJornal. А революционные настроения в РФ популярны в основном в среде интеллектуалов, которые «ВКонтакте» в явном меньшинстве. Но это, как ни крути, слабо контролируемый канал общения гигантского количества российских граждан. Сегодня эта соцсеть – туча скучающих малолетних бездельников, а завтра – если и не нервная система протеста, то место сбора реальных, а не марионеточных «почвенников», нацистов либо радикальных левых. Идеология – штука небезопасная, поскольку может за считанные дни охватывать множество ранее вполне невинных умов.

Теперешних немногочисленных «-истов» вроде симпатиков экстрадированного на этой неделе с Кубы неонациста Тесака пока можно отлавливать по неумело спрятанным IP-адресам. Но если их станет хотя бы в три-пять раз больше, на всех компьютерно грамотных сотрудников может и не хватить. Это еще одна причина для присмотра за соцсетями.

Но чисто административные, казалось бы, перемены рано ли поздно неминуемо повлияют и на работу столь любимого российской молодежью «ВК».

Во-первых, к рулю придут люди от соцсетей далекие. Несмотря на опыт успешных издательских проектов, динамика и принципы горизонтальной информационной среды социальной сети могут оказаться им чуждыми, а потому – подлежащими реформированию.

А во-вторых, продукт, принадлежащий А. Усманову, уже не сможет демонстрировать ту же невероятную свободу нравов, которой смело пользовался продукт В. Мирилашвили (первоначального собственника 60 % акций «ВКонтакте») и П. Дурова. Длинный и роскошный шлейф скандалов – с нелегальным распространением музыки, порнографии, экстремистских взглядов и т. д., который тянется за «ВКонтакте» с момента запуска, новым собственникам проекта не к лицу. И его неизбежно придется перекроить.

И если с порнографией все еще может получиться более-менее эффективно, то потеря шарового музыкального сопровождения, которым пользуются, по некоторым данным, более половины участников соцсети, может стать поистине смертельным ударом.

Таким образом, через несколько лет новые собственники рискуют отвадить от соцсети тинейджеров – ее главную ударную силу – и получить в собственность лишь бренд – с небольшой аудиторией фанатов в придачу. При этом «ВКонтакте» уже сделала свое черное дело – пристрастила миллионы школьников и студентов к «сетевой» жизни. И если любимый проект в силу чересчур серьезного подхода новых собственников станет несколько менее любимым, все они вряд ли вернутся к телевизору. Они начнут искать новую соцсеть – которую опять придется окучивать и уламывать на переход на сторону сил «добра и порядка». А то и вовсе уйдут

в недосягаемые западные сети – что будет очень кстати для того же Facebook, который начал терять аудиторию.

Таким образом, за тактической победой – получением контроля над крупнейшей социальной сетью РФ – может наступить стратегическое поражение в виде появления конкурирующих и менее подконтрольных проектов. Очередное подтверждение давнего тезиса: не стоит чинить то, что вполне неплохо работает. Ведь останься проект формально неподконтрольным приближенным к власти бизнесменам – и все его мелкие шалости можно было бы списывать на излишний либерализм разгильдяев-собственников. А те были бы вынуждены смиренно молчать (как молчал некогда сбитый П. Дуровым гаишник), выполняя любые просьбы старших товарищей ***(Туркевич И. «ВКонтакте» с Кремлем // Комментарии (http://gazeta.comments.ua/?art=1391075164). – 2014. – 31.01).***

***

СБУ собирает данные на пользователей, которые ищут в онлайне информацию о Евромайдане

Многие украинские пользователи Facebook в последнее время поменяли свои имена в соцсети и закрыли данные профилей от общего доступа. Это связано с беспокойством пользователей о собственной безопасности в связи с массовыми протестами в стране. Вполне логичный ход, учитывая, что, по некоторым данным, украинские спецслужбы еще с начала протестных движений пытаются собрать у провайдеров данные о том, что именно пользователи пишут и смотрят в Интернете.

Недавно редактор российского информагентства «Новый регион» П. Мясоедов опубликовал в Facebook фотографию письма СБУ одному из хмельницких провайдеров, в котором следователь требует сообщить данные о пользователях, которые с 6 декабря и по 27 января (дата составления письма) просматривали определенные видео в Интернете. Речь идет о нескольких роликах на YouTube – в них прикарпатский священник резко критикует власть и поддерживает протест.

Ранее сотрудники СБУ уже обращались к администраторам региональных провайдеров с запросами о тех абонентах, которые на местных интернет-форумах обсуждают и поддерживают протесты. По некоторым данным, пытались провоцировать пользователей на резкие высказывания по этому поводу.

В украинском офисе Google заявили, что не получали от СБУ никаких запросов, связанных с революцией.

Напомним, что милиция получила доступ к данным обо всех звонках и SMS, которые отправляли протестующие под Святошинским судом Киева 10–11 января 2014 г. ***(СБУ теперь контролирует пользователей Интернета (Документ) // «Свобода слова в Україні» (http://svobodaslova.in.ua/news/read/29292). – 2014. – 5.02).***

***

Британский центр правительственной связи (GCHQ) проводил DDoS-атаки на сайты, использовавшиеся для переписки участниками движений Anonymous и LulzSec. Об этом 5 февраля сообщает NBC News со ссылкой на документы, предоставленные экс-сотрудником Агентства национальной безопасности США (АНБ) Э. Сноуденом.

Компьютерным атакам со стороны спецслужбы подвергались в основном чаты Anonymous и LulzSec. Тем не менее, как следует из опубликованных данных, многие DDoS-атаки затрагивали также ресурсы, которые использовали для коммуникации политические диссиденты из разных стран мира, не нарушавшие закон и никак не связанные с хакерскими группировками.

Планированием DDoS-атак в GCHQ занималась так называемая «Объединенная группа по исследованию угроз» (Joint Threat Research Intelligence Group, JTRIG), о существовании которой прежде ничего не было известно. Проведение хакерских атак на сайты самих хакеров описывалось сотрудниками JTRIG, как «эффективный метод запугивания». По данным спецслужбы, DDoS-атаки «отпугивали» около 80 % интернет-активистов, ранее сидевших в том или ином чате.

Представитель GCHQ в ответ на просьбу NBC прокомментировать деятельность JTRIG заявил, что работа всех подразделений агентства шла исключительно в рамках закона. В свою очередь бывший офицер безопасности американского Белого дома Д. Хили назвал тактику JTRIG «безумной». Как отметил Д. Хили, DDoS-атаки обычно не применяются против хакеров и используются исключительно как инструмент борьбы против враждебных государств.

Активное противостояние движения Anonymous и спецслужб началось в конце 2010 г. Поводом для этого послужила так называемая «Операция “Расплата”» (Operation Payback), проведенная активистами хакерского движения. В рамках операции хакеры атаковали сайты государственных структур и различных коммерческий компаний. В частности, DDoS-атаке подверглись ресурсы платежной системы PayPal. Группировка LulzSec отмежевалась от Anonymous в 2011 г. Основная активность движения, также специализировавшегося на хакерских атаках, пришлась на май-июнь 2011 г. В 2013 г. к тюремным срокам были приговорены четверо хакеров LulzSec. Они получили от двух до трех лет лишения свободы. В октябре 2013 г. также были предъявлены обвинения 13 членам группировки Anonymous ***(Британские спецслужбы уличили в DDoS-атаках на чаты Anonymous и LulzSec // InternetUA (http://internetua.com/britanskie-specslujbi-ulicsili-v-DDoS-atakah-na-csati-Anonymous-i-LulzSec). – 2014. – 5.02).***

***

Количество случаев привлечения к уголовной ответственности пользователей соцсетей в России в 2013 г. увеличилось более чем вдвое. Об

этом сообщается в докладе правозащитной ассоциации «Агора» «Свобода Интернета 2013: Атака охранителей», 4 февраля поступившем в «Ленту.ру».

Согласно собранной аналитиками «Агоры» статистике, в течение 2013 г. в общей сложности было зафиксировано 226 «удовлетворительных решений» по уголовным делам, связанным с интернет-активностью и публикациями в социальных сетях. В 2012 г. таких судебных решений было всего 103.

Наибольшее количество привлеченных к ответственности пользователей зарегистрировано во «ВКонтакте» (более 30 уголовных дел за прошедший год). Четыре процесса прошло в отношении публикаций в «Одноклассниках», еще три разбирательства – по факту постов в Facebook. Уголовную ответственность за публикацию противозаконных материалов в социальной сети «Мой Мир» понес один пользователь.

Как отмечает «Агора», подавляющее большинство подобных дел связаны со статьями Уголовного кодекса РФ, устанавливающими ответственность за экстремизм. Тем не менее, отмечают авторы доклада, активнее начали применяться в судах и статьи об оскорблении представителей власти и клевете. При этом учет фактов уголовного преследования интернет-пользователей осложняется тем, что правоохранительные органы далеко не всегда указывают название социальной сети, фигурирующей в материалах того или иного дела.

По данным ассоциации, увеличилось в 2013 г. и число административных дел против пользователей сети. За 2013 г. было зафиксировано 514 случаев привлечения пользователей, администраторов ресурсов и провайдеров к административной ответственности. Для сравнения, в 2012 г. «Агора» насчитала только 208 подобных дел. Эксперты ассоциации связывают столь резкий рост судебных разбирательств с активностью Роскомнадзора и вступлением в силу так называемого «единого реестра запрещенных сайтов» ***(Количество дел против пользователей соцсетей в РФ за год удвоилось // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kolichestvo_del_protiv_polzovateley_sotssetey_v_rf_za_god_udvoilos). – 2014. – 6.02).***

Проблема захисту даних. DDOS та вірусні атаки

В Запорожье взломали сайт городской мэрии. Вместо всей информации, которая ранее была на сайте, появилось видео силового разгона мирных активистов запорожского Евромайдана от 26 января, сообщают «Комментарии».

…Кроме того, на сайте выложена хронология событий в Киеве и видеоролики с силовым разгоном активистов Запорожского Евромайдана, а также беспредел, который происходил в Киеве на улице Грушевского.

«Запорожье, проснись! 27 января в 18:00 выходи на пл. Фестивальную», – призывают взломщики сайта запорожской мэрии.

Как уточняет корреспондент proIT, по состоянию на 16:30 на сайт городской мери Запорожья поставили «заглушку» с информацией о том, что сайт отключен по причине взлома ***(Активисты взломали сайт мэрии Запорожья // proIT (http://proit.com.ua/news/internet/2014/01/27/163433.html). – 2014. – 27.01).***

***

Неизвестные хакеры проникли в компьютерные сети Министерства обороны Израиля, реализовав фишинговую атаку и заразив ряд израильских компьютеров посредством письма, имитирующего срочное сообщение от Службы общественной безопасности ШАБАК Израиля. Об этом в воскресенье сообщила израильская компания Seculert, специализирующаяся на кибербезопасности.

А. Рафф, технический директор Seculert, говорит, что в январе хакерам удалось временно получить контроль над 15 компьютерами, один из которых принадлежал Гражданской администрации Израиля, которые отслеживает Палестинские территории. А. Рафф высказывает предположение, что за хакерской атакой на сеть министерства обороны стоят палестинские хакеры.

По сведениям Seculert, для взлома использовалась вредоносная программа Xtreme RAT, рассылавшаяся на адреса электронной почты работников госслужб с адреса Shabakreport@gmail.com. Сама программа, являющаяся «троянским конем», была замаскирована под файл PDF, якобы отправленный общей службой безопасности. При открытии файла программа устанавливалась на компьютере, открывая удаленный доступ к нему.

Для компьютерной атаки использовались серверы, расположенные в США, однако, по мнению экспертов, провели ее, скорее всего, палестинские хакеры. В 2012 г. палестинцы уже использовали эту программу для проникновения в компьютерные системы полиции Израиля. Тогда для предотвращения ущерба полиции пришлось в экстренном порядке отключать внутреннюю сеть.

Объем ущерба, нанесенного хакерами до обнаружения взлома, на текущий момент неизвестен. Компания Seculert поставила в известность надлежащие структуры сразу после выявления следов атаки. Отметим, что об обнаружении следов данной хакерской атаки стало известно накануне международной конференции по компьютерной безопасности, которая проходит в Израиле ***(Хакеры проникли в компьютерные сети Министерства обороны Израиля // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/01/27/foreign-ministry-hacked.html). – 2014. – 27.01).***

***

Исследователи нашли способ значительно сократить количество злоумышленников, пользующихся краденными банковскими картами или рассылающие спам в Skype. Работа, опубликованная М. Голдшмидтом, И. Се,

Ф. Юй и М. Абади из Microsoft Reseatch и А. Леонтьевой из Тартуского университета, рассматривает применение для этой цели алгоритмов машинного обучения с учителем (supervised learning).

Исследователи анализировали 34 тыс. учётных записей из случайной выборки, содержащей 200 тыс. учётных записей Skype, которые не были заблокированы в течение первых четырёх месяцев после создания. Некоторые из этих учётных записей принадлежали обычным пользователям. Другими обладали мошенники, которые долгое время ускользавшие от внимания технологии антифрода, применяемой в Skype в настоящее время.

Взяв за основу сведения об обращениях пользователей друг к другу, исследователи построили ориентированный граф, состоящий из 677,8 млн вершин, соединённых 4,2 млрд дуг. Его дополняли 10,8 млн меток, отмечающих уже выявленных злоумышенников. Эти данные использовались сначала для обучения классификаторов, а затем для оценки эффективности их работы.

Чтобы автоматически классифицировать пользователей, потребовалось учесть массу факторов. В ход пошли данные из самых разных источников, в том числе сведения о самих пользователях (например, возраст, указанный в профиле), история действий, которые они предпринимали (примером может служить коммуникация с другими пользователями), локальная социальная активность (добавление или удаление пунктов в списке контактов) и глобальная социальная активность (её можно оценить при помощи алгоритма PageRank).

По отдельности каждого из этих факторов недостаточно для выявления злоумышленников. «Данные зачастую пестрят пробелами и содержат отсутствующие значения, – указывают авторы работы. – К тому же аномальные закономерности, связанные с атаками, могут проявлять себя в других местах». Однако если комбинировать несколько источников, то картина меняется. Эксперименты свидетельствуют, что чем больше факторов учитывают классификаторы, тем выше вероятность того, что подозрительный аккаунт будет замечен.

Как выяснилось, большинство учётных записей, рассылающих спам или связанных с краденными банковскими картами, поначалу принадлежало честным пользователям, но затем они были взломаны и сменили владельца. В публикации высказывается предположение, что анализ продолжительных временных серий позволит заметить резкую перемену в поведении пользователя, указывающую на взлом.

Исследователям удалось добиться обнаружения 68 % злоумышленников, научившихся обманывать существующую защиту Skype. Доля ложных срабатываний при этом не превышала 5 %. Это значит, что количество мошеннических учётных записей, избегающих блокирования более десяти месяцев, сократится в 2,3 раза ***(Исследователи нашли алгоритмы машинного обучения, которые лучше ловят мошенников в Skype // InternetUA (http://internetua.com/issledovateli-nashli-algoritmi-***

mashinnogo-obucseniya--kotorie-lucsshe-lovyat-moshennikov-v-Skype). – 2014. – 27.01).

***

Сайт «5-го канала» испытывает мощные хакерские атаки

27 января неизвестные злоумышленники начали очередную серию мощных DDoS-атак на сайт «5-го канала». Об этом сообщается на официальной странице канала в соцсети Facebook, передает корреспондент «proIT».

«ИТ-специалисты делают все возможное, чтобы восстановить работу сайта. Впрочем, наш канал на YouTube работает в обычном режиме. Все самое важное ищите там», – подчеркивает канал.

Также сотрудники «5-го канала» утверждают, что съемочная группа канала постоянно подвергается вмешательству в работу. «Нам создают технические проблемы с работой нашей передвижной телевизионной станции, благодаря которой журналисты вживую сообщают новости», – поясняет «5 канал». Как сообщают специалисты, сигнал оборудования «5-го канала» намеренно глушат.

Как уточняет корреспондент «proIT», по состоянию на 10:00 28 января сайт «5-го канала» работал в штатном режиме.

Напомним, это не единичный случай, когда хакеры пытались «положить» сайт канала. Так, 7 декабря непрерывные DDoS-атаки на сайт канала привели к его блокированию ***(Сайт «5-го канала» испытывает мощные хакерские атаки // proIT (http://proit.com.ua/news/internet/2014/01/28/100418.html). – 2014. – 28.01).***

***

Сайт Divan.tv зазнає масованих DDoS-атак

28 січня на сайт мультимедійного сервіс-провайдера Divan.tv, який транслює «Еспресо.TV», 5 канал, ТВі і «Громадське ТБ», здійснюються масовані DDoS- атаки. Про це повідомляє прес-служба компанії.

У колл-центр компанії Divan.tv з ранку почали надходити дзвінки користувачів зі всієї України про некоректність роботи сервісу. Нині всі оперативні ресурси R & D офісу Divan.tv задіяні під захист сервісу, повідомляє компанія.

Хто саме атакує сайт сервісу, невідомо. Однак Divan.tv пов’язує атаки з тим, що нещодавно портал опублікував інформацію про популярність інформаційних інтернет-телеканалів «Еспресо.TV», 5 канал і «Громадське ТБ» ***(Сайт Divan.tv зазнає масованих DDoS-атак // «Телекритика» (http://www.telekritika.ua/rinok/2014-01-28/89850). – 2014. – 28.01).***

***

Divan.tv восстановил штатный режим работы

Мультимедийный сервис Divan.tv прокомментировал по запросу редакции «proIT» ситуацию с активными хакерскими атаками на ресурс. В настоящее время массовые DDoS-атаки на Divan.tv прекратились.

Как уточнили в компании, технический департамент активно занимается повышением защиты сайта и самого сервиса Divan.tv, однако источники и мощности атак пока не установлены. «Единственное, что пока можем сказать – атаковали из разных мест. Это не было одним источником», – поясняют в компании.

Также в компании сообщили, что особых потерь из-за некорректности работы ресурса не была. Больше всего из-за DDoS-атак пострадал колл-центр, который принял за 28 января больше 300 звонков (без учета недозвонившихся). Как уточняют в компании, в стандартный день обычно бывает только 20–30 обращений в колл-центр.

Напомним, в компании связывают массовые хакерские атаки с недавно опубликованным рейтингом телеканалов ***(Divan.tv восстановил штатный режим работы // proIT (http://proit.com.ua/news/internet/2014/01/29/153512.html). – 2014. – 29.01).***

***

Украина по итогам 2013 г. заняла 11-е место среди стран-источников спама в мире, сообщается в отчете производителя защитных систем «Лаборатории Касперского».

Как передает IT Expert со ссылкой на УНИАН, данные компании говорят о том, что в 2013 г. доля спама, рассылаемого через расположенные в Украине компьютеры и сервера, составила 3 % от мирового объема.

При этом среднегодовое количество спама в мировом почтовом трафике составило 69,6 %, что на 2,5 % ниже показателя годом ранее.

Аналитики компании отмечают, что в 2013 г. в спам-рассылках уменьшилось количество легальной рекламы товаров и услуг и возросло число мошеннических и вредоносных сообщений. При этом большинство нежелательных сообщений (74,5 %) имели объем не больше 1 Кб ***(Украина заняла 11-е место в мире по рассылке спама // InternetUA (http://internetua.com/ukraina-zanyala-11-e-mesto-v-mire-po-rassilke-spama). – 2014. – 28.01).***

***

Возросла активность трояна Boaxxe, который заражает пользователей, перенаправляя их на рекламные сайты. Об этом предупреждает антивирусная компания ESET.

Win32/Boaxxe.BE – семейство вредоносных программ, используемых киберпреступниками для перенаправления пользователя на рекламные сайты ради получения платы от рекламодателя (эта схема называется «кликфрод»).

Данная программа попадает в систему через вредоносные ссылки, которые активно распространяются на сомнительных или зараженных

сайтах, а также через спам-рассылки. С сентября 2013 г. троян Boaxxe распространяется силами участников одной из мошеннических партнерских программ в русскоязычном сегменте сети. За последние четыре месяца к этой партнерской программе присоединились более 40 новых участников.

Согласно проанализированной статистике, за два месяца один из участников заразил трояном Boaxxe свыше 3300 устройств.

«Этот тип ПО (в отличие, например, от банковских троянов) напрямую не наносит пользователям ущерб. Основная угроза состоит в том, что пользователю будут демонстрироваться подложные сайты. К примеру, вы ищете, где купить телевизор, и вместо раскрученных магазинов браузер будет перенаправлять вас на сайты рекламодателей, – объяснил руководитель аналитического центра Zecurion В. Ульянов. – На мой взгляд, в данном случае хуже всего то, что компьютер ведёт себя “неадекватно”, не так, как ожидает пользователь. Ведь на этих “левых” сайтах пользователю могут не только предложить телевизор, но и инфицировать компьютер другим вредоносным ПО. Ещё один фактор – можно назвать неудобством – самостоятельный запуск браузера и загрузка сайтов рекламодателей».

При этом хакеры получают выгоду – отчисления сайтов-рекламодателей за переходы на их страницы. «Поэтому заработок прямо зависит от числа заражённых систем. Вообще, подобные партнерские программы не редкость. Но реальными интернет-магазинами для продвижения своих товаров и услуг используются ограниченно, в том числе из-за крайне низкого процента конвертации посещений в покупки – большинство переходов осуществляется автоматически, и пользователи быстро закрывают назойливую рекламу. Это, кстати, подтверждает и статистика исследователей – на автоматизированных переходах хакер Boaxxe заработал в несколько раз больше денег, – добавил В. Ульянов. – Аналогичный функционал (перенаправление пользователя) имеют не только вредоносные программы, но даже программы-шутки» ***(Троян Boaxxe «забивает» браузеры рекламой // InternetUA (http://internetua.com/troyan-Boaxxe--zabivaet--brauzeri-reklamoi). – 2014. – 28.01).***

***

В Thunderbird, программе для работы с электронной почтой и новостными лентами от разработчиков Mozilla, обнаружена опасная уязвимость. По данным пакистанских исследователей из Vulnerability-Lab, найденная ими брешь позволяет полностью скомпрометировать системы пользователей.

Эксплуатация уязвимости, затрагивающей Thunderbird версии 17.0.6, дает возможность атакующим обойти фильтр, не допускающий обработки HTML тегов в сообщениях. Исследователи также подчеркивают, что данная проблема существует непосредственно из-за использования движка Gecko.

Отметим, что теги <script> и <iframe> по умолчанию блокируются в Thunderbird и отфильтровываются сразу после их ввода. Однако обойти эту

защиту можно при составлении нового письма путем кодирования вредоносного кода стандартом base64 и тега <object>.

Вредоносный код будет запущен, после того как жертва попробует ответить или переслать инфицированное письмо.

В настоящее время брешь уже была устранена разработчиками Mozilla. Исправление содержится в обновлении Thunderbird версии 24.2.0. ***(Брешь в Thunderbird позволяет внедрять вредоносный код в электронные письма // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/01/29/Thunderbird-flaw.html). – 2014. – 29.01).***

***

Уязвимость в Foursquare позволяла раскрыть 45 млн адресов электронной почты.

Популярная социальная платформа Foursquare, количество пользователей которой насчитывает 45 млн человек, содержала уязвимость, позволяющую раскрыть адреса электронной почты ее пользователей. Брешь содержалась в одноименном официальном мобильном приложении.

По словам исследователя безопасности Д. Эддина, потенциальный злоумышленник мог получить доступ к адресам всех пользователей Foursquare, используя простой программный инструмент, состоящий из нескольких строк кода. Эксперт также пояснил, что уязвимость содержалась в механизме приглашения друзей в мобильном приложении Foursquare.

При получении приглашения, адресату приходит соответствующее сообщение, отображающее адрес электронной почты отправителя. При этом URL приглашения содержит идентификатор учетной записи того, кто его отослал.

Впоследствии Д. Эддин выяснил, что заменяя соответствующий параметр в URL он может получить доступ ко всем профилям в Foursquare и раскрыть указанные в них адреса ***(Уязвимость в Foursquare позволяла раскрыть 45 млн адресов электронной почты // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/01/29/Foursquare-flaw.html). – 2014. – 29.01).***

***

Компания Yahoo! сообщила об атаке хакеров и утечке данных учетных записей электронной почты своих пользователей, передает IT Expert.

«Недавно мы обнаружили скоординированные попытки получить несанкционированный доступ к аккаунтам Yahoo Mail, – говорится в сообщении компании. – После обнаружения мы немедленно предприняли действия для защиты наших пользователей».

Yahoo! отправила сообщения на резервный адрес или на телефон «пострадавших» пользователей об изменении их пароля, с дальнейшими

инструкциями. Другим пользователям компания также рекомендует сменить пароль аккаунта.

При этом в Yahoo! не стали уточнять, как долго были в курсе возможной утечки и сколько данных в итоге могло быть похищено. Но компания подчеркивает, что данные пользователей были получены не с серверов Yahoo!, а от «третьей стороны». Хакеры воспользовались логинами и паролями, которые были украдены во время другой утечки данных ***(Yahoo! сообщила об атаке хакеров и утечке данных своих пользователей // IT Expert (http://itexpert.in.ua/rubrikator/item/33605-yahoo-soobshchila-ob-atake-khakerov-i-utechke-dannykh-svoikh-polzovatelej.html). – 2014. – 31.01).***

***

Уязвимость в Facebook Connect не могут или не хотят устранять.

Брешь позволяет раскрыть учетные данные пользователей социальной сети.

Как сообщает в своем блоге исследователь безопасности Е. Хомяков, ему удалось обнаружить две уязвимости в социальной сети Facebook, позволяющие с помощью сервиса Facebook Connect скомпрометировать использующий данную службу веб-сайт, а также раскрыть учетные данные пользователей атакуемого ресурса.

По словам эксперта, злоумышленнику достаточно загрузить специальный фрейм, который будет автоматически отправлять имя пользователя и его пароль от Facebook, однако, при этом будут раскрыты учетные данные атакующего.

«Каждый веб-сайт, обладающий функционалом быстрой авторизации с помощью Facebook Connect уязвим и позволяет похищать учетные записи пользователей социальной сети», – поясняет Е. Хомяков, подчеркивая, что социальная сеть не намерена выпускать какое-либо исправление.

«Это одна из тех проблемных областей, о которой мы были осведомлены относительно давно, однако так и не смогли найти системное и эффективное решение», – прокомментировали в социальной сети ***(Уязвимость в Facebook Connect не могут или не хотят устранять // InternetUA (http://internetua.com/uyazvimost-v-Facebook-Connect-ne-mogut-ili-ne-hotyat-ustranyat). – 2014. – 30.01).***

***

Эксперт разработал вредоносное ПО, способное похищать PIN-коды пользователей через сенсорный экран.

Вирус способен отслеживать движения пальцев по сенсорному экрану, фотографии, сделанные при помощи гаджета, рисунки, созданные в графических приложениях и т. д.

Количество вредоносного ПО для мобильных устройств неукоснительно растет, в связи с чем пользователям необходимо серьезно задуматься над тем, как обезопасить себя. Примечательно, что 99 % вирусов

созданы для платформы Android, которая является самой популярной мобильной ОС.

Как сообщило издание Forbes, консультант по безопасности из компании Trustwave Н. Хиндоча разработал концепцию вредоносного ПО, предназначенного для отслеживания взаимодействия пользователя с мобильным устройством. Вирус способен отслеживать движения пальцев по сенсорному экрану, фотографии, сделанные при помощи гаджета, рисунки, созданные в графических приложениях и т. д. Вредоносное ПО фиксирует x и y-координаты любого движения по сенсорному экрану.

По словам Н. Хиндочи, инфицировать этим вирусом iOS-устройство, на котором был осуществлен джейлбрейк, а также гаджет, работающий на базе Android, не составляет труда. Например, вредоносное ПО может попасть на смартфон, если тот подключен к стационарному компьютеру через USB.

При помощи вируса, отслеживающего движения пальцев по сенсорному экрану, злоумышленники могут похищать PIN-коды пользователей. «Если вы отслеживаете взаимодействие пользователя с телефоном, и в течение часа ничего не происходило, а потом фиксируете как минимум четыре прикосновения, то наверняка пользователь ввел PIN-код», – сообщил Е. Хиндоча.

Эксперт отметил, что неважно, каким образом пользователь вводит данные, они все равно будут похищены ***(Эксперт разработал вредоносное ПО, способное похищать PIN-коды пользователей через сенсорный экран // InternetUA (http://internetua.com/ekspert-razrabotal-vredonosnoe-po--sposobnoe-pohisxat-PIN-kodi-polzovatelei-cserez-sensornii-ekran). – 2014. – 30.01).***

***

Обнаружен бот, зомбирующий ПК на Windows, Mac и Linux

Специалисты «Лаборатории Касперского» обнаружили вредоносную программу, использующую персональные компьютеры на базе Windows, Mac и Linux для проведения DDoS-атак. Управление компьютерами-зомби злоумышленники осуществляют с помощью команд в чате в сети IRC, к которой приложение подключается втайне от пользователя.

«Лаборатория Касперского» обнаружила вредоносное Java-приложение, превращающее персональные компьютеры пользователей под управлением Windows, Mac и Linux в зомби, следующие командам злоумышленников. Об этом на сайте SecureList рассказал вирусный аналитик А. Иванов.

«Основной функционал бота – проведение DDoS-атак с компьютеров зараженных пользователей. При его анализе нами была зафиксирована попытка проведения атаки на один из сервисов осуществления рассылок по электронной почте», – рассказал аналитик.

В ЛК приложению присвоили имя HEUR:Backdoor.Java.Agent.a.

«При запуске бот копирует себя в домашнюю директорию пользователя и прописывается в автозагрузку. В зависимости от платформы, выбирается следующий способ добавления в автозагрузку: в Windows – через системный реестр, в OS X – используется стандартный сервис launchd, в Linux – /etc/init.d/. После запуска и добавления в автозагрузку боту необходимо сообщить об этом своим владельцам. Для того чтобы идентифицировать каждого бота, на пользовательской машине генерируется уникальный идентификатор бота», – рассказал эксперт.

После запуска бот подключается к чат-сети IRC, появляясь в специализированном канале как пользователь с уникальным идентификатором. Для обработки команд от своих владельцев, которые находятся в этом же канале, используется открытый фреймворк PircBot (который в благих целях позволяет создавать чат-ботов).

Сеанс подключения к IRC-серверу

После того как все настроено и компьютер-зомби вышел в сеть IRC и присоединился к каналу, злоумышленники указывают ему в чате команды, которые включают адрес атакуемого, порт, тип и длительность атаки, а также сколько потоков для нее использовать.

Подключение к каналу

Аналитик добавил, что для того чтобы усложнить анализ и вредоносной программы и выявление ее предназначения, разработчики использовали обфускацию – то есть запутывание исходного кода программы ***(Обнаружен бот, зомбирующий ПК на Windows, Mac и Linux // InternetUA (http://internetua.com/obnarujen-bot--zombiruuasxii-pk-na-Windows--Mac-i-Linux). – 2014. – 30.01).***

***

Троян ChewBacca распространяется в 11 странах.

Наиболее активно троян для терминалов действует в США, России, Канаде и Австралии.

ИБ-эксперты компании RSA зафиксировали активность ботнета, главным предназначением которого было хищение данных о банковских картах пользователей через терминалы.

Как оказалось в ходе подробного исследования, распространяемое вредоносное ПО является вирусом ChewBacca, который впервые был подробно описан экспертами «Лаборатории Касперского». По словам последних, троян связывается с C&C-сервером через сеть Tor, что помогает скрывать задействованные IP-адреса.

Согласно данным специалистов RSA, машины, входящие в состав ботнета, расположены в 11 разных странах, при этом больше всего вирус распространяется на территории США. Кроме того, троян активно действует в России, Канаде и Австралии.

Напомним, что по данным «ЛК», троян является исполняемым файлом PE32, распространяемым компилятором Free Pascal 2.7.1 от 22 октября

2013 года, объемом в 5 МБ с Tor 0.2.3.25. известно, что после запуска вирус записывает нажатия клавиш в журнал system.log, который создается во временной папке на системе жертвы ***(Троян ChewBacca распространяется в 11 странах // InternetUA (http://internetua.com/troyan-ChewBacca-rasprostranyaetsya-v-11-stranah). – 2014. – 1.02).***

***

Вредоносное ПО для FTP-приложений похищает учетные данные пользователей

Злоумышленникам удалось внедрить вредоносные компоненты в открытый код FTP-приложения.

Компания Avast обнаружила вредоносное ПО для FTP-приложений под названием FileZilla, которое похищает учетные данные пользователей. FileZilla – это ПО с открытым исходным кодом. Хакеры изменили его, превратив в вирус, который распространяется через взломанные сайты, содержащие рекламные объявления и банеры.

После установки на компьютер пользователя вирус не проявляет никакой вредоносной деятельности. Программа функционирует точно также, как обычное приложение. Единственное отличие – это то, что загрузочный файл .exe поддельного приложения несколько меньше по размеру.

Известно, что вредоносная программа похищает учетные данные пользователей, а затем отправляет их на C&C-сервер, расположенный в Германии. IP-адрес, связанный с вирусом, также имеет отношение к трем другим доменам, которые связаны с распространением вредоносного ПО и рассылкой спама.

«Учетные данные отправляются злоумышленникам через FTP-соединение. Вредоносная программа не использует закладки в браузере пользователя и не отправляет любые другие файлы», – отмечают специалисты Avast.

По всей вероятности, вредоносное ПО появилось еще в сентябре 2012 г. Эксперты не исключают, что FileZilla может загружать на устройства пользователей дополнительные вирусы. В настоящее время оно распознается антивирусными программами ***(Вредоносное ПО для FTP-приложений похищает учетные данные пользователей // InternetUA (http://internetua.com/vredonosnoe-po-dlya-FTP-prilojenii-pohisxaet-ucsetnie-dannie-polzovatelei). – 2014. – 31.01).***

***

Каждую секунду в мире жертвами киберпреступников становятся 12 человек, и этот показатель увеличивается. Об этом заявил в ходе своего выступления на форуме информационной безопасности начальник Бюро специальных технических мероприятий МВД России А. Мошков.

По словам А. Мошкова, основной мотив деятельности киберпреступников – это извлечение материальной выгоды. «Количество

преступлений, совершаемых из хулиганских и иных побуждений, крайне незначительно», – подчеркнул представитель Министерства внутренних дел.

Кроме того, как отметил А. Мошков, в прошлом году сотрудниками Управления «К» было предотвращено хищение около 1 млрд р. с банковских счетов граждан. Преступники действовали, используя вредоносные программы, благодаря которым им удалось получить доступ к счетам нескольких десятков тысяч клиентов российских банков, передает РИА «Новости».

Также начальник Бюро специальных технических мероприятий МВД России заявил, что владельцы планшетных компьютеров и мобильных телефонов для обеспечения безопасности редко используют антивирусы. «Если пользователи персональных компьютеров еще как-то заботятся об обеспечении безопасности, то владельцы мобильных телефонов и планшетов практически совсем не уделяют этим вопросам внимания, – подчеркнул он. – Всего 33 % владельцев смартфонов используют антивирусы, а 57 % вообще не знают о существовании подобных программ».

По словам А. Мошкова, что термин компьютерный вирус у людей ассоциируется исключительно с персональными компьютерами, в то время как количество вредоносных программ, ориентированных на мобильные гаджеты, постоянно растет ***(Хакеры атакуют 12 человек в секунду // Internetua.com (http://internetua.com/hakeri-atakuuat-12-cselovek-v-sekundu). – 2014. – 31.01).***

***

Беспилотные автомобили станут «целью № 1» для хакеров.

Ведущие аналитики, занимающиеся вопросами систем безопасности, уверяют, что в ближайшем будущем, когда беспилотные автомобили займут полноценное место на дорогах, они превратятся в главную мишень хакерских взломов и атак.

Такое мнение высказывает Э. Шварц, вице-президент отдела по вопросам мировой безопасности Verizon. По мнению эксперта, индустрия кибербезопасности всё ещё находится в зачаточном состоянии.

Сегодня все основные производители автомобилей ведут разработку беспилотных транспортных средств. Чтобы автомобили могли самостоятельно, без участия водителя, передвигаться по дорогам общественного пользования, им необходимо поддерживать связь между собой. Именно эти каналы взаимодействия машин, о защите которых сегодня никто особо не задумывается, и станут уязвимым местом беспилотных автомобилей – уверен специалист.

Э. Шварц указывает на то, что сегодня даже обычные машины наделены возможностью обмена информацией, но производители совершенно забыли о защите каналов, по которым эта информация передаётся. Получается, что даже обычные авто подвержены хакерским атакам.

Однако у беспилотников будет больше возможностей передачи информации между участниками движения, и при этом, меньше надзора со стороны водителя, который займёт, по сути, место пассажира. Человек даже не будет знать, что происходит с его машиной в данный момент.

Э. Шварц выразил обеспокоенность тем, что чрезмерно быстрое развитие технологий, особенно в медицине, повышает риск потенциальных хакерских взломов устройств, которые хранят персональную медицинскую информацию о том или ином человеке, или отвечают за его жизнь ***(Беспилотные автомобили станут «целью №1» для хакеров // InternetUA (http://internetua.com/bespilotnie-avtomobili-stanut--celua--1--dlya-hakerov). – 2014. – 31.01).***

***

Румынская полиция деактивировала серверы трояна-вымогателя ICEPOL. Вредоносное приложение инфицировало более 260 тыс. компьютеров по всему миру.

Как сообщают исследователи из BitDefender, правоохранительным органам Румынии удалось захватить контроль над серверами трояна-вымогателя ICEPOL, заразившего за последние пять месяцев порядка 260 тыс. компьютеров по всему миру.

Отметим, что вирус блокировал доступ пользователей к собственной системе, требуя денежный выкуп за его возрат. В этих целях вредоносное приложение эксплуатировало уязвимость в Java (CVE-2013-0422), передает The Hacker News.

Заражая компьютер, ICEPOL уведомлял его владельца о том, что данная система использовалась в целях распространения пиратского ПО или порнографии. При этом выкуп за возвращение доступа преподносился жертве как штраф за незаконную деятельность. Сообщение могло отображаться на 25 языках.

Интересно также, что вирус содержит в себе дополнительный инструмент для получения прибыли – механизм переадресации пользователей на подконтрольные злоумышленникам веб-сайты.

«Несмотря на сложный характер проведенных нами исследований нам все же удалось достичь хороших результатов», – прокомментировали в полиции Румынии ***(Румынская полиция деактивировала серверы трояна-вымогателя ICEPOL // InternetUA (http://internetua.com/ruminskaya-policiya-deaktivirovala-serveri-troyana-vimogatelya-ICEPOL). – 2014. – 1.02).***

***

В социальной сети «ВКонтакте» обнаружена уязвимость.

Специалисты из Habrahabr провели исследование нескольких социальных сетей на предмет ошибок и багов. Причем именно таких, которые так или иначе дают возможность завладеть хотя бы крупицами данных пользователей.

Старания увенчались успехом: в мобильной и основной версиях «ВКонтакте» была обнаружена одна и та же ошибка. В m.vk.com, при восстановлении пароля, при введении мобильного система отображает его имя, фамилию. «Злоумышленник, завладевший номерами пользователей, сможет с легкостью составить базу всех людей, зарегистрированных в сети, – отмечает представитель Habrahabr. – А получить доступ к этим самым мобильным номерам не так уж и сложно. Что интересно – похожая ситуация наблюдается и в Facebook. Что это – случайность, или запланированные недочеты?»

О найденных багах сообщили соответствующим социальным сетям, но ни представители «ВКонтакте», ни представители Facebook никак не отреагировали на заявления.

Но буквально через несколько дней в мобильной версии ВК исправили ошибку. Теперь при введении телефона при восстановлении аккаунта отображается только аватар пользователя, последняя установленная картинка. А вот в основной версии все осталось по-прежнему.

Существует еще несколько способов завладеть данными. Например, с помощью специальной программы, заполучить аватар и с помощью поиска по картинке найти нужного пользователи вместе с необходимой информацией ***(Во «ВКонтакте» обнаружена уязвимость // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vo_vkontakte_obnaruzhena_uyazvimost). – 2014. – 30.01).***

***

Так где же прячется это самое кибероружие?

Один из самых распространённых страхов нашего времени – кибервойна. Чем больше вокруг нас «умных» вещей, тем выше уязвимость для кибероружия. Эру атомных страхов открыли взрывы над Хиросимой и Нагасаки. В 2010 г. ждали, что обнаружение боевого червя Stuxnet ознаменует вступление человечества в эпоху киберборьбы, постоянных схваток за овладение контролем над множащимися компьютерными системами вероятного или актуального противника. Однако этого не произошло. Как и взрывы над Японией, применение Stuxnet оказалось уникальным. Но почему?

Идея кибероружия, заставляющего вещи выходить из повиновения владельцам, превосходно усваивается людьми, ибо очень хорошо ложится на архетипы европейской культуры. Кажется, первым в литературной форме воплотил их российский поэт В. Брюсов в неоконченном рассказе 1908 г. (первая публикация – 1976 г.) «Восстание машин». Правда, это было именно художественное видение: о каких-либо гибких системах управления технология того времени всерьёз говорить не могла. (Вышедшая в 1909 г. антиутопия «Машина останавливается» Э. Форстера говорила об обычной поломке…)

Но прошло чуть больше века, и встроенными компьютерами с полноценными операционными системами обзаводится всё больше и больше бытовой техники. А наличие операционной системы обычно влечёт за собой функции «перепрошивки» – что обычно делаешь, купив новую электронную книжку, файлохранилище или медиаплеер. И скоро это же придётся проделывать с холодильниками и стиральными машинами. Ну а практически все промышленные и инфраструктурные контроллеры обречены на это уже сегодня. А насколько распространены вирусы – знают все…

Ну а кибероружие – это по форме тоже вредоносный софт той или иной разновидности. Только если вирус может заблокировать компьютер любителя контента для взрослых, требуя потом или денег за разблокировку, или некоторых знаний и возни для чистки системы, то кибероружие сможет вывести из строя, скажем, теплоцентраль. А когда температура окружающей среды установилась на пару недель на уровне минус двадцать восемь по Цельсию, это может быть очень страшно… Да, снабжающая район в целом котельная цифровых изысков не содержит. А вот автономная котельная на крыше управляется контроллером под одной очень известной версией ОС!

Применение ядерных бомб против японских городов было уникальным событием – как и использование Stuxnet.

И контроллер имеет разъёмы для перепрошивки. (Кстати, добросовестно опечатанные, но кому и когда это мешало?) И чем новее оборудование в энергосетях, транспортных системах, логистических центрах, банковских системах, на промышленных предприятиях – тем больше вероятность того, что в них присутствуют «разумные» и уязвимые цифровые системы управления. Но вот парадокс: со времени Stuxnet ни одного сколько-нибудь масштабного случая применения кибероружия зарегистрировано не было. Разве что система управления тоннелем в Хайфе (Китай хакнул Израиль).

Но как же? А кибератаки на такой крупный объект, как Aramco, государственная нефтегазовая компания Саудовской Аравии, поставляющей десятую часть экспортируемой на планете нефти? (Aramco Says Cyberattack Was Aimed at Production). Действительно, в августе 2012 г. вирусы поразили около 30 тыс. компьютеров этой компании. Ответственность за акцию взяла на себя хакерская группа по имени Cutting Sword of Justice («Рубящий меч правосудия»). Именно она разработала и распространила вирус Shamoon. По словам авторов – в отместку за политику саудитов в отношении Бахрейна и Сирии.

Хакерам из Cutting Sword of Justice поразить эту инфраструктуру Aramco не удалось.

Казалось бы, налицо кибергерилья, мотивированная политическими целями партизанская борьба в киберпространстве. Но говорить о том, что Shamoon был кибероружием, явно не стоит. Да, заражая компьютеры, хакеры-меченосцы надеялись сорвать поставки углеводородов на мировой рынок (чего им, кстати, сделать не удалось). Однако заражал вирус офисные

компьютеры, уничтожая и вроде бы воруя информацию с их жёстких дисков. Очень неприятно: посмотрите, как в час пик реагирует очередь в гипермаркете, когда зависает оплата картами… Но – не смертельно!

То есть «традиционный» вирус работает с информацией. А кибероружие – вероятно, пора уже ввести определение – должно с помощью модификации информации обеспечить вредоносное воздействие на объекты материального мира. Скажем, в случае Aramco подлинным кибероружием был бы вредоносный софт, перехватывающий управление насосами и задвижками, с помощью чего можно вызывать порывы на трубопроводах, разливы нефти в океан, взрывы газа… «Слава Богу, этого не произошло…», – сказал вице-президент Aramco А. аль-Саадан.

Но – почему не произошло? Трудно предположить, что «меченосцам» этого не хотелось бы… Значит, дело не в этом. А в чём – попыталась выяснить конференция Digital Bond's SCADA Security Scientific Symposium (S4), проходившая в Майами-Бич с 14 по 17 января 2014 г. И вот ответы, которые там давались, столь интересны, что их явно стоит представить читателям «Компьютерры». Прежде всего – версия о том, что Stuxnet всех так напугал, что во всех инфраструктурных и промышленных системах программные уязвимости были закрыты. Такую наивную позицию отвергает Э. Леверетт из IOActive.

По мнению этого эксперта кибербезопасности (взгляните в его Twitter хотя бы из-за забавных карикатур), даже самые элементарные меры предосторожности – о которых годы и годы, ещё с бумажной версии, пишет «Компьютерра» – всё ещё чрезвычайная редкость в мире поставщиков контроллеров, которые, доставаясь потребителю более чем по килобаксу за штуку, не имеют в составе комплектного программного обеспечения таких насущных вещей, как средства аутентификации, как электронная подпись, санкционирующая внесение изменений в софт, как журналы регистрации событий…

Может, идея кибервойны всех настолько ужаснула, что и идея о ней отброшена (как после Нагасаки никому и в голову не пришло решить проблемы с помощью деления тяжёлых или синтеза лёгких ядер)? Да вроде нет, если верить Л. Галанте, бывшей сотруднице разведки Министерства обороны США, ныне трудящейся на благо Mandiant. По её словам, США отслеживают активность в этом направлении не только Китая и России, но и Сирии. (С Россией немножко неясно: как активность отслеживается, если в ход кибероружие не шло? Это ж не ядерные испытания с их сейсмическими и электромагнитными эффектами…)

Мысль кажется правдоподобной: с чего бы люди вдруг откажутся от своего извечного стремления к войне и обретению нового оружия? И «дыр» ведь в программном обеспечении хватает… Ответ на парадокс дал Р. Лангнер, считающийся общепризнанным экспертом по Stuxnet. По его мнению, при создании кибероружия главная задача состоит отнюдь не в проникновении в систему управления (что облегчается обилием

уязвимостей). Это даже не половина, а ничтожная часть дела… Настоящая работа начинается с того момента, как кибероружие проникает в систему и получает контроль над ней.

Р. Лангнер – общепризнанный специалист по Stuxnet.

Скажем, в случае всесторонне описанного Stuxnet надо было плавно и настойчиво, чтобы не вызвать преждевременной тревоги, выводить центрифуги на пагубный для них режим. А чтобы проделать это, разработчикам кибероружия нужны были не только навыки вирусописания, но и инженерные знания. Технология обогащения урана. Конструкция высокоскоростных центрифуг. Металлургия спецсплавов. Лет шесть технического образования по каждому вопросу. И – отнюдь не по общедоступным книгам, а по материалам, доступным лишь сверхдержавам. Конечно, всё военное можно воспроизвести на основе общенаучных знаний, как Д. Менделеев восстановил рецепт пироксилинового пороха, но для этого надо было и быть Дмитрием Ивановичем...

То есть потенциальная возможность для слаборазвитых государств причинить государствам высокоразвитым значительный вред с использованием кибероружия остаётся. Только вот для того, чтобы эту потенцию актуализировать, нужны знания об инфраструктуре этих развитых государств на таком уровне, каким слаборазвитые вряд ли могут похвастаться… А случись там специалист – рентабельней ему переехать в первый мир, на куда большую и куда более стабильную зарплату! Правда, это не исключает необходимости приложить – и уже в ближайшее время – изрядные усилия к обеспечению безопасности «умных» машин.

Вернейшим способом для чего участники симпозиума считают переход на открытые системы, прозрачные для потребителя. Дело в том, что особых знаний для того, чтобы причинить ущерб соседу с помощью «умных» тостера и смывного бачка, не требуется… А пока киберугрозы все же сводятся не к тому, что «умные» вещи смогут вас тем или иным способом обидеть, а к тому, что они смогут о вас рассказать и кому. Ну, вот вызывающие большой интерес процессы на Майдане. Как пишет The New York Times, украинские власти отслеживают участников протестных действий по данным, запрошенным у мобильных операторов. Реальность пока только это, а взбунтовавшийся чайник так же далёк, как и во времена В. Брюсова… ***(Так где же прячется это самое кибероружие? // InternetUA (http://internetua.com/tak-gde-je-pryacsetsya-eto-samoe-kiberorujie). – 2014. – 3.02).***

***

Система защиты информации покажет хакерам ложные «секретные» данные.

В качестве защиты от хакерской атаки специалист по криптографии предлагает подбрасывать хакерам фальшивые «секретные» данные, которые

позволят обезопасить настоящую конфиденциальную информацию пользователей от компрометации.

Учёный-криптограф А. Джуэлс предлагает весьма остроумный способ, который позволит обезопасить конфиденциальную информацию пользователей от взлома. Свою методику замены для хакеров настоящих данных ложными А. Джуэлс называет Honey Encryption.

Суть метода заключается в том, что общая таблица пользовательских данных, в которой у каждого пользователя есть свой пароль, защищена одним настоящим паролем, а учётные данные конкретных пользователей – ложными.

Когда злоумышленники попытаются воспользоваться ложным паролем, система оповестит пользователя о возможной атаке, и это позволит ему предпринять соответствующие меры.

Honey Encryption предложит хакерам данные, очень похожие на настоящие – это уверит их в успешности осуществлённой атаки. То есть, даже если злоумышленникам удастся взломать компьютер, получить настоящие данные они всё равно не смогут ***(Система защиты информации покажет хакерам ложные «секретные» данные // InternetUA (http://internetua.com/sistema-zasxiti-informacii-pokajet-hakeram-lojnie--sekretnie--dannie). – 2014. – 4.02).***

***

Новый вариант Zeus крадет пароли и шифруется

Вредоносный код Gameover, представляющий собой вариант червя Zeus, ориентированный на кражу паролей, теперь использует шифрование для затруднения работы межсетевых экранов и систем обнаружения вторжения. Антивирусные специалисты говорят, что прежде вредоносные коды редко полностью шифровали собственные коммуникации и появление шифрованных вредоносов может значительно затруднить работу обнаруживающих средств.

Ранее вредоносный код Gameover был замечен в атаках против пользователей Bitcoin в Китае, а также против CryptoLocker. ИТ-аналитик компании Malcovery Security Г. Уорнер говорит, что все варианты Zeus в настоящее время уже детектируются антивредоносными продуктами, поэтому создатели данного вредоноса решили шифровать свою разработку, превратив ее из исполняемого EXE-файла в неисполняемый enc-файл.

По его словам, именно такое расширение и неисполняемая природа кода должны ввести в заблуждение жертв, а для дальнейшей деятельности вредоноса, код просит у пользователей через фишинговый email скачать некое обновление, которое, собственно, и дешифрует вредоносный код из его контейнера. При этом сам код даже после дешифровки продолжит шифровать свои коммуникации, а программа-распаковщик закидывает вредоносный код в неожиданную для пользователя папку.

Венгерская компания CrySys Lab в своем блоге более подробно рассматривает работу кода – http://blog.crysys.hu/2014/02/gameover-zeus-now-uses-encryption-to-bypass-perimeter-security-enc-encryption/ ***(Новый вариант Zeus крадет пароли и шифруется // InternetUA (http://internetua.com/novii-variant-Zeus-kradet-paroli-i-shifruetsya). – 2014. – 5.02).***

***

Троян инфицировал 350 тыс. устройств под управлением Android

Как сообщают исследователи Dr Web, им удалось зафиксировать распространение новой вирусной угрозы для операционной системы Android. Речь идет о трояне Oldboot, который уже успел заразить не менее 350 тыс. мобильных устройств по всему миру. Вместе с тем, отмечают эксперты, вирус явно ориентирован на пользователей из Китая.

Особое внимание к Oldboot, по мнению исследователей, привлекает наличие ряда его компонентов в загрузочном разделе файловой системы Android. Такой буткит-функционал Oldboot значительно повышает его шансы на то, чтобы не быть удаленным из системы.

При включении мобильного устройства вредоносный код, влияющий на последовательность активации компонентов ОС, инициирует работу троянской Linux-библиотеки imei_chk. Последняя, в свою очередь, вносит изменения в каталоги /system/lib и /system/app.

«Наиболее вероятным путем внедрения данной угрозы в мобильные устройства является установка злоумышленниками модифицированной версии прошивки, содержащей необходимые для работы троянца изменения», – поясняют в эксперты, подчеркивая, что пользователям не стоит приобретать Android-устройства сомнительного происхождения или использовать образы операционной системы, полученные из ненадежных источников ***(Троян инфицировал 350 тысяч устройств под управлением Android // InternetUA (http://internetua.com/troyan-inficiroval-350-tisyacs-ustroistv-pod-upravleniem-Android). – 2014. – 6.02).***

***

«Сирийская электронная армия» переписала на себя домен Facebook

Хакеры «Сирийской электронной армии» (SEA) на несколько часов переписали на себя домен социальной сети Facebook. Об этом представители SEA 6 февраля сообщили в своем Twitter.

«С днем рождения, Марк! Facebook.com теперь принадлежит нам!» – говорится в опубликованном хакерами твите, адресованном основателю соцсети М. Цукербергу. Пост сопровождается скриншотом данных Whois с информацией о домене facebook.com. Слова «с днем рождения», судя по всему, адресованы не лично Цукербергу, родившемуся в мае 1984 г., а самой соцсети, отметившей 10-летний юбилей 4 февраля.

Судя по опубликованному снимку, членам SEA удалось изменить графу «электронный адрес владельца». В ней появился имейл «армии»

syrian.es.sy@gmail.com. В качестве места регистрации домена при этом указывалась столица Сирии Дамаск. На момент написания этой заметки данные Whois по домену facebook.com уже были восстановлены.

В августе 2013 г. похожей атаке со стороны «Сирийской электронной армии» подверглась другая социальная сеть – Twitter. Хакерам удалось ненадолго переписать на себя сайт twitter.com, указав в качестве имейла администратора почтовый ящик sea@sea.sy. Таким же образом тогда были изменены регистрационные данные изданий The New York Times и The Huffington Post UK.

Хакерская группировка «Сирийская электронная армия», известная своими атаками на сайты западных медиакомпаний и аккаунты политиков в социальных сетях, выступает на стороне действующего президента Сирии Б. Асада. Участники SEA заявляют, что их действия направлены на то, чтобы отучить западные СМИ от лживой пропаганды, направленной против законных властей Сирии ***(«Сирийская электронная армия» переписала на себя домен Facebook // InternetUA (http://internetua.com/siriiskaya-elektronnaya-armiya--perepisala-na-sebya-domen-Facebook). – 2014. – 6.02).***

***

Злоумышленники используют новый вид распространения вредоносного кода

Как сообщают исследователи из Sucuri, пользователей сети подстерегает новая угроза безопасности в виде встроенного в PNG-изображения вредоносного кода. Данный вид нападения, по словам специалистов, в настоящее время активно и повсеместно используется злоумышленниками.

В ходе инъекции через iFrame на систему загружается файл jquery.js очень небольшого размера, опасность которого было крайне сложно заметить даже самим исследователям. Единственный «тревожный звоночек» в коде файла представляла собой функция loadFile(), которая загружала dron.png в iFrame.

По данным эксперта Sucuri П. Грамантика, загрузка PNG следует за декодирующим циклом. «Так, декодирующий цикл наследует обычное поведение iFrame-инъекции, встраивая ее внутрь метаданных PNG-файла. Таким образом, у нас получается новый механизм распространения», – поясняет эксперт.

Пользователь не замечает, что система подверглась нападению, поскольку iFrame позиционируется за пределами видимого экрана (-1000px). Исследователи подчеркивают, что данный метод нападения позволяет использовать и другие типы изображения ***(Злоумышленники используют новый вид распространения вредоносного кода // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-novii-vid-rasprostraneniya-vredonosnogo-koda). – 2014. – 6.02).***

***

Более 90 % пользователей Интернет обеспокоены конфиденциальностью их информации в сети. Эта цифра с каждым годом возрастает, как утверждают эксперты агентства «ВАРТО», основываясь на данных Harris Interactive.

«Более 30 % пользователей Интернет входят в сеть через прокси-сервера и виртуальные частные сети (VPN), чтобы анонимно пользоваться Интернетом. В Украине обеспокоенность возросла после принятия 16 января процессуальных законов (№ 3879) о дополнительных мерах защиты безопасности граждан» – отмечает Н. Холод, директор агентства маркетинговых коммуникаций «ВАРТО», пишет Marketing Media Review (http://mmr.ua/news/id/bolee-90-polzovatelej-internet-obespokoeny-konfidencialnostju-ih-informacii-38236/).

После прошедших скандалов с публикацией личных данных участились обвинения разработчиков мобильных приложений в умышленно вшитых функциях геолокаций в ОС, позволяющие следить за их владельцем. Интересно, что всплеск обеспокоенности по поводу цифрового обмена данными, возник на почве событий 2013 г., связанных с Э. Сноуденом. Напомним, что в начале июня 2013 г. Э. Сноуден передал нескольким газетам секретную информацию, касающуюся слежки американских спецслужб за информационными коммуникациями между гражданами многих государств при помощи информационных сетей и сетей связи. После его разоблачений люди всерьёз задумались о своей безопасности в сети ***(Более 90 % пользователей Интернет обеспокоены конфиденциальностью их информации // Marketing Media Review (http://mmr.ua/news/id/bolee-90-polzovatelej-internet-obespokoeny-konfidencialnostju-ih-informacii-38236/). – 2014. – 6.02).***

***

Количество Android-вредоносов превысило 10 млн.

«Лаборатория Касперского» подсчитала, что к настоящему моменту ее коллекция вредоносных приложений для Android составляет 10 млн образцов. При этом по итогам января текущего года эксперты компании в общей сложности обнаружили около 200 тыс. уникальных экземпляров вредоносного ПО для мобильных устройств – и это уже на 34 % больше, чем в конце 2013 г., когда в коллекции мобильных зловредов «Лаборатории Касперского» насчитывалось 148 тыс. образцов.

Платформа Android всегда была и продолжает оставаться основной мишенью злоумышленников. Для заражения устройств они избирают разные методы, в том числе создают вредоносные приложения. Так, сегодня официальный магазин Google Play предлагает пользователям более 1 млн приложений, в неофициальных же источниках приложений для Android во много раз больше, однако там они с высокой долей вероятности окажутся вредоносными и опасными.

По данным «Лаборатории Касперского», основанным на анализе мобильных угроз, большинство зловредов для Android разрабатывается злоумышленниками, имеющими российские корни. Примером этого является один из самых опасных мобильных троянцев Carberp, охотившийся за финансовыми данными пользователей Android.

«Несмотря на столь большое число мобильных угроз, в частности для платформы Android, избежать заражения довольно легко, если следовать элементарным правилам информационной безопасности. Прежде всего, не стоит устанавливать никакие приложения из неофициальных источников, а, скачивая программы из официальных магазинов разработчиков, стоит обращать внимание на то, какие права они запрашивают. Не нужно также активировать «режим разработчика» на своем устройстве», – рассказывает Р. Унучек, антивирусный эксперт «Лаборатории Касперского» ***(Количество Android-вредоносов превысило 10 млн // InternetUA (http://internetua.com/kolicsestvo-Android-vredonosov-previsilo-10-mln). – 2014. – 8.02).***

***

Троянец встраивает поддельные формы регистрации во «ВКонтакте»

Эксперты российской компании «Доктор Веб» выявили распространение рекламного троянца, который встраивает в просматриваемые пользователем страницы социальных сетей поддельные формы для ввода паролей и таким образом крадет учетные данные, говорится в сообщении компании.

Эксперты выяснили, что троянец похищает учетные данные для доступа к социальным сетям «ВКонтакте», «Одноклассники», а также к сервисам порталов yandex.ru и mail.ru.

Согласно сообщению, программа Trojan.Admess.1 распространяется преимущественно с помощью вредоносной партнерской программы installmonster.ru (zipmonster) и маскируется под проигрыватель Adobe Flash. Троянец устанавливается как надстройка к браузерам Microsoft Internet Explorer, Mozilla Firefox, Opera и Google Chrome, а после успешной установки в инфицированной системе также может подменять рекламные модули при просмотре пользователем различных веб-страниц.

Trojan.Admess.1 обладает специальными настройками для вывода рекламных баннеров на некоторых особенно популярных и посещаемых интернет-ресурсах: среди них – mail.ru, «ВКонтакте» (vk.com), «Одноклассники» (odnoklassniki.ru), yandex.ru, yandex.ua, yandex.by, youtube.com, zaycev.net и ряд других. Но даже при посещении сайтов, отсутствующих в списке «привилегированных», вредоносная программа все равно встраивает в них свои рекламные блоки.

Для демонстрации рекламы троянец Trojan.Admess.1 загружает информацию из нескольких рекламных сетей, замеченных в раскрутке сайтов-распространителей вредоносного программного обеспечения,

подозрительных и нежелательных приложений, а также рекламирующих порносайты и мошеннические интернет-ресурсы ***(Троянец встраивает поддельные формы регистрации во «ВКонтакте» // InternetUA (http://internetua.com/troyanec-vstraivaet-poddelnie-formi-registracii-vo--vkontakte). – 2014. – 7.02).***

***

Сайт противников Сочинской олимпиады nosochi2014.com заражен трояном, сообщили CNews в «Лаборатории Касперского».

Троян, распространяемый через сайт nosochi2014.com, в номенклатуре «Касперского» отмечен как Trojan-Spy.Win32.Zbot.rkie, рассказал CNews Р. Стоянов, руководитель отдела расследования компьютерных инцидентов «Лаборатории Касперского».

Семейство троянов Zbot, предназначенных для кражи банковской информации, хранящейся на компьютере жертвы, было впервые обнаружено в августе 2013 г. Его активность на антиолимпийском сайте была зафиксирована 4 февраля 2014 г.

«Такие глобальные события, как Олимпийские игры неизбежно привлекают повышенное внимание злоумышленников – подобные примеры многократно наблюдались в ходе предыдущих соревнований. Посетители и болельщики сочинской Олимпиады могут столкнуться с самыми разными угрозами. Это могут быть поддельные веб-сайты, маскирующиеся под официальные ресурсы Олимпийских игр, – через них мошенники могут продавать поддельные билеты или осуществлять сбор персональных данных посетителей. Также болельщикам на почту или в социальные сети могут приходить сообщения с вложениями, содержащими вредоносное ПО или с ссылками, ведущими на зараженные сайты», – говорит Р. Стоянов.

«Касперский» традиционно рекомендует во время Олимпиады соблюдать правила элементарной осторожности в сети: не открывать нежелательные письма от незнакомых людей, не проходить по подозрительным ссылкам и, безусловно, обновлять антивирусное ПО на своем компьютере.

Сайт nosochi2014.com, как понятно из его названия, посвящен контрпиару Олимпийских игр в Сочи. Основной претензией организаторов сайта к Олимпиаде стало место и время ее проведения. 1864 г. считается условной датой завершения русского завоевания Кавказа, а территории в районе Сочи и Красной поляны – условным местом ее окончания.

Национальные черкесские организации увязывают проведение Олимпиады-2014 со 150-летием капитуляции черкесских племен перед русским императором.

Домен nosochi2014.com зарегистрирован в 2010 г. Сам сайт хостится в штате Юта и ведется на английском языке.

Сайт nosochi2014.com обновляется нерегулярно. Последний опубликованный на нем пресс-релиз относится к июлю 2012 г., а последняя

новость – к середине декабря 2013 г. Она посвящена выступлениям черкесских активистов в Турции.

Можно вспомнить, что кибергруппировка «Кавказские анонимусы» (Anonymous Caucasus), которая пыталась атаковать сайты крупнейших российских банков в октябре 2013 г., также увязывала свою деятельность с Олимпиадой в Сочи и 150-летием «геноцида кавказских народов» ***(На сайте nosochi2014.com хакеры похищают банковскую информацию посетителей // InternetUA (http://internetua.com/na-saite-nosochi2014-com-hakeri-pohisxauat-bankovskuua-informaciua-posetitelei). – 2014. – 7.02).***

***

«Сирийская электронная армия» взломала eBay

Про-сирийская хакерская группа «Сирийская электронная армия» сегодня предоставила данные о том, что ее участникам удалось перехватить закрытые коммуникации работников интернет-компании eBay, когда они захватили контроль над британским сайтом eBay. Напомним, что о проблемах на сайте eBay.co.uk стало известно в понедельник на этой неделе, но сама компания заявила, что никакого взлома не было, а были лишь проблемы с DNS-серверами.

Судя по приведенным данным, участникам хакерской группы удалось перехватить данные, говорящие о том, что сотрудники eBay обнаружили факт взлома и общаются друг с другом на эту тему. Сообщение датировано 1 февраля и относится не только к британскому eBay, но и к платежной системе PayPal, которая также стала жертвой взломщиков.

Сегодня пресс-служба eBay подтвердила, что в воскресенье и понедельник хакерам удалось на непродолжительное время получить контроль над сервисами компании, причем атака была не только на британские, но также и на французские и индийские сайты eBay и PayPal. В пресс-службе отказались комментировать подлинность опубликованных «Сирийской электронной армией» переписок сотрудников интернет-компании.

Напомним, что за несколько дней до инцидента с eBay, стало известно о том, что «Сирийская электронная армия» получила письма ряда сотрудников Microsoft, а кроме того, атаковала DNS-серверы хостинговой компании GoDaddy ***(«Сирийская электронная армия» взломала eBay // InternetUA (http://internetua.com/siriiskaya-elektronnaya-armiya--vzlomala-eBay). – 2014. – 6.02).***

***

Согласно опросу, проведенному ThreatTrack Security, утечки секретных данных АНБ, организованные Э. Сноуденом, привели к тому, что подрядчики оборонных компаний существенно изменили подходы к вопросам ИБ.

Опубликованный отчет показывает изменения, которые наступили в американских организациях за последнее время. Так, в 75 % случаев практики защиты информационных систем изменились в одну из указанных ниже сторон:

55 % организаций обеспечили дополнительное обучение по вопросам ИБ для своих сотрудников;

52 % организаций пересмотрели уровень доступа к информации для своих сотрудников;

47 % компаний стали уделять больше внимания нестандартному поведению сотрудников в сети;

41 % компаний ввели более жесткие требования при найме новых сотрудников;

39 % компаний сократили права по администрированию IT-систем своим сотрудникам.

Помимо этого, больше половины респондентов (63 %) заявили о том, что в их организациях присутствует классификация по уровням доступа к информации.

Подавляющее количество респондентов считает, что государство обеспечивает их всей необходимой поддержкой для защиты конфиденциальных данных. При этом в 62 % компаний обеспокоены APT-угрозами, вероятностью осуществления целевых атак, а также использования злоумышленниками сложных современных шпионских программ.

В дополнение, 29 % участников опроса пожаловались на недостаточное финансирование для обеспечения защиты корпоративных систем ***(Разоблачения Сноудена привели к улучшению уровня IT-безопасности в частных компаниях // InternetUA (http://internetua.com/razoblacseniya-snoudena-priveli-k-ulucssheniua-urovnya-IT-bezopasnosti-v-csastnih-kompaniyah). – 2014. – 7.02).***