СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(24.03–6.04)

2014 № 7

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(24.03–6.04)
№ 7

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

Украинские социальные сети множатся, как санкции США и ЕС по отношению к России. Только за последние две недели было анонсировано пять проектов, которые, по словам их разработчиков, составят серьезную конкуренцию ресурсам М. Цукерберга и П. Дурова. Общее же число национальных соцсетей давно перевалило за десяток. AIN.UA подготовил подборку с кратким описанием последних творений украинских программистов (http://ain.ua/2014/04/04/518701).

WEUA.info

Эпидемия соцсетей в Украине началась 21 марта, когда был анонсирован проект WEUA.info. На момент написания публикации по этому адресу находится страница с презентацией соцсети под слоганом «Я переезжаю». В этом суть запуска: авторы надеются, что пользователи откажутся от использования российских социальных сетей, в которых их ждет антиукраинская пропаганда. «Команда WEUA 19.03.2014 г. объявляет всеукраинский бойкот российских социальных сетей “ВКонтакте” и “Одноклассники”. Просим присоединиться всех неравнодушных», – пишут создатели в презентации WEUA. Соцсеть должна была запуститься несколько дней назад, но старт проекта отложили из-за хакерских атак.

Друзі

Спустя несколько дней после анонса WEUA на просторах уанета появилась еще одна социальная сеть. Ресурс называется «Друзі» и расположен по адресу: druzi.org.ua. На сегодня в новой соцсети зарегистрировано свыше 2 тыс. пользователей, и эта цифра постоянно растет. Интерфейс сайта внешне напоминает Facebook и «ВКонтакте». Одним из серьезных отличий является то, что в качестве основного языка страницы можно выбрать только украинский. В ближайшее время администраторы ресурса собираются ограничить доступ к социальной сети пользователям из других стран.

Antiweb.com.ua

Социальная антисеть для жителей Ровно. По словам разработчиков, с ее помощью можно будет находить друзей по интересам. Для этого на сайте можно будет создавать встречи и ставить им определенные метки. Например: «Собираемся на концерт группы Metallica, только парни от 18 лет, встреча без употребления алкоголя». После окончания встречи ее можно будет оценить по пятибальной шкале и опубликовать фотографии. Оценки помогут антисети в дальнейшем рекомендовать пользователю события, которые могут быть ему потенциально интересны. Первое время сеть планируют сделать доступной только для жителей Ровенской области.

Ukrface.net

Регистрация в этой соцсети должна начаться 5 апреля в 12:00. Ее создатели уверены, что проект нужен для объединения востока и запада

страны в борьбе против иностранной антиукраинской пропаганды. Сайт будет выполнен в трех цветах: синем, желтом и черном. Судя по скриншотам, UkrFace тоже будет очень похож на «ВКонтакте» и Facebook. В новой украинской соцсети будут все те же функции: профиль, друзья, музыка, фото, видео, обложка, а еще фон страницы и общий чат.

Combine.pp.ua

Еще одна «первая украинская соцсеть». Написать про нее что-то оригинальное сложно.

Кроме вышеназванных соцсетей, в Украине с переменным успехом существует еще около десятка действующих и полузаброшенных проектов. Помимо относительно известных Connect.ua и Friends.ua, есть еще соцсеть «Українці», сайт для «реальных пацанов» vReale, соцсеть для женщин Pink Planet, для ученых – Science-community.org и торговая соцсеть Kb.ua. Не выдержали конкуренции и закрылись соцсеть для шоу-бизнеса Katmary.net, сеть для «тусовщиков» Tuse.ua, соцсеть для профессионалов Profeo.com.ua и Friendin.net, в которую, по словам создателей, инвесторы вложили 1,5 млн дол. ***(Пять украинских социальных сетей, созданных за последние две недели // AIN.UA (http://ain.ua/2014/04/04/518701). – 2014. – 4.04).***

***

Соціальна мережа weua сподівається зареєструвати понад мільйон українських користувачів за 30 днів роботи. Про це під час прес-конференції повідомив засновник інтернет-спільноти weua.info Б. Оліярчук, передає кореспондент STR.

«Маркетингова група мережі weua.info очікує привітати мільйон користувачів уже в кінці квітня. Всього у нашій штатній команді працює 22 особи, що наполегливо працюють над втіленням цього плану», – зазначив він.

За словами експерта, на сайті мережі буде заборонена будь-яка діяльність інтернет-сепаратистів, веб-тітушок, а також розміщення порнографічного контенту.

Нагадаємо, за задумкою розробників, ресурс буде відрізнятися від інших публічним авторським договором від українських митців на використання музики та відео ***(«Перша патріотична» соцмережа планує за місяць зібрати мільйон користувачів // Страйк UA – Первый социальний портал (http://www.socportal.info/news/persha-patriotichna-sotsmerezha-planuye-za-misyats-zibrati-milyon-koristuvachiv). – 2014. – 1.04).***

***

«З метою зменшення впливу Росії на український інформаційний простір у Всесвітній мережі Інтернет, виділити фінансування на запуск Національної Соціальної Мережі», – ідеться в рішенні Ради національної безпеки і оборони від 31 березня.

У понеділок, 31 березня РНБО прийняла рішення про запуск амбітного проекту – створення власної соціальної мережі та електронної пошти. Рішення отримало статус невідкладного і набуло чинності 1 квітня.

У рішенні РНБО мова йде про велику залежність українського інформаційного простору від російських інтернет-компаній. «Чотири з 5 найпопулярніших сайтів, які відвідали українці в 2013 р., належать російським компаніям: “ВКонтакте”, Mail.ru, “Яндекс”, “Одноклассники”, які забезпечують просування інтересів Російської Федерації в мережі Інтернет, – ідеться в повідомленні, розміщеному на сайті РНБО.

До створення НСМ буде залучено низку відомств – МВС, МОН, Нацагентство з питань держслужби, Держспецзв’язку, Держінвест. Також у структурі проекту передбачається участь уже недержавного Укртелекому. Але найцікавіше, що в презентації, викладеній на сайті РНБО, серед учасників вказано і маловідому компанію Digital Fotress.

Більшості українців ця назва нічого не говорить. Але таку ж назву має американська компанія, що належить засновнику соцмережі «ВКонтакте» П. Дурову.

П. Дуров створив Digital Fortress у 2013 р., ІТ-директор компанії – А. Нефф, який також є помічником директора «ВКонтакте» з міжнародних операцій. Офіс компанії розташовано в Буффало, штат Нью-Йорк. Компанія минулого року запустила месенджер «Телеграм», яким уже користується кілька десятків мільйонів користувачів у світі.

Яка роль Digital Fortress у запуску НСМ – не відомо. Можливо, саме ця компанія буде розробляти код. А можливо це буде переписаний код соціальної мережі «ВКонтакте».

Передбачається, що бета-тестування Національної Соціальної Мережі завершиться в IV кварталі 2014 р.. Скільки коштуватиме держбюджету запуск – не вказано, але фінансування буде здійснюватись через Держінвест.

На першому етапі до системи буде підключено студентів, міліцію та держслужбовців – це майже 2,5 млн користувачів.

Ще один цікавий момент – НСМ буде інтегрована з «Національною електронною поштою». У документі вказано, що вже ведуться переговори з Google та Майкрософт щодо співпраці. Держава очікує безкоштовно реалізувати амбітний проект створення власної електронної пошти в обмін на зобов’язання про прив’язку своїх продуктів до однієї з операційних систем – Android або Windows. Правда, не зрозуміло, як буде працювати середньостатистичний держслужбовець на комп’ютерах з ОС Android. Хіба, усім закуплять Хромбуки.

Очікується, що всі українці матимуть свою унікальну електронну адресу, через яку можна буде здійснювати офіційне спілкування з органами державної влади та взаємодіяти із системою електронного документообігу. Наприклад, запит, надісланий у ЖЕК з адреси користувача в «Національній Електронній Пошті», – буде автоматично включено в систему електронного документообігу.

Поки що не зрозуміло, чому центром комунікації є НСМ, а не НЕП. Можливо, пошта буде тісно інтегрована в соцмережу і стане її невід'ємною частиною ***(Дуров допоможе уряду України запустити українську соціальну мережу // UkrainianWatcher (http://watcher.com.ua/2014/04/01/durov-dopomozhe-uryadu-ukrayiny-zapustyty-ukrayinsku-sotsialnu-merezhu/). – 2014. – 1.04).***

***

Названы самые популярные среди украинских студентов соцсети

Около 95 % украинских студентов хотя бы раз в неделю заходят в свои аккаунты в социальных сетях, а больше половины (57 %) – имеют аккаунты сразу на нескольких подобных сайтах. Таковы результаты исследования сайта rabota.ua, которое проводилось в декабре 2013 г. (выборка – студенты вузов и выпускники от 18 до 25 лет, 5540 респондентов, из них 36 % – из Киева), пишет ubr.ua.

Вполне ожидаемо, самой популярной сетью среди украинских студентов стала «ВКонтакте», но число поклонников Facebook и LinkedIn также быстро растет. В то же время «Одноклассники» теряют аудиторию среди украинской молодежи:

Какой из указанных социальных сетей Вы пользуетесь? (динамика за 4 года)

Соц. сеть	2010	2011	2012	2013
vk.com / vkontakte.ru	87%	90%	90%	91%
facebook.com	23%	49%	47%	49%
odnoklassniki.ua	27%	32%	27%	18%
linkedin.com	1%	5%	7%	12%
connect.ua	4%	5%	1%	1%
Другие	9%	6%	3%	3%
Ни одной	2%	5%	5%	5%

Больше всего украинских студентов в сетях интересуют группы, связанные с музыкой, хобби, развлечениями и спортом.

Чаще всего ищут информацию о развлечениях. Но при этом в топ-8 популярных среди студентов тематик входят предложения о работе и данные о работодателях ***(Названы самые популярные среди украинских студентов соцсети // IT Expert (http://itexpert.org.ua/rubrikator/item/34626-nazvany-samye-populyarnye-sredi-ukrainskikh-studentov-sotsseti.html). – 2014. – 23.03).***

***

Twitter частенько экспериментирует с новыми функциями, некоторые из которых не доживают до релиза, а другие – распространяются впоследствии на всех пользователей.

В этот раз Twitter решил вывести на чистую воду всех, кто кичится большой и активной аудиторией – несколько пользователей приложения под iOS и Android сообщили, что в Twitter теперь отображается количество просмотров для каждого твита.

Прежде у сервиса не было ни одной метрики, которая бы показывала, сколько людей на самом деле видят ваши твиты – ведь ретвиты и «звёздочки» представляют собой крайне опосредованный показатель (хотя у рекламодателей схожая возможность есть).

Такой показатель может быть весьма болезненным для многих, если окажется, что при относительно большом количестве фолловеров твиты всё равно почти никто не видит. Или ещё хуже – твиты видят почти все, но реакция на них нулевая.

И если для кого-то Twitter остаётся лишь средством для того, чтобы выговориться (пускай даже в темноту), то для таких людей будет очень обидным узнать, что их на самом деле слышат все, но никто не обращает внимания.

Такая демотивация пользователей может стать причиной к тому, чтобы не выкатывать обновление на всех, а свернуть эксперимент.

С другой стороны, для Twitter как для компании это очередной способ заставить людей постить больше – не так давно сервис стал уведомлять пользователей, когда кто-то ретвитит или фаворитит ретвитнутый ими пост, а теперь сможет ещё и показывать количество просмотров. Это всё мотивирует твитить ещё и ещё, прекрасно осознавая, сколько людей это замечают ***(Twitter будет показывать количество просмотров отдельных твитов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_budet_pokazyvat_kolichestvo_prosmotrov_otdelnyh_tvitov). – 2014. – 24.03).***

***

Соцмережа Facebook запустила нову функцію, за допомогою якої можна заблокувати пости, які мають слова, що дратують, пише Корреспондент.net (http://ua.korrespondent.net/tech/technews/3323697-u-Facebook-teper-mozhna-pozbutysia-postiv-zi-slovamy-yaki-dratuuit).

Такий додаток до Google Chrome діє за принципом «стоп-слова».

Наприклад, можна додати слово «Росія», і пости в стрічці з таким словом не будуть висвітлюватися.

Щоб почистити стрічку Facebook, потрібно встановити спеціальний додаток-фільтр ***(У Facebook тепер можна позбутися постів зі словами, які дратують // Корреспондент.net (http://ua.korrespondent.net/tech/technews/3323697-u-Facebook-teper-mozhna-pozbutysia-postiv-zi-slovamy-yaki-dratuuit). – 2014. – 24.03).***

***

Число ежемесячно активных пользователей сервиса для размещения фотографий и коротких видеороликов Instagram превысило 200 млн, за последние полгода аудитория возросла на треть, говорится в сообщении Instagram. Об этом передает IT Expert.

В сентябре 2012 г. Facebook завершила сделку по покупке Instagram чуть меньше чем за один миллиард долларов. Примерно полгода назад компании объявили, что аудитория Instagram насчитывает 150 млн пользователей, однако с тех пор Facebook не раскрывала динамику показателей Instagram.

«На сегодняшний день мы пересекли отметку в 20 млрд фотографий, загруженных на Instagram», – сообщается в блоге сервиса. Ранее число снимков, которыми пользователи поделились с подписчиками, оценивалось в 16 млрд.

Ежедневно пользователи публикуют по 60 млн фотографий и оставляют 1,6 млрд отметок «Мне нравится» (Like) – полгода назад эта активность оценивалась в 55 млн и 1,2 млрд лайков соответственно ***(Глобальная аудитория Instagram превысила 200 миллионов пользователей // IT Expert (http://itexpert.org.ua/rubrikator/item/34700-globalnaya-auditoriya-instagram-prevysila-200-millionov-polzovatelej.html). – 2014. – 27.03).***

***

В то время как большинство социальных сетей – это возможность общаться с друзьями, задача нового приложения Cloak («Плащ») прямо противоположна: оно помогает людям избежать общества друзей и знакомых, пишет bin.ua.

Приложение Cloak использует информацию из таких социальных сетей, как Foursquare и Instragram, чтобы установить, где находятся ваши знакомые в данный момент времени, и предупреждает вас, если они где-то поблизости. Cloak – представитель новой, набирающей популярность разновидности «антисоциальных» приложений, обеспечивающих анонимность клиента.

Также все более популярными становятся приложения Snapchat и Secret. В Snapchat фотографии и видео автоматически удаляются через считанные секунды после их просмотра, а в приложении Secret сообщения выводятся на экран анонимно. Все они, также как и приложение WhatsApp, купленное недавно компанией Facebook за 19 млрд дол., свидетельство того, что все большее число пользователей Интернета предпочитают открытому общению конфиденциальные коммуникации в режиме онлайн.

Приложение Cloak предлагается пользователям в качестве метода, позволяющего «избежать встречи с вашим бывшим, с коллегами или с тем чересчур надоедливым парнем, иными словами – со всеми, с кем бы вам не хотелось столкнуться лицом к лицу».

Приложение было создано программистом Б. Муром и бывшим креативным директором новостного сайта Buzzfeed К. Бэйкером.

В интервью газете Washington Post К. Бэйкер отметил, что сервис Cloak следует тенденции, характерной для социальных сетей.

«Как мне кажется, мы наблюдаем появление нового вида социальных сетей, – сказал К. Бейкер. – Twitter и Facebook напоминают переполненные людьми кабины лифта... Я думаю, что в настоящее время на подъеме находятся альтернативные приложения».

Главный редактор журнала App Н. Джонс сказал, что он пока не окончательно убежден в значимости этой новинки, хотя и считает ее занимательной.

«Приложение кажется мне хитроумной уловкой, призванной привлечь внимание своей новизной. Но, возможно, я и сам стану его использовать», – поделился он.

По его словам, подобные нишевые приложения разрабатываются не потому, что на них уже есть покупательский спрос, а из-за того, что разработчики хотят завоевать последние нетронутые территории на рынке социальных медиа.

«Разработчики делают свои приложения более разнообразными, находят для этого какой-то уникальный ракурс, после чего продают их компании Facebook и получают за это хорошие деньги», – заметил Н. Джонс.

Тем не менее он признал то, что предлагаемая подобными приложениями скрытность имеет свои преимущества и может оказаться привлекательной для многих ***(Приложение «Плащ» поможет спрятаться от друзей // IT Expert (http://itexpert.org.ua/rubrikator/item/34645-prilozhenie-plashch-pomozhet-spryatatsya-ot-druzej.html). – 2014. – 24.03).***

***

Число пользователей Facebook, которые ежемесячно заходят в соцсеть с мобильных устройств, превысило 1 млрд – более 80 % от общей численности аудитории Facebook, заявил гендиректор соцсети М. Цукерберг.

Как сообщает IT Expert со ссылкой на Digit.ru, новую статистику М. Цукерберг огласил в ходе конференц-звонка, посвященного покупке компании Oculus VR – производителя очков дополненной реальности Oculus Rift. Как сообщал Digit.ru, по итогам 2013 г. активная мобильная аудитория Facebook насчитывала 945 млн пользователей – таким образом, за январь – март она прибавила 55 млн.

Общее число пользователей Facebook, по последним данным, оценивается в 1,23 млрд. Таким образом, ежемесячно активная мобильная аудитория составляет более 80 % от этого числа.

Рост мобильной аудитории принципиально важен для Facebook, поскольку мобильные сервисы – главный приоритет соцсети на сегодняшний день. Мобильная реклама принесла Facebook 40 % выручки по итогам 2013 г., а практически любое публичное заявление руководства соцсети о

нововведениях в мобильной сфере ведет к росту котировок на фондовой бирже.

Глава соцсети М. Цукерберг ранее заявлял, что Facebook намерена сконцентрироваться на разработке самостоятельных мобильных приложений. Сейчас таковыми в составе компании, помимо сервиса для размещения фото и видео Instagram, являются Messenger, Poke, программная оболочка Facebook Home, а также новый сервис-агрегатор новостей Paper ***(Более миллиарда пользователей сегодня заходят в Facebook с мобильных // IT Expert (http://itexpert.org.ua/rubrikator/item/34699-bolee-milliarda-polzovatelej-segodnya-zakhodyat-v-facebook-s-mobilnykh.html). – 2014. – 27.03).***

***

В мобильной версии Twitter появилась возможность просмотра видео прямо из ленты новостей

Еще совсем недавно просмотр прикрепленных видео в мобильных приложениях Twitter был настоящим мучением. Необходимо было переходить по ссылке, а там видео могло не открыться, воспроизводиться с рывками и «радовать» другого рода проблемами. Теперь же после обновления программы (неважно – на Android или на iOS) в информационной ленте на месте вставленных видеофрагментов будут появляться специальные ярлычки. При нажатии на последние воспроизведение прикрепленных клипов начнется незамедлительно.

Данное нововведение значительно облегчит жизнь тем компаниям или известным людям, у которых сфера деятельности неразрывно связана с демонстрацией видеоматериалов. Ну, конечно, и для рядового пользователя реализованная система просмотра видео прямо из приложения позволит, как минимум, беспрепятственно рассматривать неунывающих котят и т. д. ***(В мобильной версии Twitter появилась возможность просмотра видео прямо из ленты новостей // InternetUA (http://internetua.com/v-mobilnoi-versii-Twitter-poyavilas-vozmojnost-prosmotra-video-pryamo-iz-lenti-novostei). – 2014. – 26.03).***

***

Twitter продолжает развивать социальные функции, постепенно отказываясь от прежнего минимализма и превращаясь из сервиса микроблогов в аналог Facebook. Очередной шаг в этом направлении касается фотографий.

Теперь, используя последнюю версию официального приложения Twitter для iPhone, можно добавить в каждый твит до четырех фотографий. Из них будет автоматически создан коллаж, который можно просмотреть в увеличенном виде, нажав на отображаемую в твите уменьшенную и обрезанную копию. Вскоре функция появится и в клиенте для Android, а также в веб-интерфейсе сервиса по адресу: twitter.com.

Кроме того, в Twitter с сегодняшнего дня появилась возможность отмечать в твитах других пользователей, уже давно присутствующая во многих других соцсетях, включая Facebook и Instagram. В каждом твите может быть отмечено до 10 человек. При этом отметки никак не влияют на доступное число знаков в твите.

Чтобы предотвратить использование новой функции спамерами, в настройках аккаунта Twitter можно указать, кому позволено отмечать вас в твитах, а также хотите ли вы получать оповещения об отметках ***(Twitter продолжает обрастать функциями из Facebook // InternetUA (http://internetua.com/Twitter-prodoljaet-obrastat-funkciyami-iz-Facebook). – 2014. – 27.03).***

***

Собачка, постоянно мелькающая в рекламе социальной сети «ВКонтакте», превратится в стикер. Об этом сообщил Г. Лобушкин, пресс-секретарь.

«Пользователи постоянно требуют чего-то нового. Смайликов уже недостаточно – что же, мы предлагаем стикеры», – сказал Г. Лобушкин. Стикер – картинка с какой либо эмоцией. От смайликов они отличается тем, что у стикера есть так называемый «главный персонаж». В случае с «ВКонтакте» – это милый песик.

Диапазон эмоций будет колоссальным – в общей сложности в планах запустить около 150 видов стикеров. На большей части из них будет собачка, но также будут картинки с различными «улыбающимися» фруктами, овощами и даже с рыжим котом. Почему именно с котом, да еще и с рыжим – руководство «ВКонтакте» не сообщает.

Все стикеры будут разделены на четыре тематические группы. Две из них будут в свободном доступе, две – платные. По предварительным данным, стоимость картинки составит 66 р. «Мы уверены, что платные стикеры станут такими же популярными, как и “подарки”, – утверждают представители сети. – Но заработок – далеко не главная цель нововведения. В первую очередь мы собираемся привлечь новых пользователей и, конечно же, порадовать “старых”».

Использовать стикеры можно будет в диалогах, в постах, в группах – везде, где уже используются смайлы. Первую партию «картинок» пользователи в своих инструментах смогут увидеть в конце этой или в начале следующей недели ***(Стикеры: новинка от ВКонтакте! // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/stikery_novinka_ot_vkontakte). – 2014. – 27.03).***

***

Издание The Wall Street Journal со ссылкой на свои источники в Twitter сообщает о том, что в скором времени сеть микроблоггинга презентует

обновленную стратегию в области музыки. Неделю назад Twitter отозвала из Apple App Store ее неудавшееся музыкальное приложение.

WSJ сообщает, что в Twitter было принято решение отказаться от собственного музыкального плеера, встраиваемого в блоги, но вместо него компания ведет переговоры с рекорд-лейблами, чтобы предложить пользователям своего ресурса подписной музыкальный сервис. Ранее Twitter уже встречалась с менеджментом Beats Music на предмет обсуждения музыкальной стратегии, а также с руководством онлайн-платформы SoundCloud.

Источники в Twitter также сообщили, что компания работает с Vevo (совместное предприятие Universal Music и Sony Music) над программой музыкального партнерства на Twitter.

WSJ отмечает, что музыка уже занимает значительную часть Twitter, хотя компания-оператор для этого пока ничего особенного не сделала. Так, Twitter-ленты музыкальных исполнителей насчитывают десятки миллионов фолловеров, пользователи здесь постоянно обсуждают музыкальные новинки, а сами околомузыкальные тематики стабильно входят в десятку самых обсуждаемых тем в соцсети ***(Twitter разрабатывает музыкальную стратегию // InternetUA (http://internetua.com/Twitter-razrabativaet-muzikalnuua-strategiua). – 2014. – 27.03).***

***

Twitter в настоящее время тестирует еще одну функцию, которая вполне может оказаться популярной среди множества пользователей. Новинка, под названием Fave People («Избранные люди»), позволит с легкостью создать отдельную вкладку для списка ваших любимых пользователей Twitter.

Графа Fave People будет находиться рядом с Discover и Activity, таким образом, делая более удобным и быстро доступным доступ к пользователям, занесенным в этот список – всего пару нажатий.

Аналогично, новая функция Fave People проста и в создании. Для этого нужно лишь нажать на иконку-звездочку в профиле пользователя, которого хотите добавить. Кроме того, можно выбрать настройки для получения уведомлений в случае, когда кто-то из вашего списка Fave People публикует какой-нибудь твит.

Конечно, в настоящее время для данной потребности можно использовать Lists Twitter (Списки), при помощи которых создается топ пользователей, но Twitter считает, что такое новое отделение – одна из функций, которую многие пользователи хотели бы видеть на своих страницах из-за простоты и удобства.

На сегодняшний день новинка появилась в альфа-версии приложения Twitter – версия Twitter для Android, где новые идеи проходят тестирование, прежде чем их предоставят для бета-версии. Когда Fave People будет усовершенствована и полностью протестирована, то можно ожидать, что она

станет доступна всем пользователям в недалеком будущем. Тем не менее, в обратном случае, мы никогда, вероятно, и не услышим о Fave People снова ***(В Twitter появится новая функция «Fave People» («Избранные люди») // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_twitter_poyavitsya_novaya_funktsiya_fave_people_izbrannye_lyudi). – 2014. – 27.03).***

***

Хотя такие ресурсы Facebook, Twitter и «ВКонтакте» подталкивают участников обзавестись множеством виртуальных знакомых, тенденция иметь сотни человек в списке друзей может пойти на убыль. Некоторые пользователи, особенно молодежь, хотят общаться в своем маленьком кругу реальных людей. Там они будут делиться важными новостями, а через традиционные соцсети будут рассылать малозначащие картинки и репосты.

Одно из свидетельств подобной тенденции – увеличивающаяся популярность таких сервисов, как Snapchat, Vine, WeChat и др. По сравнению с, например, Facebook (свыше 1,2 млрд человек) и Twitter (240 млн) они выглядят просто крошечными. Однако это и делает их привлекательными в глазах пользователей. А также то, что они поощряют общение с индивидуальными собеседниками или с маленькими группами по сравнению с крупными соцсетями.

«Я думаю, пока еще рано говорить о том, что пользователи будут уходить из больших социальных сетей, – комментирует тенденцию профессор журналистики в Университете Миннесоты Ш. Тиель-Штерн. – Но точно можно сказать, что аудитория соцсетей уже фрагментирована».

Пользователям очень нравятся возможности, которые им дают альтернативные инструменты общения. Согласно исследованию GlobalWebIndex, чаще всего молодежь инсталлировала приложение сети Vine (позволяет создавать короткие видеоклипы) и WeChat (обеспечивает текстовое и голосовое общение). Последнее, например, за год увеличило базу своих пользователей на 1021 %, среди которых преимущественно были подростки.

При этом они стали реже пользоваться соцсетями: активно работает с Facebook лишь 56 % опрошенных, тогда как в начале прошлого года эта цифра составляла 76 %. Эти данные подтверждают и представители соцсети. «Мы наблюдали уменьшение числа ежедневных пользователей, особенно, среди молодежи», – сказал финансовый директор Facebook Д. Еберсманн.

Большой уступает дорогу маленькому

Эксперты объясняют снижение популярности крупных соцсетей у молодых пользователей тем, что это уже не модно. Именно в этом, по их мнению, кроется причина того, что мобильные клиенты для Snapchat, Instagram и Vine загружали значительно чаще из магазина утилит Apple, чем приложения Twitter и Facebook.

«Молодые люди всегда ищут новые модные вещи, но теперь, когда их родители и дедушки с бабушками пользуются соцсетями, последние утратили статус модных, – говорит Ш. Тиель-Штерн. – Кроме этого, молодые люди хотят пользоваться приложениями, которые комбинируют визуальную и социальную составляющие, а также сохраняют мобильность. Они носят телефоны, которые настроены на съемку фото и видео и они хотят делиться полученным материалом необычным способом».

Попытки ограничить круг

Исследовательское агентство Pew Research Internet Project провело опрос молодежи о том, почему им уже не нравится так сильно Facebook. Большинство ответило, что из-за растущего количества взрослых, а также слишком интенсивном обмене сообщениями. Правда, при этом они не собираются отказываться от этой соцсети вообще. Просто те, кто имеет более 600 пользователей, пользуются также другими утилитами.

Одной из таких является соцсеть Path, которую в 2010 г. создал выходец из Facebook Д. Морин. Ее задачей, помимо традиционных для социалок, является ограничение числа друзей у пользователя: их можно иметь не больше 150 человек.

Такое число создатель выбрал согласно с теорией психолога и антрополога Оксфордского университета Р. Данбара. Он считал, что человеческий мозг физически способен удержать лишь 150 стабильных взаимоотношений. Ведь поддерживать социальные отношения, пускай даже виртуальные, тоже требует энергии. Многие пользователи жалуются на усталость от того количества усилий, которые им приходится прилагать для этого в больших соцсетях.

Выбранный Path подход оказался успешным, и сегодня число ее зарегистрированных участников составляет 25 млн.

Слово специалистам

«Некоторые социальные сети стали такими большими, что им уже не хватает социальности, – говорит профессор телекоммуникаций Университета Джорджии И. Химельбоим. – Человек просто не способен поддерживать отношения с более, чем несколькими десятками друзей, будь то онлайн или офлайн».

Для многих пользователей Facebook и Twitter, по мнению эксперта, превратились в инструмент для трансляции информации, который позволяет удобно оповещать большие группы людей о событиях. Но при этом мало кто делится личными мыслями. «Маленькие социальные приложения, особенно те, что фокусируются на интересах или умениях, могут стать альтернативой. В них пользователи смогут управлять своей социальной сетью и инвестировать в межличностные отношения», – отмечает И. Химельбоим.

«Twitter и Facebook… это как большие аудитории для публичных выступлений, – говорит сооснователь анонимного социального мессенджера Cloak Б. Мур. – Поэтому появление Snapchat было глотком свежего воздуха». Snapchat позволяет пользователям обмениваться фотографиями и

посланиями, которые исчезают через несколько секунд, поэтому не нужно бояться, что его увидит кто-то еще.

Автор книги «Социальные медиа, притворные друзья и ложь фальшивой приватности» Д. Байер тоже считает, что популярные соцсети стали слишком большими. «Их главная идея в том, что общение с большим числом людей лучше, чем с маленьким. Я всегда верил, что это правда, однако теперь уже не уверен в этом», – говорит писатель ***(Общение в соцсетях: пользователи хотят меньше публичности // InternetUA (http://internetua.com/obsxenie-v-socsetyah--polzovateli-hotyat-menshe-publicsnosti). – 2014. – 28.03).***

***

Twitter – это одна из немногих соцсетей, отношение к которой у людей полярное: кто-то его обожает, твитит по сто раз на дню и собирает в списки политиков, музыкантов, ученых и друзей, чтобы почитать, а кто-то просто не переваривает весь этот микроблоггинг. Есть и такие, кто когда-то начинал пользоваться сервисом, но со временем его покинул. Мы нашли любопытную аналитику на тему того, почему люди уходят из Twitter.

Если вкратце, людям трудно разобраться, кого бы почитать. Кроме того, их не устраивает, что никто не подписывается на них самих (наверняка в основном виновен второй пункт).

На Уолл Стрит или в Кремниевой Долине люди все больше переживают насчет медленного роста пользовательской базы Twitter, и есть признаки того, что те, кто им пользовался, все меньше это делают. На днях Deutsche Bank выпустил исследование, в ходе которого было опрошено 1100 человек – текущие пользователи Twitter, бывшие пользователи и те, кто не написал ни одного твита в жизни. В результате выяснилось, что среди причин, почему люди начинают использовать сервис микроблогов и бросают это дело, лидируют три причины. Все они сводятся к тому, что пользователи не справляются с задачей поиска и фильтрации интересного им контента.

В Twitter нет недостатка информации, так что аналитики Deutsche Bank называют это проблемой «курирования», а не контентной проблемой.

Но парням из Twitter не стоит отчаиваться – почти 60 % бывших пользователей сказали, что вполне могли бы дать сервису второй шанс, если будут реализованы следующие улучшения:

И снова главная «хотелка» пользователей связана с возможностью отсеивания лишнего контента и вычленения того, что интересно. Решить это проблему вполне во власти команды Twitter. Что делать со вторым главным желанием – чтобы было больше фолловеров, – понятно в меньшей степени.

Один из способов решения проблемы курирования контента – помочь новым пользователям понять, на кого лучше всего подписаться. В настоящее время сервис предлагает функцию Discover, но, как показал опрос, почти никто из пользователей о ней не подозревает. У тех, кто разочаровывается в

Twitter, чаще всего крайне мало подписчиков, так что, если компания сможет как-то решить эту проблему, то люди могут начать твитить снова.

Twitter находится в состоянии депрессии после IPO – цена на акции в этом году упала на 24 % и вполне может еще снизиться в мае, когда истечет срок запрета на продажу акций сотрудниками компании (а таких акций 475 млн).

С другой стороны, Facebook переживал после IPO времена и похуже – особенно все сомневались в том, что М. Цукербергу удастся заставить пользователей полюбить мобильное приложение соцсети. Прошло два года, и мы все видим, что Facebook чувствует себя лучше, чем когда-либо. После выхода на биржу стагнация настигла и LinkedIn, но компании также удалось справиться с проблемами.

Так что хоронить Twitter явно рано, почему бы ему не повторить путь других социальных сетей? ***(Почему пользователи бегут из Twitter // InternetUA (http://internetua.com/pocsemu-polzovateli-begut-iz-Twitter). – 2014. – 30.03).***

***

В Долине все чаще можно услышать разговоры о том, что Facebook повторяет путь Yahoo. Зимой соцсеть отказалась от внедрения нового красивого дизайна. Официальная причина: он круто смотрелся на больших новых экранах, но не очень на старых маленьких. К сожалению, основная масса пользователей Facebook еще не разорилась на большой модный монитор, так что от нововведений пришлось отказаться.

В результате был внедрен дизайн, который работает для большинства людей нормально, хоть и выглядит пришельцем из 2009 г.

Получается, инновациям в Facebook препятствует огромное число пользователей. Если это действительно так, то соцсеть и вправду повторяет путь Yahoo, которая почти с момента своего основания сталкивалась с «дилеммой инноватора».

Компания не могла устроить на Yahoo.com что-нибудь эдакое, потому что сайт стал огромным бизнесом с сотнями миллионов пользователей.

Это, в свою очередь, ослабило позиции Yahoo в борьбе с маленькими компаниями, которые могли спокойно заниматься инновациям и внедрять какие-то радикальные вещи, поскольку еще до конца не стали действующим бизнесом. В итоге эти маленькие компании, в числе которых были стартапы Google и Facebook, превзошли Yahoo и по размерам, и по доходам.

А теперь у Facebook примерно те же проблемы. Соцсеть не может позволить себе редизайн по всем современным канонам, который бы смотрелся «как в 2017 г.», поскольку миллионам пользователей, которые пришли туда в 2004 г., такие новинки вряд ли понравятся.

При этом новым стартапам никто не мешает создавать проекты, оптимизированные под самые современные технологии. Этим стартапам не нужен миллиард пользователей, чтобы стать конкурентом Facebook.

К счастью акционеров социальной сети, CEO компании М. Цукерберг, похоже, прекрасно видит текущую ситуацию и знает, что надо делать.

Он использует ресурсы Facebook для покупки прорывных стартапов, делающих те вещи, которые в рамках Facebook.com реализовать уже не получится. За последние 16 месяцев М. Цукерберг потратил 22 млрд дол.: на покупку Instagram (1 млрд дол. – как оказалось, дешево), WhatsApp (16 млрд дол.+ еще три акциями RSU для сотрудников) и Oculus (2,2 млрд дол.).

Напрашивается вопрос – а почему же боссы Yahoo 10 лет назад не сделали то же самое? Дело в том, что на самом деле они пытались. Но совершили ошибку, которую не делает М. Цукерберг. Они слишком зацикливались на том, чтобы заплатить правильную и точную цену конкретного проекта.

Вот вам иллюстрирующий пример. В 2006 г. Yahoo вполне могла купить небольшой быстрорастущий проект, который впоследствии сильно возрос. Начальство Yahoo и боссы этого стартапа сошлись на 1 млрд дол. Но затем, едва ли не в самый последний момент, CEO Yahoo Т. Семел вдруг решил, что миллиард – это многовато. Поэтому он сказал CEO того стартапа, что за его компанию заплатят лишь 850 млн дол. – эта цена больше нравилась CFO Yahoo С. Декер, она считала, что именно такие цифры ближе к реальности.

Единственное, чего боссы Yahoo не учли, так это то, что CEO стартапа не хотел его продавать. Просто однажды он сказал совету директоров, что если кто-то предложит миллиард, то почему бы и нет. Так что когда стартап оценили именно в эту сумму, у его CEO уже не было варианта отыграть назад. Но этот ход с понижением цены до 850 млн дол. стал отличным шансом отменить сделку.

Вот так, сэкономив 150 млн, компания потеряла 150 млрд. Что это была за компания?

Facebook.

Кто был тот парень, которого не устроили 850 млн, но устроил бы 1 млрд?

М. Цукерберг.

Урок здесь не в том, что Facebook избежит участи Yahoo, потому что не боится потратить лишние деньги на приобретение перспективных проектов. В конце концов, Yahoo тоже купила немало компаний, включая Geocities и Broadcast.com.

М. Цукерберг, похоже, научился на ошибке Т. Семела тому, что если уж ты решился на сделку, надо идти до конца и осуществить ее, не потеряв все из-за пары лишних чемоданов с долларами. То, что можно таким образом сэкономить, в будущем может составить лишь пару процентов стоимости возросшей из стартапа компании.

М. Цукерберг знает, что в технологическом бизнесе у всех поглощений есть два возможных результата: они либо спасут от дилеммы инноватора,

либо нет. И действует соответственно ***(Станет ли Facebook новым Yahoo // Marketing Media Review (http://mmr.ua/news/id/stanet-li-facebook-novym-yahoo-39054/). – 2014. – 31.03).***

***

Facebook обновила свой мессенджер для операционной системы iOS, сделав его несколько более полезным для тех пользователей, кто любит общаться друг с другом посредством социальной сети. В выпущенной 28 марта версии Facebook Messenger присутствует возможность группировать собеседников по различным признакам, например «коллеги», «друзья», «родственники» и т. д.

Кроме того, у пользователя появилась возможность рассылки сообщений или фото всем или избранным участникам группы в приложении. Также в приложении есть возможность включения новых участников в многостороннюю беседу с автоматической отправкой им всей ранее созданной ветви беседы.

Новый функционал – это часть масштабных обновлений, которые Facebook реализует в четвертой версии своего мессенджера.

Новая версия также обзавелась возможностью общения между собеседниками без непосредственного запуска платформы Facebook в браузере, что дает мессенджеру большую степень автономности.

Впрочем, стоит заметить, что судьба Facebook Messenger остается несколько неясной в свете недавнего поглощения WhatsApp со стороны Facebook. Вполне вероятно, что в перспективе WhatsApp полностью заменит Facebook Messenger ***(Facebook обновляет Messenger для Apple iOS // InternetUA (http://internetua.com/Facebook-obnovlyaet-Messenger-dlya-Apple-iOS). – 2014. – 31.03).***

***

Mail.Ru Group на основе данных TNS Web-Index за январь 2014 г. провела анализ пяти крупнейших социальных сетей в России. Самая большая месячная аудитория у «ВКонтакте». На втором месте – «Одноклассники», а на третьем – «Мой мир», который опережает Facebook и Twitter.

Половозрастная структура пользователей социальных сетей распределилась примерно одинаково. Наиболее активными являются люди в возрасте от 25 до 34 лет. Facebook отличается от остальных социальных сетей более возрастной аудиторией, в то время как у Twitter и «ВКонтакте» много молодёжи до 24 лет.

В исследовании отмечается, что «поведение участников разных социальных сетей существенно отличается: если пользователи “Одноклассников” заходят реже, но проводят на страницах соцсети достаточно долгое время, то для пользователей “ВКонтакте”, наоборот, характерны более частые, но краткие визиты».

Среднее посещение «Одноклассников» вдвое дольше, чем «ВКонтакте», но в течение месяца во «ВКонтакте» заходят в 1,3 раза чаще, чем в «Одноклассники». При этом по количеству просмотров страниц за месяц «Одноклассники» являются безоговорочным лидером, более чем в 1,7 раз обгоняя число просмотров в сети «ВКонтакте».

Пресс-секретарь «Одноклассников» И. Грабовский прокомментировал ЦП результаты исследования: «С “Одноклассниками”, к сожалению, связано много мифов. К счастью, ничего общего с действительностью они не имеют, достаточно взглянуть на цифры. Наша месячная аудитория – свыше 42,6 млн человек, ядро которой составляют молодые люди в возрасте 25–34 лет.

Помимо всего прочего, наши пользователи еще и одна из самых активных и лояльных аудиторий. В среднем, они проводят на сайте немногим более 20 мин., что вдвое больше, чем у ближайшего конкурента. Да и по количеству просмотренных страниц за месяц мы тоже обгоняем преследователей как минимум в два раза.

Думаю, что большой показатель времени связан, в первую очередь, с популярностью видео (ежедневно около 70 млн просмотров), музыки и игр у наших пользователей, не говоря уже о других не менее важных сервисах».

Пресс-секретарь «ВКонтакте» Г. Лобушкин касательно сравнения времени, проведённого пользователями на сайте, отметил: «Независимые счетчики, такие как, например, liveinternet.ru или наши собственные наблюдения, не подтверждают данные в исследовании Mail.ru» ***(Отчёт Mail.Ru: «Одноклассники» опережают «ВКонтакте» по количеству просмотров страниц // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/otchyot_mail_ru_odnoklassniki_operezhayut_vkontakte_po_kolichestvu_prosmotrov_stranits). – 2014. – 31.03).***

***

Основатель «ВКонтакте» П. Дуров отозвал заявление об уходе из компании, которое он сделал 1 апреля, сообщает Обозреватель со ссылкой на Forbes (http://tech.obozrevatel.com/news/53794-durov-ne-pokidaet-post-gendirektora-vkontakte-smi.htm).

Напомним, что П. Дуров сложил с себя обязанности генерального директора социальной сети «ВКонтакте», сообщив об этом на своей странице в «ВКонтакте».

Но уже в ночь на четверг, 3 апреля, прислал членам совета директоров письмо, отзывающее его заявление об уходе. Текст письма, написанного на английском языке, имеется в распоряжении Forbes.

«Since it came to my knowledge that my resignation at this moment can create unnecessary risks for our company, I intend to remain and serve as the CEO» («Поскольку до моего сведения дошло, что моя отставка сейчас может создать ненужные риски для нашей компании, я намерен остаться и работать в качестве генерального директора»), – сказано в документе.

Два источника, близких к совету директоров «ВКонтакте», сообщили Forbes, что 2 апреля П. Дуров встречался с И. Щербовичем, президентом фонда United Capital Partners (UCP), владеющем 48 % «ВКонтакте».

В фонде UCP 3 апреля подтвердили получение письма П. Дурова, пообещав прокомментировать ситуацию после выяснения всех деталей. Связаться с главой USM Advisors И. Стрешинским не удалось. В USM Advisors отказались от комментариев. USM Advisors управляет активами холдинга USM Holdings Ltd., объединяющего активы А. Усманова, А. Скоча и Ф. Моширi. А. Усманов через Mail.ru Group владеет 51,99 % «ВКонтакте». PR-директор Mail.Ru Group К. Чабаненко сказала, что не знает об отзыве заявления П. Дурова. Исполнительный директор «ВКонтакте» Д. Сергеев затруднился прокомментировать информацию о письме ***(Дуров не покидает пост гендиректора «ВКонтакте» – СМИ // Обозреватель (http://tech.obozrevatel.com/news/53794-durov-ne-pokidaet-post-gendirektora-vkontakte-smi.htm). – 2014. – 3.04).***

***

64 % всех американских пользователей предпочитают Facebook другим социальным платформам. 30 % аудитории Facebook просматривают на сайте новости.

Facebook популярен среди людей старше 30 лет. Хотя молодежь моложе 30 лет предпочитает Twitter и YouTube.

Из тех, кто читает новости, 22 % действительно считают Facebook полезным информационным источником, треть отмечают понравившиеся им сообщения.

Больше всего люди читают о развлечениях, хотя 49 % интересующихся новостной информацией просматривают хотя бы 6 различных тематик ***(Исследование: 30 % пользователей Facebook в США смотрят в нем новости // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/issledovanie_30_polzovateley_facebook_v_ssha_smotryat_v_nem_novosti). – 2014. – 2.04).***

***

Ряд крупнейших компаний мира представляют WebScaleSQL, спецпроект, расширяющий возможности MySQL. В список вошли Facebook, Twitter, LinkedIn и Google.

«Новая разработка будет ориентирована на работу с крупными клиентами, с массивами данных, – утверждает представитель Facebook. – Совместные усилия принесут значительно больший результат, я уверен в этом».

Суть проекта очень простая. За основу взят MySQL пятой версии. Разработчики, программисты из всех вышеназванных компаний создали единый программный код. Каждый ресурс может совершенствовать этот код,

изменять его, повышать производительность всей системы в рамках проекта WebScaleSQL и предлагать новинки остальным членам «союза». Если хотя бы один участник поддержит возникшее предложение – оно внедряется в работу всех четырех гигантов. «Каждый из нас привнесет что-то свое, приложит максимум ресурсов, – не сомневается в успехе проекта представитель Google. – Тем самым мы все будем экономить время, деньги, и при этом будем получать в 4 раза больше результата – или еще больше».

WebScaleSQL – проект, который будет существовать параллельно MySQL, а не как-то замещать его. В настоящее время Facebook представил партнерам для одобрения свою последнюю разработку – код асинхронного клиента, который убирает время ожидания после запроса. Следующий проект – разработка нового языка программирования ***(Facebook, Google, Twitter и LinkedIn запустили совместный проект // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_google_tvitter_i_linkedin_zapustili_sovmestnyy_proekt). – 2014. – 2.04).***

***

Появилась первая в мире католическая социальная сеть

М. Капелло, президент Католического института евангелизации, при поддержке Совета Кардиналов, призывает всех католиков объединиться. Теперь – в режиме онлайн.

Речь идет о новой католической социальной сети – DeoSpace, расположенной по адресу: www.deospace.com. Но, несмотря на католическую позицию, на ресурсе могут регистрироваться все желающие без исключения. Пользователям достаточно предоставить свои личные данные.

«Двери Deospace, как и двери церкви, открыты для всех, – утверждает кардинал, О. А. Родригес, один из кураторов социального проекта. – Наша сеть будет интересна не только католикам, но и всем остальным людям». Много интересного можно будет найти в архивах и на официальных страницах ресурса тем, кто изучает католицизм – или хочет с ним ознакомиться.

Структура сети очень похожа на многие другие социальные сети. Есть только несколько специфических отличий. Во-первых, в Deospace будет создан несколько более строгий свод правил, чем на остальных подобных ресурсах – все-таки речь идет о вере. Во-вторых – пользователи не вступают в сообщества, а присоединяются к тому или иному приходу, апостольской группе или диоцезу. «Deospace адаптирована под католиков, – говорит М. Капелло. – И мы сделаем все возможное, чтобы еще больше усилить эту адаптацию. Сеть уже запущена и функционирует, но в тоже самое время ведутся активные работы по ее развитию и дополнению» ***(Появилась первая в мире католическая социальная сеть // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/poyavilas_pervaya_v_mire_katolicheskaya_sotsialnaya_set). – 2014. – 2.04).***

***

Недавно правила социальной сети «ВКонтакте» были дополнены пунктом 5.3.16. Если пересказать его, окажется, что «накрутки» отметок «Мне нравится» и «Рассказать друзьям» теперь караются баном, пишет AIN.UA (http://ain.ua/2014/04/04/518702).

Полностью подпункт правил теперь звучит так: «пользователю при использовании сайта запрещается …осуществлять самостоятельно либо от имени других пользователей с использованием функционала их аккаунта, в т. ч. путем введения в заблуждение или с обещанием поощрения, в т. ч. с использованием любых программ, автоматизированных скриптов, массовые однотипные действия, направленные на искусственное повышение показателей счетчиков сайта (числа друзей, отметок “Мне нравится”, событий “Рассказать друзьям” и т. д.)».

В пресс-службе сети AIN.UA рассказали, что администрация обычно не ограничивает пользователей в выражении одобрения авторам – понравившиеся материалы можно добавлять в закладки с помощью кнопки «Мне нравится». Однако «ВКонтакте» не одобряет ситуации, когда подобные действия превращаются в чей-то некрасивый бизнес – пользователей сайта поощряют ставить отметки данной кнопкой или, к примеру, используя возможность «Рассказать друзьям». К нарушителям будут применяться санкции, в частности – блокировать ***(Во «ВКонтакте» будут банить за накрутки «лайков» // AIN.UA (http://ain.ua/2014/04/04/518702). – 2014. – 4.04).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Сообщество Евромайдана в Facebook, на которое в настоящее время подписано более 280 тыс. пользователей, вышло в финал конкурса The Bobs, который ежегодно проводит немецкая медиакомпания Deutsche Welle. Всего в финал было отобрали 154 интернет-проекта из более чем 3 тыс. заявленных блогов на 14 языках из Европы, Азии и Америки, пишет AIN.UA (http://ain.ua/2014/04/02/518380).

Пользовательское голосование стартовало 2 апреля, и пока что украинский «Евромайдан» лидирует по числу голосов в номинации «Лучший блог», обгоняя такие проекты, как блог фотографа И. Варламова или The Intercept – блог о системе слежения, которую используют в Агентстве нацбезопасности США (NSA).

Евромайдан – самое крупное некоммерческое Facebook-сообщество в украинском сегменте. Эта страница была одной из центральных точек в сети, где публиковались новости о протестах, координировались действия

протестующих, собиралась помощь для них. За последние полгода, по данным SocialBakers, страница набрала значительную аудиторию и продолжает рост.

Среди других финалистов из Украины в конкурсе:

– в номинации «Лучшая инновация» – сайт «Хроніки революції»;

– в номинации «Лучшая общественная кампания в социальных сетях» – проект «Є люди»;

– в номинации «Приз организации “Репортеры без границ”» – проект YanukovychLeaks;

– в номинации «Приз GlobalMediaForum» – Facebook-сообщество «Євромайдан SOS»

– в номинации «Самый креативный и оригинальный» – творческое объединение «Вавилон’13»;

– в номинации «Выбор пользователей: лучшая страница на украинском» – «Евромайдан», «Крим SOS», «Є люди», «Але є одне але» (Телебачення Торонто) и блог С. Лещенко.

Напомним, в конкурсе The Bobs проекты на украинском языке могут принимать участие с начала 2013 г. Украину в жюри представляет О. Романюк – исполнительный директор Института массовой информации и представитель «Репортеров без границ» в Украине.

В этом году с 5 марта по 2 апреля жюри определило финалистов в каждой из номинаций. Пользователи могут голосовать за блоги со 2 апреля по 7 мая. Жюри проголосует за проекты 4 и 5 мая (победители по версии пользователей и по версии жюри определяются отдельно). Все победители будут названы 7 мая этого года ***(Facebook-сообщество «Евромайдан» лидирует в международном конкурсе блогов // AIN.UA (http://ain.ua/2014/04/02/518380). – 2014. – 2.04).***

***

В последнее время украинские СМИ пестрели сообщениями о том, что страны «большой семерки» осуждают действия России и поддерживают Украину. Но таким ли важным иностранные политики считают «украинский вопрос» для своих избирателей на самом деле? Чтобы понять это, Marketing Media Review заглянул в их Facebook-аккаунты (http://mmr.ua/specarticles/id/chto-v-facebook-u-politikov-g7-38912/).

Заметим, что мы анализировали только те аккаунты, которые социальная сеть верифицировала как подлинные.

Б. Обама, президент США (39 млн фолловеров). Страница полностью отведена под кампанию о медицинском страховании. За последнюю неделю – ни одного упоминания об Украине.

Д. Кэмерон, премьер-министр Великобритании (150 тыс. фолловеров). Пишет о госбюджете, налогах и британских паралимпийцах. За последнюю неделю – ни одного упоминания об Украине.

С. Харпер, премьер-министр Канады (106 тыс. фолловеров). Прибыл с визитом в Киев. Кроме сообщений об официальных встречах, есть фото с прогулок по местам недавних трагических событий. Страница ведется на двух языках – английском и французском.

А. Меркель, канцлер ФРГ (516 тыс. фолловеров). Есть официальный комментарий от 20 марта, в котором осуждается аннексия Крыма.

Ф. Олланд, президент Франции (448 тыс. фолловеров). Последняя запись датирована 8 марта и посвящена Международному женскому дню. Об Украине – ни слова.

М. Ренци, премьер-министр Италии (628 тыс. фолловеров). Обсуждает поддержку людей с синдромом Дауна и гендерное равенство. Об Украине – ни слова ***(Что в Facebook у политиков G7? // Marketing Media Review (http://mmr.ua/specarticles/id/chto-v-facebook-u-politikov-g7-38912/). – 2014. – 24.03).***

***

Користувачів соцмереж закликають поширювати перевернуте фото президента Росії В. Путіна на знак протесту проти його політики

Таку пропозицію у Facebook поширив користувач Ю. Крикунов, передає Еспресо.TV.

Нагадаємо, 2 грудня 2013 р. луцькі активісти провели пікет біля Волинської обласної ради, тримаючи перевернуті портрети тодішнього президента України В. Януковича. За це проти них були порушені кримінальні справи ***(У соцмережах вслід за Януковичем перевернули догори дригом портрет Путіна // Espreso.tv (http://espreso.tv/new/2014/03/24/u_socmerezhakh_vslid_za_yanukovychem_perevernuly_dohory_dryhom_portret_putina). – 2014. – 25.03).***

***

У період, коли на столичному майдані масово гинули герої Небесної сотні, українські користувачі соцмереж звели до мінімуму кількість постів про котиків і песиків та «себе любимих». Симпатичні портретні світлини витіснив квадрат Малевича. Коментарі під такими фотографіями були на кшталт: «Почорнів від горя український Фейсбук».

Та віднедавна ситуація змінилася. З появою «Сервісу патріотичних аватарок» люди для своїх сторінок створюють яскраві образи на тлі жовто-блакитного прапора ***(Українці у соцмережах розміщують патріотичні аватарки // Від і До (http://vidido.ua/index.php/pogliad/article/ukrainci_u_socmerezhah_rozmiujut_patriotichni_avatarki/). – 2014. – 27.03).***

***

24 марта в Facebook создали специальную группу под названием Krym_Rabota_SOS с целью помощи в поисках работы беженцам из Крыма. В настоящее время она уже объединяет более 270 пользователей соцсети.

На странице информируют по поводу имеющихся вакансий, а также предлагают присылать резюме на специальный электронный адрес.

Кроме того, группа намерена информировать пользователей об особенностях и тонкостях поиска работы в Украине ***(Facebook-группа «Krym_Rabota_SOS» поможет найти работу крымским беженцам // IT Expert (http://itexpert.org.ua/rubrikator/item/34788-facebook-gruppa-krymrabotasos-pomozhet-najti-rabotu-krymskim-bezhentsam.html). – 2014. – 29.03).***

***

Черкащан закликають блокувати і скаржитися на пабліки та сторінки відверто екстремістського спрямування, що поширюються в соціальній мережі «ВКонтакте».

Про це йдеться в дописі пабліку Черкащани [LIVE], інформує сайт «Про все».

«Доки колишні опозиціонери самозахоплено ділять посади, у країні вже іде війна. Справжня. Її поле битви – інформаційне. Наразі у соціальних мережах набирають обертів пабліки відверто екстремістського спрямування. Зокрема, інформаційна війна добралась і до тихих Черкас. Нехай вас не вводять у оману мала кількість підписників пабліку. Найкраща війна – зруйнувати замисли противника», – ідеться в дописі.

Групи:

1. «Антимайдан. Славянский треугольник. Черкассы» http://www.vk.com/club65186401
2. Антимайдан Черкассы http://www.vk.com/club67395565
3. http://vk.com/id245302012
4. http://vk.com/antimaydan
5. http://vk.com/club66581631
6. http://vk.com/k_shtab
7. http://vk.com/antimaydanukraineourhome
8. http://vk.com/maidan_bez_grima
9. http://vk.com/mirperedel
10. http://vk.com/pomogi_bratiyam

Список буде поповнюватися.

Заблокувати окупантську групу дуже просто.

1. Виберіть допис і натисніть «хрестик».
2. Оберіть причину «насильство/екстремізм».
3. Насолоджуйтесь почуттям виконаного обов’язку.

Максимально застосуйте цю нескладну комбінацію до дописів групи та дописів її активних учасників, які пропагують окупантську ідеологію і закликають когось «по-братськи рятувати».

Чим більше людей це зробить, тим швидше групу буде заблоковано.

Також можна поскаржитись адміністрації «ВКонтакте» за посиланням: http://vk.com/support?act=new ***(Черкащан закликають блокувати окупантів у соцмережах // ПРОЧЕРК (http://procherk.info/news/7-cherkassy/22381-cherkaschan-zaklikajut-blokuvati-okupantiv-u-sotsmerezhah). – 2014. – 29.03).***

***

У мережі Facebook зародився рух за підвищення патріотизму в місті Чернігів. Активісти пропонують усім підприємствам міста та його мешканцям прикрашати жовто-блакитними стягами фасади будівель, вікна, автомобілі. У першу чергу заради протистояння російським ЗМІ, які намагаються показати, що Чернігів – проросійське місто.

«Український прапор, насправді, не панацея. Він не вирішить глобальні проблеми нашого часу. – вважають автори ідеї. – Але він здатен нагадати, що в кожному з нас присутній мініатюрний портрет нашого народу. Що ми, українці, одне ціле. І що у нас усіх – єдина мета: жити та творити на цій землі. Під цим прапором!» ***(Акція «Жовто-блакитний Чернігів» // Чернігівщина: події і коментарі (http://pik.cn.ua/print/8806/). – 2014. – 1.04).***

***

Заместитель Луганского городского головы А. Ткаченко предложил организовать традиционную акцию «Лента Памяти – символ Победы, связавший поколения» путем самоорганизации людей с помощью социальных сетей. Об этом он написал на своей странице в Facebook.

«Предлагаю провести своеобразный эксперимент. В прошлом году организация “Ленты Памяти” при проведении комплекса мероприятий ко Дню Победы легла, в основном, на административный ресурс. Сейчас ситуация изменилась, и я уверен, что мы сможем сделать это все вместе, просто самоорганизовавшись. Революции собирают при помощи социальных сетей – давайте покажем, что и почтить память воинов Великой Отечественной нам по силам», – написал А. Ткаченко.

Мероприятие, по словам чиновника, начнется 8 мая в 14:00. Традиционно акция начнется в сквере имени 9-го Мая, после чего пройдет по улице Советская через площадь Героев ВОВ возле Пилона Славы и могилы Неизвестного солдата, после до сквера Освободителей по улице Оборонная к памятнику советским воинам-танкистам. Завершит свой путь лента на Мемориальном комплексе Острая Могила возле братской могилы советских воинов.

А. Ткаченко призвал всех сделать репост данного заявления и откликнуться на эту инициативу ***(Заместитель мэра Луганска ко Дню***

Победы предлагает провести эксперимент // CXID-INFO (http://cxid.info/zamestitel-mera-luganska-ko-dnu-pobedy-predlagaet-provesti-eksperiment-n113409). – 2014. – 4.04).

***

Івано-франківських студентів навчають, як боротися з інтернет-тролями

У рамках «Волонтерського руху Прикарпаття» на базі Прикарпатського національного університету ім. В. Стефаника організовані різні цікаві для студентів навчання, з-поміж яких медична підготовка, допризовна підготовка, заняття із самооборони, з журналістики, лекції юридичної тематики.

Одним з видів занять є інтернет-журналістика та робота в соцмережах. Зокрема, тролінг як засіб маніпуляції.

Цей курс читає студент-активіст І. Харків. Слухачі мають можливість прослухати лекцію, задати лектору запитання, які їх цікавлять, і отримати домашнє завдання. Одним з таких домашніх завдань було долучити у друзі в соцмережах студента зі сходу України і поспілкуватись із ним. Надалі планується знайомство зі студентами з Росії. Також слухачів навчили, як поводитись із тролями і не вестися на їх провокації та як грамотно нейтралізувати троля влучним коментарем ***(Івано-франківських студентів навчають, як боротися з інтернет-тролями // NEWS.IF.UA (http://news.if.ua/news/34233.html). – 2014. – 4.04).***

***

Пропонуємо вам рейтинг українських сторінок у соціальній мережі Facebook за показником talking about this (ТАТ), який демонструє кількість унікальних користувачів, які протягом тижня активно взаємодіяли зі сторінкою – коментували, лайкали, ділились контентом сторінки.

ТАТ, на відміну від кількості лайків, є хорошим показником цікавості сторінки для її читачів. Чим він вищий – тим більше людей взаємодіють з контентом сторінки.

Цікаво, що в ТОП-3 одразу дві гумористичні спільноти. На першому міст – Баба і Кіт зі 101 тис. ТАТ, на третьому – Церковь Свидетелей Покращення – 89 тис. Баба і кіт також є лідером за співвідношенням ТАТ до кількості прихильників сторінки – більше ніж 2:1.

На другому місці на сьогодні перебуває сторінка Євромайдану, яка була створена всього 4,5 місяців тому і весь цей час мала високі показники по ТАТ. А в пікові моменти – у другій половині лютого – цей показник перевищив 300 тис.

У рейтинг потрапили одразу чотири медійні сторінки (УП, 5 канал, TVi та ТСН), що демонструє високий рівень зацікавленості аудиторії новинами ***(ТОП-10 українських сторінок у Facebook за рівнем взаємодії з аудиторією***

// UkrainianWatcher (http://watcher.com.ua/2014/04/04/top-10-ukrayinskyh-storinok-u-facebook-za-rivnem-vzayemodiyi-z-audytoriyeyu/). – 2014. – 4.04).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Брендам стоит прекратить использовать огромное количество хэштегов в своих официальных группах в Facebook, пишет adindex.ru. Согласно докладу Socialbakers, это ведет к сокращению численности их целевой аудитории.

Как пишет Mashable, чем больше хэштегов используется в сообщении бренда в Facebook, тем меньше откликов получает данное сообщение. И это несмотря на то, что хэштеги помогают людям находить публикации на темы, которые их интересуют.

Исследование Socialbakers базировалось на анализе 200 тыс. официальных сообщений брендов в Facebook в феврале 2014 г. В результате выяснилось, что посты с одним-двумя хэштегами получали в среднем 593 отклика. Показатель взаимодействия с аудиторией сообщений брендов, в которых стояло от трех до пяти хэштегов, сократился до 416 откликов. В постах, в которых использовалось до 10 хэштегов, пользователи были заинтересованы еще меньше (307 откликов). Сообщения брендов с использованием больше 10 хэштегов оказались наименее популярны среди аудитории (188 откликов).

Любопытно, что в исследовании Socialbakers, посвященном Instagram, уже говорилось о том, что злоупотребление хэштегами – плохая практика как для брендов, так и для обычных юзеров. Twitter, кстати, в ближайшем будущем собирается и вовсе отменить функцию хэштегов.

Кроме того, напомним, что недавно чешская фирма Kentico Software выяснила, что 68 % подписчиков вне зависимости от использования хэштегов вообще никак не реагируют на посты, которые появляются на официальных страницах брендов в Facebook, Twitter и Instagram ***(Хэштеги в Facebook отнимают у брендов аудиторию // Media бізнес (http://www.mediabusiness.com.ua/content/view/38771/126/lang,ru/). – 2014. – 24.03).***

***

Реклама в мобильной версии социальной сети «ВКонтакте» появится летом 2014 г. Об этом заявил исполнительный директор компании Д. Сергеев. «Ориентируемся на лето этого года», – заявил он.

Д. Сергеев рассказал, что продажей рекламных возможностей мобильного приложения будет собственный департамент «ВКонтакте» по рекламе. «Мы не будем рекламировать сторонние сайты – акцент будет

сделан на группы и сообщества “ВКонтакте”», – подчеркнул исполнительный директор компании.

Ранее «ВКонтакте» объявила о запуске платных и бесплатных стикеров – картинок, изображающих различные эмоции и использующихся при обмене личными сообщениями ***(Реклама в мобильной версии «ВКонтакте» появится летом 2014 года // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/reklama_v_mobilnoy_versii_vkontakte_poyavitsya_letom_2014_goda). – 2014. – 25.03).***

***

На время праздничных пиков продаж (новый год, рождество, «черная пятница») Facebook предлагает использовать свои рекламные инструменты ритейлерам.

Крупнейшая социальная сеть в мире Facebook inc предлагает ритейлерам увеличенный объем рекламных инструментов своей соцсети, которые позволят им делать актуальные предложения своим покупателям. Инструмент Custom Audiences от Facebook широко используется маркетологами, а в III квартале его использование возросло на 75 % по сравнению с предыдущими периодами, сообщает компания в своем блоге.

Custom Audiences – это механизм, позволяющий рекламодателям находить в автономном режиме потребителей/аудиторию, используя личные данные и контакты клиентов, https://www.facebook.com/help/459892990722543/.

Для использования механизма необходимо лишь ввести лист MailChimp или список адресов электронной почты.

Благодаря Custom Audiences маркетологи могут превратить покупателей, однажды совершивших покупку, в постоянных клиентов, пользуясь индивидуальным таргетингом рекламы. Так же программа позволяет макретологам осуществлять выборку на основе исключений.

По причине наступающего сезона праздничного шоппинга, Facebook делает новые предложения для ритейлеров. Руководство соцсети преследует цель привлечь большие рекламные бюджеты своих пользователей, число которые давно превышает 1 млрд человек.

Для продвижения предпраздничных акций и предложений калифорнийская кампания настоятельно рекомендует маркетологам использовать Custom Audiences.

По оценке специалистов, он-лайн-продажи в США на период праздников этого года возрастут не менее чем на 15 % ***(Facebook увеличивает праздничные продажи // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_uvelichivaet_prazdnichnye_prodazhi). – 2014. – 26.03).***

***

Крупнейшая социальная сеть мира Facebook вышла на второе место на рынке мобильной рекламы, уступая только поисковому гиганту Google. За 2013 г. объем рынка возрос на 105 %, достигнув отметки 17,96 млрд дол.

За 2013 г. объем рынка мобильной рекламы возрос на 105 %, достигнув отметки 17,96 млрд дол.

Несмотря на рост рынка, его темпы всё же начинают падать, по итогам 2014 г. этот показатель может составить 75,1 % (105 % в 2013 г.). По прогнозам, к 2018 г. темпы роста рынка сократятся до 22,2 % в год, тогда как объем достигнет 95 млрд дол.

Основными драйверами роста являются всего две компании – Google и Facebook. При этом неоспоримым лидером на рынке остается Google, который по итогам текущего года займет долю в 46,8 %, хотя ещё в 2012 г. этот показатель составлял 52,6 %.

Инициативу потихоньку начинает перехватывать Facebook, который за год увеличил свою долю в три раза (5,4 % в 2012 г. и 17,5 % в 2013 г.) и останавливаться не планирует. Ожидаемый показатель по итогам 2014 г. – 21,7 % рынка всей мобильной рекламы.

Чистая прибыль Facebook от рекламы на мобильных устройствах в 2013 г. составила 45,1 % от всех рекламных доходов, а в 2014 г. этот показатель может достичь отметки в 63,4 %.

В список лидеров по продаже мобильной рекламы также входят сервис микроблогов Twitter с 2,4 % рынка, мобильное приложение Yellow Pages и сервис Pandora – по 2,1 %. Ещё 25,6 % рынка взяли компании, занимающие на нем менее 1 % каждая ***(Facebook начинает сокращать отставание от Google на рынке мобильной рекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_nachinaet_sokraschat_otstavanie_ot_google_na_rynke_mobilnoy_reklamy). – 2014. – 26.03).***

***

26 марта Facebook объявил о том, что добавляет новые таргетинговые возможности в Lookalike audiences. Теперь у рекламодателей есть возможность создавать аудитории, основываясь на пользователях, которые заходили на их сайт, используют мобильное приложение или связаны с Facebook-страницей.

На этапе бета-тестирования новый функционал был опробован компанией Spotify, результат – уменьшение стоимости лида в два раза.

Нововведение появится в ближайшее время у всех рекламодателей в Power Editor ***(Facebook расширяет таргетинг для Lookalike Audiences // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_rasshiryaet_targeting_dlya_lookalike_audiences). – 2014. – 27.03).***

***

Как работодатели следят за страницами сотрудников и соискателей в социальных сетях

Страничка в Facebook или «ВКонтакте» давно уже перестала быть просто «личным пространством». Ведь фото с алкогольной вечеринки или стрип-клуба смогут оценить не только друзья, но и потенциальные работодатели, которые уже привыкли «пробивать» данные о будущем работнике в социальных медиа. По данным исследования портала rabota.ua, около 22 % украинских работодателей регулярно проверяют страницы соискателей. В то же время еще 28 % никогда таким не занимаются, а 50 % – делают это иногда, пишет AIN.UA (http://ain.ua/2014/03/27/517637).

В 40 % случаев страницы соискателя просматриваются еще перед тем, как позвать его на собеседование. Чуть меньше работодателей (37 %) изучают информацию из социальных сетей перед повторным интервью, а 18 % – перед самим приемом на работу. Некоторые участники опроса упоминали, что просматривают страницы уже оформленных на работу сотрудников.

49 % опрошенных работодателей заявили, что данные из социальных сетей могут быть поводом для отказа в месте, а 51 % с этим мнением не согласились.

Тех, кто в настоящее время ищет работу, может заинтересовать информация о том, что именно настораживает потенциального работодателя, когда он заходит на страницу будущего сотрудника. В первую очередь, это может быть провокативная и компрометирующая сотрудника информация (68 %). Также, работодателей может смутить ръяное отстаивание политических и общественных позиций в сети (23 % опрошенных). Правда, здесь нужна ремарка: опрос проводился осенью прошлого года, до начала протестных акций в Украине. А результаты портал опубликовал только сейчас.

Еще 23 % опрошенных считают, что интернет-активность не является отражением профессиональных качеств человека. Также среди негативных факторов упоминался мат и вранье – «несоответствие информации на страничке и изложенной на собеседовании». Отсутствие любой интернет-активности у соискателя натолкнет на негативные размышления 2 % работодателей.

53 % работодателей отслеживают социальную активность своих нынешних сотрудников, а 43 % опрошенных совершенно не тратят на это свое время и внимание.

Также интересными для соискателей могут показаться ответы работодателей на вопрос, с какой целью они следят за страницами сотрудников в социальных медиа:

53 % – чтобы отслеживать аспекты профессионального становления (просмотр публикуемых статей, интересов, заметок);

42 % – чтобы быть в курсе их личной жизни (просмоть фотографий, статусов);

19 % – чтобы отслеживать их гражданскую позицию (посты об экономике, политике и т. д.);

5 % – другое.

Среди прочих вариантов ответа назывался контроль активности сотрудника в рабочее время и контроль его профессиональной деятельности в социальных сетях.

В большинстве случаев работодатели не ограничивают активность своих сотрудников в социальных сетях: работники ведут себя так, как считают допустимым.

В 30 % случаев активность сотрудника в социальных сетях может стать поводом для увольнения или выговора (если таким образом установлена ложь или мошенничество). В 28 % случаев такие последствия могут стать ответом на неадекватное или вредящее имиджу компании поведение сотрудника. В 35 % случаев интернет-активность не может стать поводом для таких последствий.

Исследование проводилось в сентябре 2013 г., среди работодателей-пользователей портала. Выборка – 192 компании со всей Украины ***(Как работодатели следят за страницами сотрудников и соискателей в социальных сетях // AIN.UA (http://ain.ua/2014/03/27/517637). – 2014. – 27.03).***

***

Компания Facebook, которой принадлежит крупнейшая в мире социальная сеть, создает лабораторию Connectivity Lab, где сотрудники будут разрабатывать новые авиационные и коммуникационные технологии для обеспечения доступа в Интернет пока еще не охваченной им части населения Земли. Об этом сообщает IT Expert.

Facebook является лидером проекта Internet.org, цель которого – обеспечить людям по всему миру доступ к базовым интернет-сервисам бесплатно или с небольшими финансовыми затратами. Ранее в этом месяце в СМИ появилась информация, что Facebook ведет переговоры о покупке компании Titan Aerospace, которая производит беспилотные летательные аппараты (БПЛА).

«Facebook Connectivity Lab планирует разрабатывать беспилотники, атмосферные спутники и лазеры, чтобы обеспечить доступ к Интернету всем нуждающимся. В нашу команду входят лучшие эксперты по аэрокосмическим и коммуникационным технологиям, включая специалистов NASA», – написал на своей странице гендиректор Facebook М. Цукерберг.

Также, объявил М. Цукерберг, к Facebook Connectivity Lab присоединяются сотрудники британской компании Ascenta. Ее разработчики занимаются созданием летательных аппаратов с большой продолжительностью полета на больших высотах (HALE), прототип

подобного беспилотника на солнечной энергии носит название Zephyr. Специалисты из Ascenta присоединятся к команде по разработке летательного аппарата, который призван обеспечить связь для выхода в Интернет.

Инициатива Internet.org, которую возглавляет Facebook, составляет своеобразную конкуренцию проекту Project Loon от Google, в рамках которого компания намерена обеспечивать удаленные территории Wi-Fi-подключением с помощью аэростатов. Однако отличие подхода Facebook – в использовании атмосферных оптических линий связи (FSO), обеспечиваемых летательными аппаратами на солнечной энергии, низкоорбитальными и геостационарными спутниками ***(Лаборатория в Facebook создаст беспилотники для «раздачи» интернета // IT Expert (http://itexpert.org.ua/rubrikator/item/34775-laboratoriya-v-facebook-sozdast-bespilotniki-dlya-razdachi-interneta.html). – 2014. – 28.03).***

***

Планы М. Цукерберга неизвестны, но намерения вполне понятны – 2 млрд дол. потрачены на стартап Oculus Rift не ради прихоти, это инвестиции в будущие проекты. Но, как именно социальная сеть может использовать технологии виртуальной реальности? Спору нет, они представляют ценность сами по себе, однако на рынок нужно выходить с конкретным продуктом.

Креативщики из студии Chaotic Moon попробовали смоделировать концепт такой системы, используя всю доступную информацию. Непременная составляющая Facebook – реклама всего и всея, предельно таргетированная, с демонстрацией товара «лицом». В этом и кроется ответ на мучающий многих вопрос о том, ради чего потрачены целых два миллиарда американских денег. Очки и, что более важно, интерфейс виртуальной реальности необходимы для того, чтобы создать самую удобную и практичную версию «магазина на диване». Предполагается, что на страничках с рекламой в Facebook появится еще одна кнопка, активирующая для счастливого обладателя очков Oculus Rift соответствующий сервис.

В нем – трехмерная копия условного торгового центра с тематическими отделами, для создания иллюзии шоппинга вживую. В магазины можно зайти, приглянувшиеся товары – «потрогать», повертеть в руках, примерить на себя, поэкспериментировать с расцветками и фасонами и т. д. Разумеется, не вставая из-за компьютера, причем все понравившееся покупается сразу же, быстро и без лишней суеты – система давно отлажена. Изюминка версии именно для Facebook в том, что виртуальный тур по магазинам может быть совместным. И, прибегнув к помощи зарегистрированных друзей, можно в реальном времени обсудить достоинства товаров – все как в жизни.

Несколько лет назад стало очевидным, что интернет-магазины основательно потеснили реальные заведения, теперь же речь идет о

качественном новом уровне развития виртуальной торговли. И, скорее всего, именно этот революционный прорыв и имел в виду М. Цукерберг, когда говорил, что намерен развивать технологии виртуальной реальности далеко за пределы игрового сегмента. Есть множество подводных камней, но у затеи такой огромный потенциал, что никто не удивится, если компания потратит еще пару миллиардов на доводку сервиса до ума.

Просто потому, что потом она сможет зарабатывать на этом десятки миллиардов и как бы не ежемесячно. Да, очки виртуальной реальности стоят немало, а солидный перечень товаров нельзя оценить лишь «на глаз». Но, сколько мужчин будут бесконечно благодарны Facebook, избавившему их от ненавистного шоппинга. А за возможность с чистой совестью остаться дома и не таскаться за супругой с ворохом сумок и пакетиков многие с удовольствием оформят платную подписку на сервис и даже больше ***(Вот для чего Facebook купила стартап Oculus Rift // InternetUA (http://internetua.com/vot-dlya-csego-Facebook-kupila-startap-Oculus-Rift). – 2014. – 31.03).***

***

Чего только не делают маркетологи, чтобы привлечь внимание хотя бы небольшой части аудитории Facebook, которая в настоящее время составляет 1,23 млрд ежемесячных активных пользователей. Иногда они идут по пути создания более высококачественного контента или интеграции Facebook со своей маркетинговой стратегией. Привлечение клиентов таким способом, конечно, занимает больше времени, но число подписчиков на страницу компании в Facebook неуклонно растет, что дает ощутимые результаты, пишет Marketing Media Review (http://mmr.ua/news/id/7-rasprostranennyh-marketingovyh-fokusov-v-facebook-ot-kotoryh-stoit-otkazatsja-39099/).

Однако бывают случаи, когда маркетологи ищут легкие пути. Узнав, что какая-то компания при помощи «хака» смогла быстро набрать тысячи последователей, просмотров страниц или комментариев, они решают поступить таким же образом. У них нет времени на создание собственного сообщества лояльных клиентов и поклонников их компании, им необходимо привлечь внимание пользователей здесь и сейчас.

Вот только доказательств того, что подобные трюки работают, практически нет. Они сродни рекламе, обещающей быстрое похудение на 5 кг в неделю. Кроме того, некоторые из этих «советов» вполне могут стать вредными и снизить эффективность уже существующей кампании в Facebook.

Поэтому, если маркетологи намерены потратить время на создание органичной маркетинговой кампании на Facebook, они должны держаться подальше от этих рекомендаций, которые могут принести им больше вреда, чем пользы, или в лучшем случае просто не будут работать.

1. Включение ссылки в первый комментарий.

Около года назад появился довольно популярный миф, согласно которому включение ссылок на маркетинговый контент или сайт компании в первые комментарии, а не в само сообщение, увеличит шансы публикации на появление в ленте новостей. Это происходит якобы потому, что сообщения, содержащие только фото или только текст, лучше продвигаются системой, чем сообщения со ссылками.

На самом деле, это не совсем так. В действительности алгоритм Facebook в последнее время более лояльно относится к сообщениям со ссылками, хотя в прошлом это утверждение относилось к обновлениям статуса с фотографиями. Правда, мало кто видел даже неофициальные данные о том, что это работает.

Возможно, что использование этого «трюка» на некоторое время увеличит посещаемость страницы компании в соцсети, но на практике этот способ не совсем гуманный с точки зрения пользователя. Вряд ли стоит рассчитывать на лояльность поклонников и последователей, которым каждый раз для получения информации нужно будет делать лишние шаги, в отличие от одного простого клика на сообщении. А при наличии достаточно большого числа подписчиков комментарий со ссылкой вообще может затеряться в цепочке обсуждения (что совершенно контрпродуктивно).

2. Автопубликация твитов в Facebook.

В Facebook и Twitter предлагается синхронизировать аккаунты в этих двух соцсетях для автоматической кросспубликации контента. Каждое сообщение в Twitter будет продублировано на странице Facebook и наоборот. По крайней мере, этот трюк поможет сэкономить время и до последнего времени считался успешным инструментом расширения присутствия компании в соцсетях и «объединить» аудитории двух сервисов.

Что касается первого преимущества, несомненно, эта функция избавит от необходимости тратить время на публикацию одной и той же новости в каждой соцсети отдельно. Но в отношении второго утверждения есть три момента, которые его опровергают.

Во-первых, аудитория пользователей, которые следят за компанией в Facebook, – это не то же самое, что подписчики в Twitter. У поклонников в Facebook и в Twitter различные вкусы и предпочтения по форме и содержанию контента и даже по времени его предоставления. Если компания стремится вырастить свою аудиторию, необходимо размещать материалы с учетом потребностей своих почитателей, чтобы они видели заботу компании об интересах клиента.

Во-вторых, при синхронизации аккаунтов в Facebook и Twitter сообщения будут выглядеть странно – специфический формат Twitter не совсем уместен для сообщений Facebook (и наоборот).

В-третьих, говорят, что Facebook понижает позиции публикаций от сторонних сервисов в лентах новостей пользователей. Так что ваши твиты в Facebook будут замечены меньшим количеством читателей, чем если бы вы опубликовали эти сообщения напрямую в Facebook.

Кроме того, в твитах, попавших в Facebook, не отображаются ссылки и фотографии, потому что их просто «вытащили» из Twitter.

Так что не стоит полагаться на бездумную автоматизацию, которая будет делать работу маркетолога. Вместо этого необходимо разработать индивидуальные посты для каждой платформы. Дополнительное время, затраченное на создание контента в соответствии с особенностями каждой соцсети, окупится в долгосрочной перспективе ростом аудитории и вовлечения пользователей.

3. Покупка поклонников.

Это, вероятно, одна из лучших «хитростей», которые рекомендуют для построения армии последователей в Facebook. Это работает, если под «построением аудитории» подразумевать рост разношерстной и бессмысленной толпы «поклонников». Единственное, чего можно добиться таким путем – увеличения показателей самой страницы (цифры могут быть использованы в качестве аргумента перед начальством для обоснования прибавки к зарплате специалисту по SMM).

Однако если Facebook используется не только для того, чтобы собирать лайки на странице, то этот «трюк» лучше проигнорировать. Задача маркетинговой кампании в соцсети состоит в создании заинтересованной аудитории, которая может конвертироваться в клиентов. Покупка поклонников и последователей на самом деле принесет лишь вред для бренда.

Система Facebook, увидев, что процент взаимодействия страницы с последователями вдруг снижается, несмотря на рост аудитории, может не включить следующие обновления статуса страницы компании в новостные ленты поклонников или радикально понизить их позиции. Тем самым, использование «мертвых душ» может привести к тому, что вполне реальные и заинтересованные подписчики не смогут получать обновления или будут получать их с опозданием.

4. Отметки на фотографиях людей, которые не имеют к ним отношения.

Если какого-нибудь пользователя пометить на фотографии в Facebook, он получит уведомление. Таким образом, трюк состоит в том, чтобы помечать фотографии компании тегами случайных пользователей, чтобы как можно больше людей обратили внимание на бренд.

Этого делать не стоит. Эта тактика напоминает приемы спамеров, которые они использовали в прошлом, и пользователи Интернета уже выработали иммунитет к таким методам. Получив уведомление о том, что кто-то неизвестный отметил пользователя на своем фото, большинство пользователей Facebook будут держаться от него подальше. Это чистейшей воды спам, и это не сработает, зато репутацию бренду, наверняка, подпортит.

5. Тэгирование других брендов.

Недавно Facebook обновила свой алгоритм новостной ленты с целью поощрить бренды, которые отмечают другие бренды в своих сообщениях

(такие сообщения появляются на страницах отмеченных брендов). Это совсем не значит, что теперь необходимо помечать другие бренды в каждом отдельном сообщении. Facebook внимательно следит, насколько релевантны ссылки на другие страницы соцсети и как аудитория чужих компаний взаимодействует со страницей, сославшейся на бренд.

Из этого следует вывод – эта тактика должна применяться только тогда, когда маркетинговая кампания обладает ценным контентом для обеих аудиторий.

6. Приманки для лайков и комментариев

Многим знакомы сообщения в ленте новостей, которые выглядят, например, как картинка с подписью типа: «Сегодня мы предлагаем два вида мороженого: ванильное и шоколадное. Если вы предпочитаете ваниль, оставьте комментарий, если вы предпочитаете шоколад – поставьте лайк, или поделитесь сообщением, если вам нравится и то и другое!».

Даже если сообщение такого вида на странице Facebook соберет много читательских реакций, вряд ли оно принесет много пользы для бренда.

Максимум, что оно может сделать, – уведомить аудиторию о новом продукте компании и потенциально подготовить почву для нового сообщения в новостной ленте соцсети. Но это вряд ли сильно скажется на росте прибыли компании. Этот трюк может дать краткосрочные положительные результаты, но в долгосрочной перспективе он не приведет к росту сознательной аудитории.

Вместо этого нужно писать интересные сообщения, а не играть в игру «Обмани систему Facebook». Контент просто должен нравиться пользователям и получать за это лайки, комментарии и вирусное распространение.

7. Чрезмерное увлечение хэштегами.

Когда Facebook впервые запустил хэштеги, все начали включать их в свои посты. Однако с тех пор исследование страниц при помощи Edgerank Checker показало, что сообщения с хэштегами обладают меньшей вирусностью, чем сообщения без хэштегов.

Так что в будущем следует использовать хэштеги в Facebook разумно и экономно – только тогда, когда этого требуют условия кроссплатформенной маркетинговой кампании.

Мораль всего этого в том, что не стоит обманывать ни Facebook, ни поклонников, ни самих себя, играя в игры с созданием присутствия компании в Facebook. То, что могло сработать на пользу, в один прекрасный день может оказаться вредным. Построение аудитории в Facebook, ее расширение и вовлечение с целью конверсии требуют кропотливого и упорного труда, затрат времени и усилий ***(7 распространенных маркетинговых фокусов в Facebook, от которых стоит отказаться // Marketing Media Review (http://mmr.ua/news/id/7-rasprostranennyh-marketingovyh-fokusov-v-facebook-ot-kotoryh-stoit-otkazatsja-39099/). – 2014. – 2.04).***

***

В магазинах приложений каждый может найти средство для общения на свой вкус: WhatsApp, Line, Kakao Talk, WeChat и многие другие. И при этом пользователям не нужно платить что-либо за разговоры и переписку. Казалось бы, денег эти сервисы не приносят, но в то же время Facebook готова заплатить за WhatsApp 16 млрд дол. Очевидно, социальная сеть надеется как-то вернуть вложенные инвестиции. Но как зарабатывают мессенджеры? Читайте об этом ниже.

Если брать с пользователей прямые платежи нельзя, тогда требуется использовать альтернативные методы. Так, популярный в Японии, Тайване и Таиланде мессенджер Line приносит своим создателям прибыль при помощи трех источников: бесплатных игр, мультяшных картинок и официальные аккаунты для бизнеса и звезд. Игры в этом приложении распространяются на условиях free-to-play. Это значит, что сами развлечения бесплатны, а прибыль приносят внутриигровые покупки. Платные открытки, которые пользователи пересылают друг другу, используются также и многими другими интернет-сервисами. А платные официальные аккаунты для бизнеса и звезд позволяют им легально спамить пользователей Line различными промосообщениями и акциями.

«Вместо того, чтобы полагаться на одну бизнес-модель, мы пытаемся комбинировать несколько разных подходов», – отметила маркетинговый директор коммуникатора на очередной пресс-конференции. И это дает хорошие результаты: благодаря этим способам монетизации мессенджер постоянно наращивает выручку. Так, за один лишь IV квартал прошлого года она увеличилась в пять раз до 12,2 млрд йен (120 млн дол.). Годом ранее эта сумма составляла лишь 2,2 млрд йен.

При этом в Line отказались от обычной рекламы, которая, по мнению компании, является слишком навязчивой. Ее функции как раз взяли на себя официальные аккаунты для бизнеса и звезд. При этом компания даже им не рекомендует рассылать слишком много сообщений и стараться излагать мысли максимально кратко. А если же пользователю покажется, что ему не нужна эта информация или он получает слишком много посланий, тогда он имеет возможность отписаться от рассылки.

Деньги за дополнительные сервисы к сообщениям

Мессенджер Kakao Talk, который завоевал большую популярность в Южной Корее, использует похожие методы для зарабатывания денег. Он, например, предлагает пользователям сыграть во встроенную видеоигру Anipang. Кроме этого, сервис позволяет известным брендам и именам проводить платные массовые рассылки.

Но на этом руководство Kakao не останавливается и продолжает искать дополнительные деньги. Исполнительный директор этой платформы для общения С. Ли говорит, что компания в настоящее время экспериментирует с семью новыми источниками. Среди них – электронная коммерция и распространение музыки.

В Китае большую популярность завоевало приложение WeChat, которое создал местный интернет-гигант Tencent Holdings. Он, помимо применяемых Line и Kakao способов монетизации, внедрил сервис микроплатежей. Пользователи могут пересылать друг другу небольшие суммы денег и оплачивать товары, а мессенджер получает за это свой процент.

Миллиарды без прибыли

Иногда бесплатный мессенджер означает действительно отсутствие платы любыми способами. Одним из таких является приложение WhatsApp, которое недавно купила крупнейшая в мире социальная сеть Facebook. При этом в нем нет никаких дополнительных средств монетизации, как у Line, Kakao Talk и WeChat. Пользователи могут лишь отправлять друг другу сообщения.

По словам аналитиков, такая стратегия очень ограничивает возможности заработка для WhatsApp. В настоящее время этим приложением пользуются свыше 450 млн человек, но оно генерирует лишь 20 млн дол. Именно столько денег WhatsApp зарабатывает на тех, кто пользуется сервисом больше года, – именно столько длится бесплатный пробный период. Сами представители мессенджера не раскрывают число пользователей, которые платят.

В самом WhatsApp пока не переживают о монетизации – это дело будущего. Сперва представители компании хотят еще больше увеличить абонентскую базу и внедрить механизмы оплаты уже после этого. «Монетизация не будет приоритетом для нас, – сказал исполнительный директор WhatsApp Я. Коум на конференции по сделке с Facebook. – Мы сфокусированы на росте».

В Facebook тоже не волнуются о том, что переплатили и не вернут свои деньги. «WhatsApp на пути к тому, чтобы соединить миллиард человек. Сервисы, которые достигают этой планки, обладают невероятной ценностью, – комментирует покупку гендиректор Facebook М. Цукерберг. – Я давно знаком с Я. Коумом и с нетерпением жду начала сотрудничества с ним и его командой, чтобы сделать мир более открытым и коммуникабельным» ***(Миллионы на бесплатном: как мессенджеры зарабатывают деньги // InternetUA (http://internetua.com/millioni-na-besplatnom--kak-messendjeri-zarabativauat-dengi). – 2014. – 2.04).***

***

Крупнейшие мировые студии звукозаписи Sony Music, Universal Music и Warner Music подали иски в отношении «ВКонтакте». Социальная сеть обвиняется в распространении нелицензионной музыки, сообщает cnews.ru

Международная федерация производителей фонограмм (International Federation of the Phonographic Industry, IFPI), представляющая интересы около 1,3 тыс. звукозаписывающих компаний в 66 странах, инициировала судебное разбирательство против российской социальной сети «ВКонтакте».

Всего в Арбитражный суд г. Санкт-Петербурга и Ленинградской области было подано три отдельных иска от Sony Music Russia, Universal Music Russia и Warner Music UK.

«Предметом исков является создание на базе сети VK.com сервиса, который способствует крупномасштабным нарушениям смежных и авторских прав. Компания управляет нелицензированным музыкальным сервисом, содержащим огромную библиотеку музыкальных композиций, хранящихся на сайте компании. Сервис предоставляет десяткам миллионов пользователей неограниченный доступ к данной библиотеке, позволяя им осуществлять поиск и прослушивание музыки в потоковом режиме», – говорится в сообщении IFPI.

В исках приводится список исполнителей, в интересах которых звукозаписывающие компании добиваются судебных решений, обязывающих соцсеть удалить контрафактные музыкальные файлы со своего сервиса.

Звукозаписывающие компании также добиваются вынесения судебного решения о необходимости принятия сетью VK.com общепринятых в отрасли эффективных мер защиты собственности правообладателей.

Правообладатели также требуют возмещении материального ущерба в связи с нарушением смежных и авторских прав на сумму более 50 млн р. (1,4 млн дол.).

«Для успешного развития музыкальной индустрии в России необходимо, чтобы цифровые партнеры осуществляли лицензирование своей деятельности, соблюдали смежные и авторские права и выплачивали вознаграждение исполнителям и продюсерам за их работу и инвестиции», – считает Ф. Мур, исполнительный директор IFPI.

«В течение продолжительного периода времени мы неоднократно обращали внимание на данную проблему. Мы рекомендовали VK.com прекратить нарушения смежных и авторских прав и провести переговоры со звукозаписывающими компаниями. На данный момент компания не предприняла никаких существенных шагов по решению проблемы», – добавила она.

Это не первый иск в отношении «ВКонтакте», связанный с распространением нелицензионного контента. В октябре 2013 г. соцсеть выиграла один из таких исков. Он был подан звукозаписывающей студией «Союз». В решении суда отмечается, что сама «ВКонтакте» не участвует в распространении контрафактного контента, а нести ответственность за действия пользователей она не обязана. В самой соцсети ранее заявляли, что они всегда удаляют нелицензионный контент по запросу правообладателей, но удалять все файлы самостоятельно не могут, так как для этого требуются огромные ресурсы ***(Sony Music, Universal Music и Warner Music объявили войну «ВКонтакте» // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/38920/126/lang,ru/). – 2014. – 3.04).***

***

Facebook анонсировал, что метрика «Обсуждают это» (Talking About This (TAT)), введённая в 2011 г., в ближайшем будущем перестанет существовать. Этот параметр включал себя такие данные, как количество лайков, вовлечённых пользователей (уникальных посетителей, совершивших какое-либо действие на странице), упоминаний, чекинов и других способов взаимодействия со страницей.

После появления информации об исчезновении метрики «Обсуждают это», её прекратил учитывать и сервис по медиааналитике SocialBakers.

Мы опросили несколько российских экспертов, работающих с социальными медиа, и узнали, как они относятся к ликвидации метрики «Обсуждают это».

А. Усманов, экс-руководитель SMM «РИА Новости»: «Это правильный шаг со стороны Facebook. Надеюсь, он заставит маркетологов и SMM-специалистов сфокусировать свою работу на оценку своих действий с помощью более совершенных и целевых метрик: engagement, reach и других».

А. Круглов, евангелист «ВКонтакте»: «Меня регулярно просят оценить уровень вовлечения и с текущим подходом к метрикам мне это очень не нравится. Начнем с того, что показатель “вовлечения” можно считать по-разному – можно делить сумму действий на число подписчиков, а можно число уникальных активных пользователей. TAT, насколько я знаю, показывал именно число пользователей, что кажется более разумным.

Но беда маркетинга (особенно отечественного) в том, что никто не оценивает показатели разумно, а просто хочет быть повыше в “пузомерке”. Раньше все бренд-менеджеры ставили KPI в числе подписчиков. Подрядчики, как правило, всеми силами пытались этот показатель накрутить. Наиболее разумные измеряли и вовлечение, но после того, как Facebook ввел показатель TAT, подрядчики начали накручивать и его. Думаю, все помнят, как резко с вводом TAT стали популярны опросы, голосование в которых добавляло 1 пунктик к заветной “пузомерке”.

В гонках за количеством никто не смотрит на качество. На мой взгляд, любые метрики должны быть перевзвешены. Первоочередное взвешение должно быть на целевую аудиторию (ЦА) – то есть бренд-менеджер должен спрашивать с агентства не сколько фанов, а сколько целевых фанов (в абсолютном и относительном показателе). Если доля нецелевых высока – необходим комментарий, с чем это связано. Это может быть абсолютно нормальная история – на группу “Порше” будут подписываться дети, а в группу магазина женского белья вступит какое-то количество мужчин. Причины и того, и другого, думаю, объяснять не надо. Но может быть и обман клиента, когда абсолютно белыми методами в группу привлекают левую аудиторию, которая просто дешевле.

Когда речь идет о контенте, то помимо взвешивания ЦА (что именно она лайкает ваши посты) надо проводить оценку и самого контента по степени важности для бренда. Это довольно субъективный показатель, но, тем не менее, очевидно, что 20 лайков к продуктовому посту в разы ценнее ста лайков к “смишной” картинке зачем-то размещенной в группе бренда».

В. Стоколос, SMM-фрилансер: «Отмена “Обсуждают это”, конечно, удар по общему сбору статистики по странице. Благодаря метрике можно было оценивать популярность контента по трем важным показателям: лайкам, шэрам и комментариям. Теперь станет сложнее качественно и быстро измерять вовлечённость. Последнее время очень снизилось количество показов в лентах действий пользователей на страницах. У меня очень редко показываются репосты, их лайки и комментарии. Возможно, новые алгоритмы edgerank уже делают неактуальной данную метрику».

Е. Проскурина, сотрудница московского рекламного агентства: «Конечно, удобно зайти на страницу, не являясь её модератором, и сразу посмотреть, сколько людей вовлечены в процесс общения с брендом. По соотношению количества подписчиков страницы и метрики “Обсуждают это” можно понять, насколько аудитория этой страницы живая. Собственно, для администраторов в Facebook есть показатель охвата и реакции к конкретному посту в статистике, поэтому этот показатель также можно будет рассчитать и представить в отчете для клиента. Вот для анализа конкурентов станет сложнее. Чтобы понять, насколько страница читаема, нужно будет по старинке вручную подсчитывать количество отметок like, share и комментариев. Хотя, эти показатели и сейчас выводятся в отчетах».

П. Гуров, PR-специалист кинокомпании «ПРОвзгляд»: «Это странно, что Facebook отказывается от своей официальной метрики Talking About This, ведь они ей так гордились: чтобы презентовать новинку, посол Facebook в России Е. Скоборогатова собрала целую пресс-конференцию в 2011 г., что бывает крайне редко.

“Обсуждают это” позволял легко посчитать рейтинг вовлеченности аудитории (Facebook Engagement Index) для любой страницы, в том числе и чужой. Facebook Engagement Index считается так: количество “Обсуждают это” делится на общее количество подписчиков и умножается на 100 %. В итоге мы получаем показатель, который позволяет понять, насколько размещаемый контент работает – то есть вызывает лайки, комментарии и перепосты.

Зная “Обсуждают это” для страницы любого бренда (скрыть этот показатель невозможно) мы можем понять, например, что кинокомпания, где я работаю, имеет рейтинг вовлечения в 4,7 %, а сама компания Facebook – всего лишь 0,87 %. Получается, наш контент в 5,4 раза успешней стараний работников Facebook. Дело в том, что из-за новых алгоритмов Facebook у страниц брендов-гигантов рейтинг вовлечения начал катастрофически проседать. Видимо, чтобы скрыть эту неудобную правду, Facebook и решил

отказаться от метрики, с которой они еще недавно носились как с писаной торбой».

С. Беганский, независимый SMM-консультант: «Значение Talking About This, которое мы видим в Facebook, – общий показатель всех взаимодействий со страницей. После обновления раздела статистики, где представлены подробные данные о всех типах действий пользователей на странице бренда, нет смысла держать ещё одну общую суммарную цифру. Все данные теперь есть в статистике, их можно отфильтровать, выгрузить в отдельный документ. Не понимаю, почему кто-то переживает из-за этого. Скорее всего, не все коллеги до конца разобрались в том, что на самом деле убирают, и какие данные теперь доступны в других местах. Это всё, конечно, теперь будет видно только администраторам, сторонним пользователям информация будет недоступна. Но никто не мешает зайти на страницу и «по-старинке» оценить активность пользователей: количество комментариев, лайков, расшариваний.

Что касается возможности быстрой оценки качества работы других страниц (например, конкурентов) по этому параметру, то я считаю это не совсем правильной практикой. Просто для сведения, может быть, это и интересно, но не нужно опираться в своей работе на данные конкурентов. У каждого бренда есть своя аудитория со специфическими чертами поведения. Не всегда она любит комментировать, не всегда лайкать… Да и сама цифра – не показатель, его можно при желании накрутить. Количество комментариев на странице не означает популярность бренда, это могут быть негативные комментарии. Чекины в ТЦ (и это тоже считалось в ТАТ) не означают, что контент на его странице крутой и популярный, а работа специалистами по социальным медиа ведётся превосходно. Нужно работать со своими пользователями и контентом исходя из задач, которые ставятся для работы в соцсетях».

Н. Белоусов, CEO Madrobots.ru: «Метрики, предлагаемые социальными медиа, до сих пор представляют собой своеобразный зоопарк. Twitter, “ВКонтакте”, Facebook – все предлагают что-то своё.

Facebook, как крупнейшая социальная сеть, да ещё и публичная компания, задает в тон в создании метрик, имитирующих бизнес-показатели. Если обратите внимание, в сети постоянно выходят статьи о том, что метрики, используемые в социальных медиа, ничего не значат.

Я вижу суть проблемы в пересечении двух категорий рекламного рынка – бренд-менеджеров и самих социальных медиа.

Бренд-менеджеры гонятся за круглыми числами лайков, так как «у конкурентов больше фолловеров» и чьи бонусы привязаны к этим надуманным показателям.

Социальные медиа, которые постоянно меняют правила игры и не предлагают метрик, которые бы помогли измерять влияние присутствия в социальных медиа на бизнес. У социальных медиа есть две опции, в сторону которых можно развивать свои метрики:

– мимикрировать под показатели медийной рекламы (охват, частота, CTR и пр.);

– давать бизнес-показатели (помечать лиды и их “теплоту”, считать стоимость целевого действия для клиента, но не лайки).

Пока они движутся в сторону медийной рекламы, намекая, что социальные медиа – это штука для больших брендов. А попутно они изобретают массу ненужных показателей вроде того же Talking About This».

Р. Зарипов, SMM-менеджер: «Показатель TAT был полезен для поверхностной оценки конкурентного окружения бренда.

В целом, эта цифра не очень объективно позволяет оценивать успешность страницы. Если людям нравится делиться вашими новостями, показывать их друзьям и не только ради розыгрыша приза со случайным выбором победителя, не ради халявного айфона (которого в 99 % случаев не существует), а просто потому, что они клевые и интересные – это лучшая заслуга» ***(Facebook избавится от метрики Talking About This (+комментарии экспертов) // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_izbavitsya_ot_metriki_talking_about_this_kommentarii_ekspertov). – 2014. – 4.04).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Исследователи выяснили, что головной мозг у юношей и девушек еще недостаточно сформирован, чтобы противостоять той зависимости, которая возникает при многочасовом пользовании социальными сетями. Специалисты определили, что, общаясь во всемирной паутине, мы так или иначе рассчитываем на некое поощрение нас другими пользователями Интернета. Такого рода поощрение может выражаться, например, в том, сколько раз наши виртуальные собеседники нажимают кнопку «мне нравится», когда хотят дать положительную оценку нашим фотографиям или мыслям, опубликованным во всемирной паутине, или же в том, какие эмоции они выражают посредством так называемых «смайликов».

В тот момент, когда наши друзья по переписке ставят нам «лайки», мы получаем определенное удовлетворение, обусловленное выделением в головном мозге гормона под названием дофамин. Это вещество представляет собой нейромедиатор, который служит важной частью «системы поощрения» мозга, поскольку вызывает чувство удовольствия, чем влияет на процессы

мотивации и обучения. Данный гормон естественным образом вырабатывается в больших количествах во время некоего позитивного, по субъективному представлению человека, опыта – к примеру, полового акта, приёма вкусной пищи, приятных телесных ощущений, а также наркотиков.

Мексиканские исследователи обнаружили, что у подростков, которые проводят в социальных сетях, таких как Facebook или Twitter, по 4–5 часов в день, уже прослеживаются определенные симптомы зависимости. В качестве сравнения, если раньше юноше или девушке для выработки дофамина в их головном мозге достаточно было получить 5–7 «лайков», то теперь подсознательно молодые люди ожидают уже 20–30 «лайков», чтобы почувствовать себя интересными для окружающих.

По мнению ученых, эта тенденция пагубно сказывается на жизни подрастающего поколения вне всемирной паутины. Так, у зависимых от Интернета подростков наблюдаются существенные проблемы при общении со сверстниками и взрослыми в реальной жизни. Кроме того, согласно исследованию, неконтролируемое пребывание в виртуальном пространстве может пагубно сказаться и на образовательном процессе.

Специалисты Национального института психиатрии настоятельно рекомендуют родителям ограждать своих отпрысков от чрезмерного увлечения различного рода социальными сетями до тех пор, пока их психика не окрепнет окончательно, чтобы противостоять многочисленным соблазнам и негативным факторам, присутствующим в Интернете ***(Исследование: в соцсетях «виснет» молодежь до 18 лет // NewsOboz (http://newsoboz.org/obshchestvo/issledovanie-v-sotssetyah-visnet-molodezh-do-18-let-30032014235800). – 2014. – 30.03).***

***

Тревожит ли вас то, что пишут и публикуют ваши друзья в социальных сетях?

Личная информация, которую вы публикуете в Интернете, может обернуться против вас. Исследователи из Корнеллского и Северо-Западного университетов (оба – США) предупреждают, что, вообще говоря, думать надо не только о себе.

Опрос пользователей Facebook выявил множество историй о том, как Facebook-друзья размещали в сети разнообразные фотографии, которые могли нанести ущерб третьим лицам. О чём речь? Это, например, были снимки пьяных приятелей или просто фотографии, представляющие человека в том виде, в котором он сам себе не нравится. Сам бы он их никогда публиковать не стал, а вот его «заботливые» друзья, думающие только о себе...

Беда лишь в том, что в эпоху цифровых технологий ваше само- и просто мнение больше вам не принадлежит. Вот что говорит корнеллский профессор Д. Хэнкок: «Социальные медиа перестали быть периферией нашей жизни, они давно стали её частью!» И с этим трудно не согласиться.

Профессор, его аспирантка Э. Споттсвуд и их коллеги представили исследование «Эти неловкие моменты: коллективное самомнение и потеря лица в Facebook» на конференции ACM, проходившей 15–19 февраля в Балтиморе (США).

Работа строилась на опросе 150 пользователей Facebook, которых попросили описать то, какие именно чужие сообщения в соцсети им неприятны. Затем респонденты должны были оценить уровень дискомфорта таких постов. Кроме упомянутых «неприятных» фотографий, пользователям не нравится, когда их друзья (вдруг) делают политические заявления, которых те от них не ожидали. Или банально лгут. Наконец, многие обеспокоены тем, что потенциальный работодатель может увидеть нечто их компрометирующее. В общем, всё ожидаемо: испуг, ложь и опять испуг.

Исследователи замечают, что у человека может быть несколько разных аудиторий. И то, что может устраивать одну, другой покажется неприятным. Если ваш коллега посмеётся над карикатурой, то ваша бабушка, например, посчитает её вульгарной и осудит вас. Интересно, что чем разнообразнее были группы друзей у опрашиваемых, тем выше они оценивали уровень дискомфорта, который испытывали при чтении неприятных сообщений или просмотре неудобных фотографий. К тому же некоторые люди уделяют больше внимания своему имиджу, чем другие. Так вот те, кого это особенно волнует, тоже описывали уровень дискомфорта в подобных ситуациях как повышенный.

Испытуемых также просили сообщать о том, как долго они пользуются Интернетом и сетью Facebook. Как и ожидалось, Facebook-профи меньше беспокоились о том, что в соцсети может быть опубликовано что-то, что им не понравится. Потому что они знают, как с этим бороться: к примеру, можно убрать отметку о себе на неприятном фото. С другой стороны, старожилы Интернета (а не только соцсети) испытывали больший дискомфорт. Потому, наверное, что понимают, как далеко может зайти публикация информации во Всемирной сети...

Исследователи считают, что социальные сети должны иметь функции, которые способны предотвратить такие проблемы. Скажем, перед отправкой сообщения пользователь должен иметь возможность сделать пометку, каким группам друзей это будет видно. Или хотя бы просто получить сначала такое предупреждение: «Вы уверены, что хотите, чтобы этот пост увидели все?»

В любом случае мы должны хорошенько подумать, прежде чем публиковать в сети что-то касающееся других людей. И, думается, это относится не только к сетевой жизни. Впрочем, всё это такие прописные истины... ***(Как потерять лицо в Facebook // InternetUA (http://internetua.com/kak-poteryat-lico-v-Facebook). – 2014. – 6.04).***

Лже-смс отправлют на благо военных

Нестандартный метод информвойны придумали пользователи соцсетей. «Для ускорения получения паспорта РФ необходимо отправить СМС на 565 (фиксация для сокращения очередей). Данная услуга ФМС является бесплатной и действует на всей территории Украины и Крыма», – говорится в объявлении. На самом деле пользователи сети сыграли злую шутку с желающими побыстрее получить паспорт РФ – со счета после отправки СМС снимается 5 грн в пользу украинской армии, потому как номер был создан для пожертвований украинским военным ***(Серов И. Поскорее получить российский паспорт поможет СМС на номер 565 – соцсети // Сегодня (http://www.segodnya.ua/regions/krym/poskoree-poluchit-rossiyskiy-pasport-pomozhet-sms-na-nomer-565-socseti-505036.html). – 2014. – 25.03).***

***

Власникам сторінки «Типичный Киев» у «ВКонтакте» пропонували розмістити фейкову новину про те, що нібито українське Міністерство фінансів планує підвищити мінімальну ставку податку на доходи фізосіб з 15 до 20 %.

Як повідомляють власники сторінки, за розміщення новини їм пропонували 3000 російських рублів. Пропозиція надійшла через внутрішню систему розміщення платних постів.

Власники групи відмовились від пропозиції і вирішили зробити цю історію публічною.

«Кремлевские рабы предлагают нашей группе “ВКонтакте” 3000 рублей за публикацию фейковой информации об якобы увеличении минимальной ставки подоходного налога для физических лиц с нынешних 15 до 20 %.

Заявку мы отклонили. Не секрет что размещаем рекламу, это помогает нам каждый день максимально отдаваться нашим читателям. Но обойдемся без тысячных кремлевских бюджетов как и обходятся без них украинские солдаты что до последнего стоят в Крыму за Украину!»

Цікаво, що пропозицією скористалося чимало популярних пабліків у «ВКонтакте». Їх можна знайти, наприклад, задавши такий пошук у соцмережі ***(В соцмережах платять майже $100 за поширення антиукраїнських новин // UkrainianWatcher (http://watcher.com.ua/2014/03/24/v-sotsmerezhah-platyat-mayzhe-100-za-poshyrennya-antyukrayinskyh-novyn/). – 2014. – 24.03).***

***

Соціальна мережа Twitter активно просуває фейкову сторінку кандидата в Президенти України П. Порошенка, що вводить в оману засоби масової інформації, повідомила 2 квітня прес-служба політика, пише

Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3343360-nevidomi-pyshut-u-Twitter-vid-imeni-poroshenka).

«Так, у соціальній мережі Twitter невідомими робляться записи від імені П. Порошенка і, використовуючи можливості Twitter, дезінформують читачів», – зазначили в повідомленні.

У прес-службі повідомили, що відкриття всіх комунікаційних платформ і майданчиків П. Порошенка відбудеться найближчим часом із широким анонсуванням ***(Невідомі пишуть у Twitter від імені Порошенка // Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3343360-nevidomi-pyshut-u-Twitter-vid-imeni-poroshenka). – 2014. – 2.04).***

***

Властям Кубы не понравилась американская социальная сеть ZunZuneo. Кубинское правительство назвало «нелегальными и подрывными» попытки США запустить на острове новую социальную сеть.

По мнению ведомства, подобная попытка в очередной раз доказывает, что США не отказались от своих подрывных планов против кубинских властей. В ведомстве полагают, что США продолжают дестабилизировать ситуацию на Кубе, дабы спровоцировать изменения в политической системе страны. Власти Кубы призвали США отказаться от своих нелегальных и подрывных намерений на Кубе и начать уважать международное право.

Социальная сеть под названием ZunZuneo была запущена в 2009 г. Она была сделана на базе сотовой связи, так, чтобы обойти действующие ограничения на доступ в Интернет. ZunZuneo визуально и практически очень напоминала популярный сервис микроблогов Twitter. С помощью ZunZuneo можно было быстро передавать короткие сообщения между пользователями.

Куба обвиняет США в том, что социальная сеть предназначена для ведения антиправительственной пропаганды. Проект финансировался Агентством международного развития США и был закрыт в 2012 г. в связи с недостаточным финансированием ***(Властям Кубы не понравилась американская социальная сеть // InternetUA (http://internetua.com/vlastyam-kubi-ne-ponravilas-amerikanskaya-socialnaya-set). – 2014. – 5.04).***

Зарубіжні спецслужби і технології «соціального контролю»

Новые данные, обнародованные Э. Сноуденом, вновь бросают тень на деятельность АНБ США. В новых утечках Э. Сноуден рассказывает о кибер-шпионаже США за китайскими производителями электроники, а также за китайскими высокопоставленными чиновниками. Немецкое издание Der Spiegel сообщает о том, что АНБ США с 2009 г. активно шпионило за компанией Huawei Technologies, крупнейшим китайским производителем

телекоммуникационного оборудования, а также за тогдашним главой КНР Х. Дзиньтао.

Отметим, что именно с 2009 г. США начали активно давить на Huawei, а также заявлять о нескончаемых атаках китайских госхакеров. В 2011 г. Вашингтон настоятельно рекомендовал американскому госсектору отказаться от закупок оборудования Huawei, так как заподозрил Huawei в связях с китайской разведкой и заявил, что в оборудовании Huawei возможны аппаратные закладки для осуществления шпионажа. В итоге, Huawei была вынуждена отказаться от продажи своего телеком-оборудования в США, сохранив там лишь каналы продаж смартфонов.

Согласно данным Э. Сноудена, США шпионили не только за Х. Дзиньтао, но и за неназванными чиновниками из китайского Минфина, Министерства торговли и Министерства иностранных дел. Также объектами шпионажа стали представители крупнейших китайских банков.

Э. Сноуден передал Der Spiegel презентацию, которую тот в свое время похитил из АНБ, где была подробно расписана схема, кто, когда и за кем следил. Согласно схеме, объектом шпионажа являлся и основатель компании Huawei Р. Чженфей. АНБ, в частности, удалось перехватывать сообщения топ-менеджера компании. В статье не уточняется, о каких именно сообщениях идет речь.

АНБ также получило доступ к исходным кодам программного обеспечения некоторых продуктов Huawei. Кража исходников производилась в рамках операции Shotgiant, в которой принимали участие Белый дом, ЦРУ США, а также ФБР. Э. Сноуден отмечает, что все эти ведомства были в курсе программ шпионажа, хотя публично говорили прямо противоположные вещи.

Der Spiegel приводит слова Б. Пламмера, пресс-секретаря Huawei, который говорит, что если США такой шпионаж осуществляли, то они «должны были знать, что Huawei является независимой компанией, не имеющей никаких связей с правительством». Он также отметил, что в свете новых данных становится очевидно, что Вашингтон намеренно проводил кампанию по дискредитации Huawei и дезинформации ее клиентов.

Немецкий журнал отмечает, что АНБ США отказалось как-либо прокомментировать готовящиеся к публикации данные. Der Spiegel приводит выдержки из внутренних документов АНБ, в которых говорится, что в рамках кампании было собрано так много данных о Huawei, что АНБ «теперь не знает, что с ними делать». Сообщается, что специалисты АНБ взломали внутреннюю сеть Huawei, скопировали данные о 1400 клиентах этой компании, а также получили доступ к корпоративной документации ***(Сноуден: АНБ шпионило за Huawei и китайскими лидерами // InternetUA (http://internetua.com/snouden--anb-shpionilo-za-Huawei-i-kitaiskimi-liderami). – 2014. – 24.03).***

***

Турецкий суд разблокировал на территории страны сервис микроблогов Twitter, сообщает Hurriyet Daily News. Доступ к сервису был закрыт 20 марта.

Административный суд Анкары постановил, что блокировка Twitter противоречит принципам правового государства. Управление по связи и коммуникации Турции может оспорить решение, но до этого оно обязано открыть доступ к ресурсу.

С требованием восстановить доступ к Twitter в суд обратилась коллегия адвокатов Турции. Кроме того, множество турецких пользователей подали похожие иски в Констиуционный суд.

Управление по связи и коммуникациям заблокировало Twitter после того, как закрыть доступ к сервису микроблогов пообещал премьер-министр страны Р. Эрдоган. Глава страны требовал, чтобы Twitter удалил твиты со ссылками на прослушку его телефонных разговоров, в которых шла речь о взятке размером в 10 млн дол. Власти Турции пытались заставить администрацию сервиса сделать это через суд, но представительство Twitter не отреагировало на иски. Тогда правительство решило полностью закрыть доступ к платформе.

Twitter в Турции пользуются около 10 млн человек. Сервис был запущен в 2006 г., а турецкий интерфейс появился в апреле 2011 г. Несмотря на блокировку, количество твитов, отправленных турецкими пользователями, продолжило расти. За первый день блокировки их было больше 2,5 млн, в то время как обычно этот показатель составляет 1,8 млн твитов ***(Турция разблокировала Twitter // InternetUA (http://internetua.com/turciya-razblokirovala-Twitter). – 2014. – 26.03).***

***

Власти Турции сняли запрет на использование социальной сети Twitter. Об этом сообщает BBC, пишет Обозреватель (http://obozrevatel.com/abroad/31924-v-turtsii-otmenili-zapret-na-twitter.htm).

Правительство выполнило решение Конституционного суда, который признал запрет пользования социальной сетью нарушением свободы выражения взглядов ***(В Турции отменили запрет на Twitter // Обозреватель (http://obozrevatel.com/abroad/31924-v-turtsii-otmenili-zapret-na-twitter.htm). – 2014. – 4.04).***

***

Администрация Б. Обамы предложила внести поправки в законодательство, которое положит конец сбору телефонных данных американцев, собранных Агентством национальной безопасности (АНБ). Об этом сообщило издание the New York Times.

В соответствии с предлагаемым законодательством, АНБ прекратит массовый сбор телефонных метаданных телекоммуникационных компаний, сообщает the New York Times. Агентство, в свою очередь, будет иметь

возможность получить определенные записи от носителей только с разрешения судьи.

Согласно новому плану Белого дома, операторы связи должны будут сохранять записи телефонных разговоров не дольше полутора лет вместо нынешних пяти лет. К тому же, АНБ имеет право располагать доступом к нужной ему информации и записям с разрешения судьи.

Таким образом, администрация Б. Обамы предоставляет судьям право принимать решение об оправданности подозрений относительно того или иного телефонного номера.

В издании отмечают, что Белый дом планирует соблюдать программу АНБ по сбору данных еще в течение одного 90-дневного срока. Нынешнее судебное разрешение на сбор данных истекает 28 марта ***(Белый дом планирует запретить АНБ собирать записи телефонных разговоров американцев // InternetUA (http://internetua.com/belii-dom-planiruet-zapretit-anb-sobirat-zapisi-telefonnih-razgovorov-amerikancev). – 2014. – 25.03).***

***

Согласно новым данным, опубликованным в немецкой прессе 30 марта, британская радиоэлектронная разведка GCHQ шпионила за немецкими интернет-компаниями, а разведка США осуществляла более масштабную, нежели считалось ранее, слежку за канцлером Германии А. Меркель.

Новый отчет базируется на новых данных, переданных журналу Der Spiegel Э. Сноуденом. В статье отмечается, что британский Правительственный центр связи регулярно следил за деятельностью всех основных немецких провайдеров. Э. Сноуден сообщил, что за крупнейшими операторами проводилась «глубокая и постоянная» слежка. Сообщается, что конечной целью британцев и их американских партнеров был доступ к значительным объемам интернет-трафика внутри Германии.

В статье, в частности, говорится, что за немецкой компанией Stellar была установлена практически тотальная слежка. Компания Stellar арендует спутниковые мощности и управляет рядом наземных станций в Германии, предоставляя услуги беспроводного доступа в сеть, передачи данных и голоса для немецких властей, буровых платформ в море, удаленных офисов немецких компаний и др.

Der Spiegel сообщает, что британская сторона была заинтересована не только в наблюдении за сетевым трафиком, но и занималась «идентификацией важных клиентов немецких провайдеров, изучала их технологических поставщиков, а также технологические тренды в среде немецких поставщиков услуг связи».

Э. Сноуден отметил, что в АНБ США была внедрена автоматизированная система сбора и записи данных Nymrod, которая следила в том числе и за А. Меркель. По данным Э. Сноудена, всего в системе около 300 упоминаний о А. Меркель. В данных Der Spiegel сказано, что в марте прошлого года подразделение АНБ Special Sources Operations получило

разрешение суда по иностранной разведдеятельности на реализацию широкой программы шпионажа за Германией. В статье не говорится, на каком основании вынесено такое решение.

На фоне полученных данных, Der Spiegel делает логичное предположение о том, что АНБ США занималось не только отстаиванием государственных интересов США, но и занималось экономическим шпионажем в интересах ряда американских компаний. Официально американская разведка категорически отвергает идею экономического шпионажа. Кроме того, Der Spiegel отмечает, что в президентском докладе от 17 января 2014 г., когда Б. Обама говорил о президентской реформе АНБ после разоблачений Э. Сноудена, первый говорил о том, что АНБ выполняет директивы, направленные «исключительно на обеспечение национальной безопасности», тогда как новые данные говорят о том, что АНБ проводило программы экономического шпионажа, о которых Б. Обама не мог не знать ***(АНБ занималось экономическим шпионажем в Германии // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/31/economic-espionage.html). – 2014. – 31.03).***

***

На території Росії заблокували доступ до сайтів та груп у соціальних мережах, які висвітлюють діяльність «Правого сектору».

Голова Служби з нагляду у сфері зв'язку, інформаційних технологій і масових комунікацій Росії О. Жаров наголосив на тому, що росіяни не зможуть отримати доступ до сайтів та сторінок у Facebook і Twitter, пов'язаних із «Правим сектором», – пише ТСН.

«Ми припинили повністю їх поширення на всій території Російської Федерації, у всіх мережах, в тому числі в Facebook і в Twitter. Ця робота принципово важлива, ми її маємо намір продовжувати», – сказав представник Роскомнагляду.

За словами О. Жарова, у відомство вже направили 30 вимог від Генпрокуратури щодо блокування сайтів екстремістського змісту ***(У Росії заблокований доступ до сайту і соцмереж «Правого сектору» // ВолиньPost (http://www.volynpost.com/news/30372-u-rosii-zablokovanyj-dostup-do-sajtu-i-socmerezh-pravogo-sektoru). – 2014. – 2.04).***

***

Прокуратура Москви винесла попередження двом російським контент-провайдерам за перепости О. Навального, який перебуває під домашнім арештом. Про це повідомляється в блозі Навального, у якому розміщено попередження прокуратури, передає Еспресо.TV.

«Боротьба з блогом О. Навального стала прямо справжнім "завданням державного значення"», – наголошується в повідомленні.

У прокуратурі звернули увагу на те, що в соціальних мережах, блогах та інших сервісах, що надають можливість розміщення й поширення інформації від імені опозиціонера та групи пов'язаних з ним осіб, здійснюється систематична публікація текстів, відео- та аудіоматеріалів.

Прокуратура підкреслює, що надання послуг з поширення «забороненої» інформації перешкоджає виконанню судового рішення, а «невиконання рішення суду – це кримінальний злочин». Окрім того, порушення заборони, встановленої судом, може стати підставою для зміни самому О. Навальному запобіжних заходів.

Член Ради з прав людини при президенті І. Засурський вважає, що спроби вилучити з мережі згадки про О. Навального лише привертають до нього увагу.

Нагадаємо, суд заборонив О. Навальному користуватися Інтернетом. На час арешту опозиціонера блог веде його дружина Ю. Навальна і співробітники Фонду боротьби з корупцією ***(Прокуратура Росії заборонила репостити в соцмережах записи з блогу Навального // Espreso.tv (http://espreso.tv/new/2014/04/01/prokuratura_v_rosiyi_zaboronyla_repostyty_v_socmerezhakh_zapysy_z_blohu_navalnoho). – 2014. – 1.04).***

***

Правила применения дополнительных мер и временных ограничений в условиях чрезвычайного положения, которые позволят вводить комендантский час, прекращать деятельность партий и проверять публикуемую в СМИ информацию, утвердило правительство Казахстана своим постановлением. Документ опубликован в информационно-правовой системе нормативных правовых актов республики. Сообщает jourdom.ru

Для «осуществления контроля за средствами массовой информации» комендатура местности в течение суток с момента принятия ограничений направляет запросы собственникам СМИ о предоставлении обязательных экземпляров печатных изданий и материалов радио- и телепередач, говорится в правилах.

Предполагается, что в комендатуру местности для согласования их содержания предоставляются обязательные экземпляры печатных изданий и материалов радио- и телепередач за сутки до их выпуска (выхода в эфир), а при невозможности выполнения данного условия (формирование срочных новостных выпусков) непосредственно перед выпуском (выходом в эфир).

Согласно правилам, при выпуске несогласованных печатных изданий, радио- и телепередач комендант местности направляет собственнику СМИ распоряжение о приостановлении и/или прекращении выпуска СМИ либо распространении его продукции ***(Власти Казахстана утвердили правила для СМИ при чрезвычайном положении // Media бізнес (http://www.mediabusiness.com.ua/content/view/38897/126/lang,ru/). – 2014. – 2.04).***

Проблема захисту даних. DDOS та вірусні атаки

ИБ-эксперты обнаружили в ОС шесть Pileup-уязвимостей, которые присутствуют в версиях Android Open Source Project и более чем 3,5 тыс. кастомизированных версий платформы.

Более миллиарда устройств, работающих на базе Android, уязвимы к атакам класса «повышение привилегий». Об этом свидетельствует доклад, подготовленный совместными усилиями Индианского университета в Блумингтоне и Microsoft.

Как утверждают специалисты, повышение привилегий через обновление (privilege escalation through updating, pileup) предоставляет злоумышленникам большие возможности установить вредоносные приложения послу установления апдейта. При этом пользователь может даже не подозревать о происходящем.

В докладе эксперты по вопросам ИБ отметили, что обновления для ОС выпускаются раз в несколько месяцев, что приводит к появлению огромнейшего количества новых и дополнительных файлов. Для того чтобы программа не затронула уже установленные на устройстве приложения, ее необходимо очень тщательно настроить.

В докладе также сообщается о том, что в Android обнаружено шесть Pileup-уязвимостей, которые присутствуют в версиях Android Open Source Project и более чем 3,5 тыс. кастомизированных версий Android, а это свыше миллиарда уязвимых устройств. Google уведомили о брешах, и на текущий момент уже исправлена одна уязвимость.

По словам исследователей, главная проблема заключается в том, что для большей удобности пользователя уведомления о появлении на платформе нового приложения не отображаются, а устанавливаются в фоновом режиме. Таким образом, владелец Android-устройства не может повлиять на процесс обновления ***(Более миллиарда устройств на базе Android уязвимы к атакам класса «повышение привилегий» // InternetUA (http://internetua.com/bolee-milliarda-ustroistv-na-baze-Android-uyazvimi-k-atakam-klassa--povishenie-privilegii). – 2014. – 24.03).***

***

Транспортный департамент Калифорнии, США, стал жертвой масштабной хакерской атаки. По предварительным данным, жертвами инцидента могли стать несколько тысяч жителей американского мегаполиса.

Впервые об инциденте стало известно на прошлой неделе. Так, представители MasterCard сообщили, что кредитные карты, используемые посетителями веб-сайта транспортного департамента для различных транзакций, могут фигурировать в различных инцидентах безопасности, связанных с кражей персональных данных и личной информации. По данным компании, в руках злоумышленников могли оказаться номера кредитных

карт, информация о сроке их годности, а также «трехзначные коды безопасности».

Точное количество скомпрометированных карт в настоящее время не раскрывается, однако, по информации независимого исследователя Б. Кребса, сам факт нападения подтвердили не менее пяти финансовых организаций, заинтересованных в расследовании инцидента. Кроме того, эксперт уверен, что взлом произошл в период с 2 августа 2013 г. по 21 января 2014 г.

Интересно, что согласно официальной статистике атакованного департамента, по итогам 2012 г. он обработал порядка 12 млн онлайн-транзакций (на 6 % больше, чем в 2011 г.) ***(Калифорнийский транспортный департамент атаковали хакеры // InternetUA (http://internetua.com/kaliforniiskii-transportnii-departament-atakovali-hakeri). – 2014. – 24.03).***

***

Одним из наиболее распространенных средств незаконной монетизации на китайском рынке Android-приложений является внедрение стороннего функционала и рекламных модулей в популярные программные продукты, а также навязывание программ пользователям и максимальное увеличение трафика для веб-сайтов, распространяющих те или иные приложения. Очень часто для этих целей злоумышленники используют различные вредоносные программы-загрузчики, и именно группу таких троянцев удалось выявить специалистам компании «Доктор Веб».

Центральную позицию в данной группе занимает вредоносная программа Android.DownLoader.49.origin, являющаяся стандартным Android-приложением. Запускаясь после установки в качестве системного сервиса, этот троянец соединяется с удаленным сервером, откуда получает список объектов, которые ему требуется загрузить. Среди них присутствует ряд содержащих dex-файлы архивов, которые помещаются на карту памяти в каталог /cache/sysjar/ и затем при помощи метода DexClassLoader загружаются в оперативную память мобильного устройства. Один из этих исполняемых файлов представляет собой троянца-загрузчика, внесенного в вирусную базу под именем Android.DownLoader.43.origin и способного скачивать различные приложения, включая вредоносные. Другой файл содержит троянца-«дроппера», который, в зависимости от модификации, при наличии root-доступа может устанавливать другие вредоносные приложения в системный каталог.

Помимо этих архивов, Android.DownLoader.49.origin может загрузить и ряд различных программ, которые также устанавливаются без разрешения пользователя. Если же root-доступ отсутствует, владелец мобильного устройства увидит стандартный системный запрос на установку скачанной программы.

В свою очередь, троянец Android.DownLoader.43.origin способен аналогичным образом связываться с удаленным сервером с целью получения списка приложений для загрузки и установки на инфицируемом мобильном устройстве. Примечательно, что в этом списке присутствуют и другие троянцы-загрузчики, обладающие схожим функционалом. Таким образом, вирусописатели создали цепочку из вредоносных программ, осуществляющих распространение как друг друга, так и приложений, установка которых по тем или иным причинам выгодна для киберпреступников. В общей сложности специалистами компании «Доктор Веб» было обнаружено около 10 подобных троянцев-загрузчиков, а сервер, принадлежащий злоумышленникам, содержит почти 600 программ, предназначенных для несанкционированной установки.

Наиболее вероятным мотивом создателей данной схемы является несанкционированная установка различных приложений на мобильные устройства пользователей с целью их незаконной популяризации и получения соответствующего заработка с каждой их инсталляции. Однако помимо обычных программ по команде с сервера в любой момент могут быть загружены и другие вредоносные приложения, например, СМС-троянцы или троянцы-шпионы, которые также могут принести владельцам этой сети дополнительный доход ***(Новые Android-троянцы выполняют несанкционированную установку приложений // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/25/Android-trn.html). – 2014. – 25.03).***

***

В НАИРИТ оценили масштаб внешнего воздействия на объекты инфраструктуры российской экономики. По данным исследования, проведенного экспертами НАИРИТ, совместно с ИСА РАН и Институтом социально экономической модернизации, количество DDOS-атак на государственные и коммерческие инфраструктурные институты за последний год возросло на 178 %, тогда как в прежние годы их темпы роста не превышали в среднем 15 %. При этом общий объем потерь отечественной экономики от попыток незаконного электронного вмешательства за этот период времени превысил 1,3 трлн р.

Как заявила президент НАИРИТ О. Ускова, выступая на заседании Комиссии Государственной думы РФ по развитию стратегических информационных систем, необходимо в срочном порядке принять меры по предотвращению подобного вмешательства в первую очередь за счет создания эффективных отечественных средств информационной инфраструктуры. Кроме того, считает О. Ускова, в России существует богатый опыт разработки и эксплуатации стратегических информационных систем, создания собственных технологий информационной безопасности, и этот опыт необходимо использовать в масштабах страны ***(Количество***

DDOS-атак на инфраструктурные объекты российской экономики возросло на 178 % // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/25/ddos-stats.html). – 2014. – 25.03).

***

Не менее 800 серверов в России были заражены в ходе кибератаки Windigo, сообщает Eset. Россия входит в число стран, где находится больше всего атакованных серверов, добавили в антивирусной компании.

Эксперты выяснили, что в кибератаке Windigo было задействовано шесть видов вредоносного ПО и сервисов. При этом Россия занимает восьмую строку списка государств, где находятся серверы, зараженные трояном Linux/Ebury, и входит в тройку стран, где обнаружено больше всего машин, пострадавших от трояна Perl/Calfbot.

Троян Linux/Ebury компрометирует серверы под управлением Linux, предоставляет злоумышленникам полный доступ к системе через командную строку и возможность кражи учетных данных SSH. В свою очередь, Perl/Calfbot компрометирует все ОС, которые имеют в своем составе установленный пакет Perl, и отвечает за рассылку спама.

Операция Windigo началась предположительно в 2011 г. В течение нескольких лет ее организаторам удалось скомпрометировать более 25 тыс. Linux- и UNIX-серверов и широкий спектр операционных систем, включая Windows, OS X, OpenBSD, FreeBSD и Linux. В числе пострадавших от Windigo такие организации, как cPanel и Linux Foundation.

«Мы установили, что атакующие смогли провести операцию установки вредоносной программы на десятках тысяч серверов, – говорит М.-Э. Левейе, вирусный аналитик Eset. – Использование антивирусных продуктов и механизмов двухфакторной аутентификации для рабочих станций является обычным явлением, но, к сожалению, эти способы редко применяют для защиты серверов. Как следствие – злоумышленники могут установить вредоносный код и похитить аутентификационные данные учетных записей».

Для получения доступа к серверам авторы Windigo не использовали какие-либо уязвимости – только украденные учетные данные и изначально скомпрометированные приложения. В дальнейшем база учетных записей пополнялась за счет вновь зараженных машин.

Сегодня в мире используется порядка 10 тыс. зараженных серверов. Ежедневно на набор эксплойтов перенаправляются свыше 500 тыс. посетителей скомпрометированных сайтов. Windigo отвечает также за рассылку порядка 35 млн спам-писем в день.

Веб-сайты, которые обслуживаются зараженными Windigo серверами, перенаправляют пользователя на потенциально опасный контент в зависимости от установленной операционной системы. Так, компьютеры с Windows заражаются вредоносным ПО, использующим уязвимость в браузере или плагине к нему. Пользователь OS X будет перенаправлен на сайт знакомств, а iPhone – на страницу с порнографическим контентом.

Участники рабочей группы Eset отмечают, что вредоносные программы Windigo разработаны на достаточно высоком уровне. В них используются техники сокрытия присутствия в системе, переносимость между различными платформами, криптография.

Если система заражена, потребуется полная очистка памяти, переустановка операционной системы и всего программного обеспечения. Необходимо также сменить все используемые пароли и ключи, поскольку существующие учетные данные могут быть скомпрометированы, отмечают эксперты ***(В ходе крупнейшей кибератаки в России были заражены 800 Linux-серверов // InternetUA (http://internetua.com/v-hode-krupneishei-kiberataki-v-rossii-bili-zarajeni-800-Linux-serverov). – 2014. – 26.03).***

***

Ряд записей на сайте микроблогов Twitter, включая многие популярные «твиты», стали недоступны в результате внутреннего сбоя. Об этом пишет РИА Новости со ссылкой на сообщения западных СМИ.

По данным информагентства, администрация Twitter знает о возникших проблемах и принимает меры для их решения. «В настоящее время мы изучаем ошибку, которая привела тому, что часть записей была скрыта», – заявили в компании. Масштабы произошедшего не разглашаются.

В числе пропавших оказался и самый популярный «твит» за всю историю сервиса. Он был сделан в начале марта ведущей церемонии вручения премии «Оскар» Э. Дидженерес и в течение часа собрал около 1,8 млн ретвитов.

В настоящее время запись уже вернулась в открытый доступ. Количество ее ретвитов превышает 3,4 млн, а 2 млн человек добавили «твит» в число избранных.

Помимо этого, проблемы с доступностью записей наблюдались у официальных микроблогов телеканала CNBC, газеты The Daily Mail, группы One Direction, исполнителей Lady Gaga и Д. Бибера ***(Ошибка в Twitter привела к пропаже самых популярных записей // InternetUA (http://internetua.com/oshibka-v-Twitter-privela-k-propaje-samih-populyarnih-zapisei). – 2014. – 26.03).***

***

Антивирусные компании выражают обеспокоенность по поводу окончания поддержки Windows XP со стороны Microsoft. Почти все банкоматы в мире работают под управлением этой ОС и после прекращения поддержки станут чрезвычайно уязвимыми к хакерским атакам. Специалисты Symantec, например, выявили новый метод взлома банкоматов с помощью обычного текстового сообщения, пишут «Экономические известия» (http://news.eizvestia.com/news_technology/full/462-hakery-nachali-vzlamyvat-bankomaty-s-pomoshhyu-obychnogo-sms).

Для этого, правда, злоумышленникам надо проделать достаточно опасную для них работу. На банкомат необходимо установить вредоносное ПО Ploutus, затем к устройству с помощью кабеля надо подсоединить телефон и отослать на него два определенных SMS. Текстовые сообщения трансформируются в сетевой пакет, который заставляет банкомат выдавать наличные, информирует news.eizvestia.com.

В Symantec рассказали о новом способе взлома АТМ, чтобы продемонстрировать уязвимость банкоматов. Пока о массовом взломе с помощью SMS речь не идет, хотя в Мексике подобные случаи уже были зафиксированы ***(Хакеры начали взламывать банкоматы с помощью обычного SMS // «Экономические известия» (http://news.eizvestia.com/news_technology/full/462-hakery-nachali-vzlamyvat-bankomaty-s-pomoshhyu-obychnogo-sms). – 2014. – 27.03).***

***

Летающие дроны могут быть приспособлены для перехвата личных данных пользователей смартфонов и планшетов, включая логины, пароли и даже домашние адреса, передает The Daily Mail.

Пока неизвестно, действительно ли подобные случаи происходили в США или Великобритании, однако эксперимент, проведенный журналистами CNN в Лондоне совместно со специалистом в области компьютерной безопасности Г. Вилкинсоном, дал хороший и наглядный результат.

В ходе эксперимента дрон, которого назвали Снупи (Любопытный), летал над городскими улицами и получал доступ к гаджетам, на которых был включен приемник Wi-Fi-сигнала. Оборудование, установленное на дроне, передавало устройствам ложный сигнал, маскируясь под публичную сеть. В результате «шпион» получал доступ ко всей информации, которую смартфон или планшет передавал в сеть, включая логины и пароли на разных сайтах или данные о кредитных картах владельца.

Журналисты сняли новостной сюжет про подвиги Снупи, в котором Г. Вилкинсон демонстрирует сведения об учетной записи несуществующего пользователя Yahoo, созданной для демонстрации возможностей дрона.

Эффективным способом предотвратить подобную потерю данных (даже если в роли похитителя выступает не дрон, а наземный прибор) является отключение Wi-Fi-приемника устройства или запрет на использование публичных беспроводных сетей ***(Хакеры могут использовать дронов для перехвата паролей // InternetUA (http://internetua.com/hakeri-mogut-ispolzovat-dronov-dlya-perehvata-parolei). – 2014. – 26.03).***

***

Корпорация Symantec обнаружила новую разновидность червя Linux.Darlloz, нацеленного на так называемый «Интернет вещей» (Internet of Things) – роутеры и сет-топы (ресиверы цифрового телевидения).

Специалисты обнаружили более 31 тыс. устройств, подключенных к Интернету и зараженных этим червем. Кроме того, эксперты Symantec выяснили, что задача новой версии червя – добыча виртуальной валюты. Специалисты компании полагают, что вирусописатель продолжит совершенствовать данную вредоносную программу для повышения ее монетизации.

В ноябре прошлого года специалисты корпорации Symantec обнаружили червь под названием Linux.Darlloz, зона поражения которого – «Интернет вещей» (Internet of Things): жертвой вредоносной программы являются компьютеры, построенные на архитектуре Intel x86, а также ARM, MIPS и Power PC, которые обычно встречаются в роутерах и сет-топах (ресиверы цифрового телевидения). В середине января этого года эксперты компании встретились с новой разновидностью этой программы. Судя по результатам анализа, автор червя постоянно совершенствует код и добавляет новые функции, особенно в плане монетизации вируса.

Эксперты Symantec обнаружили, что задача данной версии червя – добыча (так называемый «майнинг») криптовалюты. Как только компьютер, построенный на архитектуре Intel, заражается новой версией вируса, червь устанавливает на систему cpuminer− программу для майнинга виртуальной валюты. Затем зараженный компьютер начинает осуществлять добычу одной из двух малопопулярных криптовалют Mincoin или Dogecoin. К концу февраля 2014 г. злоумышленнику удалось таким образом добыть 42438 Dogecoin (около 46 дол. на момент написания) и 282 Mincoin (около 150 дол. на момент написания). Это относительно небольшие суммы денег для киберпреступления, поэтому специалисты Symantec полагают, что вирусописатель продолжит совершенствовать свое детище для повышения его монетизации.

Эта новая функция активируется только на компьютерах с архитектурой Intel x86 и обходит стороной более слабые сетевые устройства. Это связано с тем, что майнинг требует значительных вычислительных ресурсов, которыми такие устройства не располагают.

Зараженные вирусом устройства начинают осуществлять майнинг электронных валют под названием Mincoin и Dogecoin, вместо того чтобы заниматься самой популярной и самой ценной криптовалютой Bitcoin. Причина состоит в том, что Mincoin и Dogecoin используют алгоритм шифрования, позволяющий успешно осуществлять майнинг и на домашних компьютерах, в то время как для успешной и более быстрой добычи Bitcoin уже требуется ASIC чип.

Исходная версия Darlloz имела девять комбинаций «логин − пароль» для роутеров и сет-топов. Последняя версия имеет 13 таких комбинаций, которые также работают и для IP-камер, обычно используемых для видеонаблюдения.

Суть «Интернета вещей» заключается в объединении между собой множества разнообразных устройств. В то время как большинство

пользователей может обеспечить надежную защиту своего стационарного компьютера, многие из них и не подозревают о том, что другие устройства, подключенные к «Интернету вещей», также нуждаются в защите. В отличие от обычных компьютеров, многие такие устройства поставляются с уже установленными на них по умолчанию комбинациями «логин – пароль», а пользователи, в свою очередь, не удосуживаются их поменять. В результате, использование стандартных комбинаций логина и пароля – один из лучших способов взлома таких устройств. Многие из них содержат также уязвимости, о которых неизвестно пользователям.

В настоящее время угроза направлена на компьютеры, роутеры, сет-топы и IP-камеры, однако в будущем в этот список могут войти и другие устройства, такие как, например, устройства элементы «умного» дома и нательные компьютеры.

Как эксперты Symantec писали в предыдущей публикации, червь не дает другим вирусам, таким как, например, Linux.Aidra, атаковать устройства, уже зараженные Linux.Darlloz. Автор этой вредоносной программы включил эту функцию в первую версию червя, появившуюся в ноябре 2013 г.

В начале ноября поступали сообщения о существовании некого бэкдора на ряде роутеров. Используя этот бэкдор, злоумышленники могли удаленно получать доступ к роутеру и заражать сеть. Автор Darlloz воспринял это как угрозу, в результате чего, заражая роутер, червь стал создавать в межсетевом фильтре новое правило, блокирующее порт для этого бэкдора, тем самым блокируя доступ другим злоумышленникам.

Заразив устройство, Darlloz запускает веб-сервер на порте 58455, при помощи чего затем осуществляет самораспространение через Интернет. На сервере размещаются файлы вируса, которые загружаются на компьютер любого, кто подаст запрос HTTP GET по этому адресу. Мы искали статичные IP-адреса, где был открыт этот порт и где были размещены файлы Darlloz. Исходя из того, что Darlloz можно скачать, мы попытались собрать интернет-отпечатки серверов, на которых он был размещен ***(Червь атакует сетевые устройства для добычи криптовалюты // ITnews (http://itnews.com.ua/news/72129-cherv-atakuet-setevye-ustrojstva-dlya-dobychi-kriptovalyuty). – 2014. – 26.03).***

***

Вероятность заражения компьютера при установке контрафактного программного обеспечения (ПО), загруженного с веб-сайтов или файлообменных сетей, достигает 76 %, заявил на круглом столе 26 марта директор по консалтингу компании IDC в России Т. Фарукшин.

Сама программа может и не содержать вирусы, а заражение произойдет при попытке скачать ее из сети, отметил эксперт. По словам руководителя отдела по продвижению лицензионного ПО Microsoft Д. Берестнева, в среднем ресурсы с пиратским ПО тратят на свое продвижение по 20–

30 тыс. дол. в месяц и зарабатывают эти деньги именно на торговле доступом к компьютерам либо информации пользователей.

При использовании нелегальных ключей активации программ вероятность заражения оценивается в 68 %, а при покупке устройств с установленным контрафактным ПО в рознице – в 50 %. «Чтобы обезопасить себя от этого риска, необходимо приобретать компьютеры в крупных розничных сетях и проверять наличие лицензий», – отметил Т. Фарукшин.

По данным IDC, многие пользователи сами облегчают задачу злоумышленникам, пренебрегая обновлениями функций безопасности. Обновления, с помощью которых разработчики ПО устраняют уязвимости, своевременно не устанавливают 53 % «домашних» пользователей и 28 % IT-директоров в России, среднемировые показатели чуть ниже – 43 % и 26 % соответственно. При этом почти 80 % респондентов IDC, имевших проблемы с программным обеспечением на домашнем ПК, либо скачали его в Интернете, либо взяли у знакомых.

Больше всего при использовании программного обеспечения пользователи опасаются потери данных и личной информации, временных и материальных затрат на решение проблем, а также взлома учетных записей и банковских счетов. Несмотря на это, желание сэкономить «перевешивает» эти риски и остается основной причиной использования пиратского ПО домашними пользователями. При этом около 68 % респондентов знают, что ПО защищено авторским правом, а 79 % осведомлены об ответственности за использование контрафактных программ ***(Три четверти пиратского ПО в Интернете содержит вредоносные коды // InternetUA (http://internetua.com/tri-csetverti-piratskogo-po-v-internete-soderjit-vredonosnie-kodi). – 2014. – 27.03).***

***

Французская некоммерческая ассоциация потребителей UFC-Que Choisir подала от имени пользователей исковое заявление в Верховный суд Парижа против компаний Facebook, Twitter и Google, в котором требует удалить из пользовательских соглашений компаний с ее точки зрения несправедливые или незаконные пункты. Группа заявляет, что три компании никак не отреагировали за письма юристов ассоциации, отправленных еще в июне прошлого года, в которых UFC-Que Choisir просила изменить тексты соглашений, определяющих условия работы с личными данными.

В ассоциации говорят, что компании намеренно делают их пользовательские соглашения необоснованно большими, сами соглашения изобилуют юридическими терминами и оборотами, которые непонятны простому обывателю, помимо этого, в сообщениях часто фигурируют гиперссылки на документы на иностранных языках, которые могут быть в принципе недоступны читателю.

Помимо этого, UFC-Que Choisir отмечает, что компании крайне неохотно что-либо поясняют пользователям относительно принципов работы

с информацией. Вдобавок к этому, контакты по юридическим вопросам в целом – это проблема для пользователей сервисов всех трех компаний.

В иске французская правозащитная группа хочет добиться от компаний более коротких, простых и четких правил работы с информацией, в идеале на 1–2 страницах, не более. Кроме того, группа заявляет, что компании регулярно и в одностороннем порядке меняют правила работы с пользовательской информацией, тогда как пользователи (это оговорено в соглашении) по умолчанию принимают любые модификации без возможности их оспаривания (главное, чтобы они в целом соответствовали закону конкретной страны). Зачастую скорость изменения так называемых Terms and Conditions поражает. К примеру, в UFC-Que Choisir зафиксировали случай, когда Facebook дважды меняла политику в течение семи дней.

Также в иске группа заявляет, что нынешние соглашения составлены таким образом, что интернет-компании получают безусловное право на сбор, обработку и дальнейшее использование в собственных целях пользовательских данных. Группа заявляет, что данное обстоятельство приобрело характер эпидемии: соцсети разворачивают кампании по тотальной слежке за пользователями и региструют каждый их шаг.

Согласно французскому законодательству, компании имеют возможность предоставить письменный ответ на жалобу UFC-Que Choisir в суде ***(Французская правозащитная группа судится с Google, Facebook и Twitter // InternetUA (http://internetua.com/francuzskaya-pravozasxitnaya-gruppa-suditsya-s-Google--Facebook-i-Twitter). – 2014. – 27.03).***

***

По словам экспертов из IBM Security Systems, им удалось обнаружить несколько уязвимостей (CVE-2014-1484, CVE-2014-1515, CVE-2014-1506) в Firefox для Android, которые позволяют вредоносным приложениям перехватывать данные из профиля пользователя.

Для того чтобы проверить действие брешей, специалисты разработали несколько атак, в рамках которых изначально определялось имя каталога профиля в веб-браузере, а затем похищен ряд данных, среди которых файлы cookie и кэшированная информация. При этом исследователям IBM «вытаскивали» данные из случайной папки и нарушали работу песочницы Android.

Отметим, что Firefox для Android хранит личные данные в каталоге, находящемся в /data/data/org.mozilla.firefox/files/mozilla/.default. Рандомизация имя каталога позволяет более надежно защитить данные от перехвата.

Для генерации имени каталога используются символы, находящиеся в восьми случайных индексах в буквенно-цифровом массиве.

По словам экспертов, эксплуатировать уязвимости можно несколькими способами, но результат будет одним и тем же: злоумышленник установит имя каталога профиля и похитит важную информацию, в том числе, cookie-

файлы, кэш и историю браузера ***(Уязвимости в Firefox для Android позволяют перехватывать данные из профиля пользователя // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/27/Firefox-Android-flaw.html). – 2014. – 27.03).***

***

Мобильными ботнетами под Android никого не удивишь. Вредоносные программы обычно распространяются через сторонние каталоги приложений и вместе с переупакованными оригинальными программами. Однако антивирусная компания TrendMicro обнаружила нечто новенькое: скрытым модулям для майнинга криптовалюты удалось проникнуть даже в Google Play. Причем они распространяются с некоторыми довольно популярными приложениями. Например, с программой Songs, у которой более миллиона скачиваний!

TrendMicro классифицировала новое семейство зловредов-криптомайнеров как AndroidOS_KageCoin.HBT. Как же им удалось спрятаться от эмулятора Google Bouncer, который автоматически проверяет функциональность приложений перед регистрацией в каталоге?

TrendMicro выяснила, что в этих приложениях код для майнинга активируется только во время зарядки устройства. Вероятно, подобные сценарии не отрабатываются в эмуляторе. Очень логичное поведение для майнера: повышение энергопотребления остается незамеченным для пользователя. Более того, сам пользователь может рассматривать такой «нежный» режим майнинга как приемлемую альтернативу рекламным баннерам, которые сжигают трафик и заряд аккумулятора, да еще и раздражают своим видом. Вот вам и решение давней проблемы микроплатежей!

Конечно, процессор мобильного устройства обладает мизерной вычислительной мощностью и способен сгенерировать сущие копейки, но если таких устройств миллионы, то овчинка стоит выделки.

В конфигурационном файле указаны учетные данные для загрузки результатов в пул для совместной добычи монет ***(CPU-майнеры прячутся в приложениях Google Play // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/27/mobile-malware-mines-dogecoins-and-litecoins-for-bitcoin-payout.html). – 2014. – 27.03).***

***

Командование южнокорейских военных IT-экспертов предотвратило попытку хакерской атаки с целью хищения секретных военных материалов. По словам представителя Министерства обороны страны, в ходе нападения злоумышленники намеревались использовать инфицированный вредоносным ПО ноутбук. Устройство принадлежало человеку, имевшему доступ к внутренней компьютерной сети ведомства.

Поскольку предотвратить взлом удалось на самом раннем этапе, в руки злоумышленников не успела попасть какая-либо ценная информация. В то же время эксперты смогли выяснить, что для кражи информации неизвестные намеревались использовать сервер в Австрии.

«Мы считаем, что вредоносный код был написан по заказу правительства Северной Кореи или северокорейскими хакерами», – прокомментировал представитель Минобороны.

По его словам, к такому выводу расследовавших инцидент экспертов привел обнаруженный ими удаленный сервер злоумышленников ***(Южная Корея предотвратила попытку кражи секретных военных материалов // InternetUA (http://internetua.com/uajnaya-koreya-predotvratila-popitku-kraji-sekretnih-voennih-materialov). – 2014. – 29.03).***

***

Эксперты по вопросам информационной безопасности Indian Computer Emergency Response Team (CERT-IN) сообщают, что на сегодняшний день вирус Dendroid активно используется во вредоносной кампании, направленной на владельцев Android-устройств из Индии.

По данным издания The Hacker News, злоумышленникам вредонос необходим для создания приложений с трояном, которые инфицируют смартфоны на базе ОС от Google.

Dendroid способен создать кастомизированную версию APK-файла. Благодаря этому вредонос может удалять и изменять список контактов и другие журналы, открывать любые веб-страницы через установленный веб-обозреватель, набирать любой номер, записывать телефонные разговоры, перехватывать SMS-сообщения, загружать изображения и видео на удаленный сервер и пр.

Напомним, что в начале текущего месяца стало известно о существовании Dendroid. Тогда эксперты из Lookout отметили, что вредонос способен взять под свой контроль практически любое Android-устройство ***(Злоумышленники используют Dendroid для атак на пользователей // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-Dendroid-dlya-atak-na-polzovatelei). – 2014. – 30.03).***

***

Facebook разработал платформу для сбора и систематизации информации об интернет-угрозах. Проект под названием ThreatData позволяет собирать и хранить информацию в произвольной форме. Также фреймворк в реальном времени предоставляет данные для защитных систем и долгосрочного анализа.

«Сейчас очень сложно поддерживать безопасность сети. Для успешного выполнения этой задачи мы должны постоянно следить за новыми угрозами

и изучать уже существующие. Проект ThreatData был создан, чтобы облегчить эту работу», – сообщают представители Facebook .

«Летом 2013 г. мы зафиксировали высокое число вирусных атак, антивирусная сигнатура которых содержала строку J2ME. Дальнейший мониторинг выявил спам-кампанию, которая использовала фиктивные аккаунты Facebook. После этого мы смогли определить название вируса, проанализировать его и применить меры по прекращению спам-кампании. Скриншот показывает пример подобной активности за декабрь 2013 г.», – продолжают они.

Ниже представлена карта, показывающая совокупный объём вредоносных и пострадавших IP-адресов по странам. Круговая диаграмма демонстрирует разбивку таких адресов по провайдерам для США.

Платформа ThreatData позволяет специалистам с лёгкостью строить подобные карты и графики в течение минуты ***(Facebook запустил фреймворк для сбора информациии об интернет-угрозах // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_zapustil_freymvork_dlya_sbora_informatsiii_ob_internet_ugrozah). – 2014. – 1.04).***

***

Двадцать один из 25 крупнейших мировых поставщиков новостного контента являются целями крупномасштабной хакерской атаки, за которой стоит одно из государств. Об этом говорится в докладе специалистов Google по информационной безопасности, информирует news.eizvestia.com (http://news.eizvestia.com/news_abroad/full/474-google-preduprezhdaet-o-hakerskoj-atake-na-novostnye-agentstva).

Ш. Хантли, специалист по безопасности программного обеспечения Google, говорит, что атаки были инициированы хакерами, работающими при поддержке властей или непосредственно на них. В рамках атаки атакующие рассылают целевые поддельные письма журналистам. М. Маркис-Буа, соавтор отчета, подчеркивает, что атака на информационные агентства происходит независимо от страны базирования агентства и тематической ориентации агентства.

Оба специалиста отказались раскрыть данные о том, как именно Google вышла на следы атаки, но они заявляют, что следы атаки ведут к хакерским группам, которые в прошлом уже были ассоциированы с так называемыми госхакерами. Ш. Хантли говорит, что недавно Google начала рассылать предупреждения журналистам, если есть подозрения относительно того, что они стали объектом наблюдений и/или атак.

Достоверно неизвестно о какой именно группировке хакеров идет речь, однако ранее просирийская группа Сирийская электронная армия атаковала журналистов Forbes, the Financial Times и the New York Times. Кроме того, ранее появлялись данные о том, что хакеры из Китая атаковали крупные западные новостные организации ***(Google предупреждает о хакерской***

атаке на новостные агентства // «Экономические известия» (http://news.eizvestia.com/news_abroad/full/474-google-preduprezhdaet-o-hakerskoj-atake-na-novostnye-agentstva). – 2014. – 31.03).

***

Согласно свежему исследованию RAND Corporation, украденные Twitter-аккаунты теперь стоят больше, чем банковские карты. Авторы исследования объясняют, что это действие закона спроса и предложения: стоимость кредиток заметно упала, когда на рынок хлынули десятки миллионов карт, полученные после больших взломов последнего времени, в том числе после успешной атаки на американскую сеть магазинов Target (во время декабрьского взлома в руки хакеров попали около 40 млн карточек).

Стоимость карточек сильно зависит от их «свежести». Наиболее высокая цена держится в первые дни после взлома, потому что в это время наиболее высока вероятность, что карточки работают, а не заблокированы владельцем. Со временем цена падает, и рынок переполняется товаром. Например, стоимость одного пользовательского аккаунта (с паролем, домашним адресом и другой личной информацией) снижается с 20–135 дол. в первые дни после взлома до 0,75 дол.

Исследователи отмечают, что за минувшие годы рынок криминальных товаров эволюционировал от частного бизнеса к организованной торговле, в которой участвуют крупные группы, иногда имеющие отношение к традиционной организованной преступности и связи с государственными структурами. По этой причине рынок привлекает больше внимания со стороны правоохранительных органов.

Рынок этих товаров принципиально не отличается от обычного рынка. Здесь тоже продавцы и покупатели общаются и совершают сделки по разным каналам, размещают заказы и предлагают товар на форумах, на открытых и закрытых торговых площадках.

На рынке особенно высоко ценятся аккаунты в Twitter. Даже спамерский аккаунт в Twitter стоит в пять раз больше, чем спамерский аккаунт на Yahoo. Это тоже часть эволюции рынка: если в середине 2000-х тут в основном торговали дампами банковских карт, то в настоящее время рынок расширяется в сторону социальных медиа, аккаунтов на сайтах электронной коммерции и проч.

Некоторые участники подпольной торговли получают сверхприбыли, превышающие возможный доход от торговли наркотиками, считают эксперты. Вообще, продавцы здесь обычно имеют крайне узкую специализацию.

Отличие подпольной торговли от обычной в том, что здесь зашкаливает уровень паранойи: после множества арестов и облав последних лет участники рынка не доверяют новым игрокам и друг другу, чаще используют криптографические инструменты, обфускаторы, анонимайзеры и т. д. Больше стало форумов, закрытых от посторонних, сообщает RAND

Corporation ***(Хакономика: твиттер-аккаунты дороже банковских карт // InternetUA (http://internetua.com/hakonomika--tvitter-akkaunti-doroje-bankovskih-kart). – 2014. – 28.03).***

***

Программные продукты Word и Excel стали объектами новой хакерской атаки с участием нового вредоносного программного обеспечения, похищающего данные пользователей и скрывающего перемещения в сети при помощи анонимной сети Tor, говорится в новом бюллетене по безопасности антивирусной компании Trend Micro.

Инженер по безопасности Trend Micro A. Нието говорит о проведении вредоносной кампании на протяжении некоторого периода времени неизвестной хакерской группой. По его словам, обнаруженный Word- и Excel-вредонос входит в семейство вредоносов Crigent (также известных как Power Worm). Данные вредоносы используют несколько новых техник, которые ранее не находили значительного применения. A. Нието говорит, что пока данные техники были использованы только против Word и Excel, но в будущем они могут быть применены и против других программных продуктов.

При попадании на компьютер вредонос подгружает дополнительные модули, которые скачивают ПО для работы с Tor, а также модуль Polipo, представляющий собой персональный веб-кэш и прокси.

На первой стадии атаки организаторы используют Windows PowerShell для кражи данных и системе-жертве, такие как ее IP-адрес, местонахождение, привилегии аккаунта, версию ОС, архитектуру процессора и данные о компонентах Microsoft Office. В Trend Micro говорят, что организаторы кампании собирают большой диапазон данных, которые в будущем потенциально могут быть использованы как-то иначе.

Собрав аналитические массивы, они подселяют модули-анонимайзеры, которые прячут сетевой трафик, по которому передаются краденные данные на C&C-сервер посредством сети Tor.

В Trend Micro говорят, что им пока не удалось установить, как именно используются краденные данные, так как местоположение контрольного сервера пока неочевидно ***(Новый Tor-вредонос ворует данные из Word и Excel // InternetUA (http://internetua.com/novii-Tor-vredonos-voruet-dannie-iz-Word-i-Excel). – 2014. – 1.04).***

***

Компания Symantec проанализировала программу под названием CryptoDefence, появившуюся в прошлом месяце. Она является одним из членов семейства вредоносных программ, которые шифруют пользовательские файлы и не снимают блокировку до момента оплаты. В Symantec говорят, что данный вид шантажа очень давно известен в ИТ-отрасли, однако, он, судя по всему, еще работает.

CryptoDefence использует инфраструктуру Microsoft и Windows API для генерации шифровой последовательности и шифрования/дешифрования данных. Шифруются файлы при помощи RSA-ключей с длиной последовательности 2048 бит. Здесь применяются закрытые ключи, необходимые для дешифрования контента и отправки его на сервер атакующего, чтобы вернуть их клиенту, когда тот выплатит требуемую сумму.

Однако авторы вредоноса неверно реализовали алгоритм шифрования и не учли или не знали, что частный ключ по умолчанию сохраняется на компьютере пользователя в папке, откуда целевой файл вызывал соответствующие системные функции. «Авторы атаки оставляли ключи от шифров на компьютере пользователей, что позволяло пользователям без каких-либо платежей самим расшифровать зашифрованные вредоносом данные», – говорят в Symantec.

Между тем авторы атаки требовали от своих жертв сумму в 500 дол. или евро за расшифровку, причем если жертва не выплачивала их в течение четырех дней, то на пятый день сумма требований удваивалась. Согласно оценкам Symantec, организаторы кампании заработали шантажем не менее 34 тыс. дол. в месяц. Судя по данным срабатывания антивирусного софта Symantec, CryptoDefence заразил около 11 тыс. хостов в более чем 100 странах. Большая часть заражений пришлась на США, Великобританию, Канаду, Австралию, Японию, Индию, Италию и Нидерланды ***(Разработчики троянца-шантажиста забыли удалить крипто-ключи // InternetUA (http://internetua.com/razrabotcsiki-troyanca-shantajista-zabili-udalit-kripto-kluacsi). – 2014. – 1.04).***

***

В последние годы двумерные (матричные) QR-коды (от английского Quick Response, то есть «быстрый отклик») получили самое широкое распространение: их нередко используют в рекламе, в различных вывесках и музейных табличках, на плакатах и в журналах. Это произошло в значительной степени благодаря популярности смартфонов и планшетов, способных после установки небольшого приложения безошибочно распознавать такие коды. Чаще всего в QR-кодах зашифрованы ссылки на страницы в Интернете, сведения о сети Wi-Fi, СМС с номером и сообщением, текст или географические координаты объекта, но теоретически в них могут скрываться какие угодно данные.

Однако популярность любой технологии, особенно значительно упрощающей какие-то не слишком удобные действия, неизбежно вызывает повышенный интерес злоумышленников, пытающихся использовать её для извлечения незаконной выгоды. И QR-коды не стали исключением из правила, хотя на первый взгляд совершенно непонятно, как их можно использовать, к примеру, для кражи личной информации или денежных средств.

По уже весьма устаревшим данным ComScore за июнь 2011 г., только за один тот месяц в США более 14 млн человек старше 13 лет просканировали какой-либо QR-код своим мобильным телефоном: около 39 % сделали это в магазинах, примерно 20 % – на работе, а приблизительно 58 % – у себя дома. И это данные, касающиеся исключительно территории США!

Большая часть из тех, кто воспользовался QR-кодами, – мужчины (60,5 %), более половины любителей инноваций (53,4 %) приходится на возраст от 18 до 34 лет, около трети (36 %) – от 25 до 34, при этом годовой доход семей 36,1 % пользователей (более чем одного из трёх) превышал 100 тыс.! Молодые состоятельные мужчины – лакомый кусочек для любых мошенников.

Между тем приёмы взломщиков применительно к QR-кодам остаются теми же самыми, что используются при взломе любых других электронных систем: это, как всегда, сочетание чисто технических средств с элементами социального инжиниринга. Цели тоже остаются неизменными: похищение cookies и личных данных, фишинг, взлом виртуальных магазинов и даже Google Glass.

Чтобы приобрести что-нибудь в интернет-магазине, виртуальном магазине либо через рекламу на улице, в журнале или в Интернете с помощью QR-кода, нужно просто просканировать этот код камерой смартфона или планшета, после чего вы будете перенаправлены на веб-страницу с дополнительной информацией о товаре и способах оплаты и доставки. При этом вы отправляете в Интернет какие-то ваши личные данные, в том числе и реквизиты оплаты для карточной или какой-то другой платёжной системы.

Вот самая элементарная схема мошенничества с QR-кодами, расположенными в публичных местах. Возьмём для примера виртуальные магазины, которые представляют собой просто большие стенды с фотографиями товаров, их ценами и соответствующими QR-кодами. Обычно в таких магазинах есть три варианта доставки после оплаты: скачивание (для музыки, видео или программного обеспечения), распечатка (для билетов или флаерсов) или собственно доставка (для каких-то физических предметов).

Чтобы перехватить личные данные и, если повезёт, одновременно и денежные средства жертвы, достаточно просто подменить QR-код, который отправлял бы на сфальсифицированную страницу и заставлял покупателя перечислить деньги на подставной счёт. Программ для генерирования такого кода существует множество, в том числе и совершенно бесплатных. В результате злоумышленник может получить практически полный пакет данных: имя и адрес покупателя и номер его платёжной карты.

Более затратный, но, возможно, ещё более эффективный способ мошенничества – это печать и распространение рекламных буклетов, каталогов и прочего маркетингового хлама, распространяемого по почтовым ящикам и просто в разных общественных местах. При этом злоумышленнику

даже не обязательно маскироваться под какой-то известный магазин или торговую сеть: достаточно предложить какие-нибудь сногсшибательные «акции и скидки», и этот примитивнейший приём социальной инженерии сделает своё дело. В остальном же результат всё тот же: вы дарите мошенникам не только деньги, но и номер кредитки и свой адрес.

Для хищения личных данных, используемых вами в Интернете, применяется ещё один способ – кража файлов cookies браузера, в которых хранится самая разнообразная информация о посещённых вами сайтах, включая настройки и данные о сессии, позволяющие не авторизоваться всякий раз при заходе на ресурс. Для этого достаточно просканировать подложный QR-код: он переправит вас на фейковую страницу, которая не будет выглядеть особенно подозрительной и не сделает ничего заметного, а лишь похитит файлы cookies. И если «большие» антивирусы сегодня почти в обязательном порядке проверяют соответствие реального URL тому, что демонстрируется пользователю, упрощённые версии для смартфонов и планшетов могут пропустить подобную подмену.

Перехватив вашу сессию, например, в интернет-магазине, злоумышленник сможет добраться не только до личных данных, но и до сведений о платёжной карте. При этом он, скорее всего, не будет заказывать что-то именно в этом магазине, а воспользуется полученными сведениями для фабрикации карты-двойника или для добывания какой-то более подробной информации о жертве.

Хорошо известен также случай, когда по QR-коду на смартфоны под управлением Android вместо интернет-мессенджера загружался СМС-троян Jimm, рассылавший платные эсэмэски с аппарата жертвы.

Всё это довольно простые и незатейливые способы, но среди взломщиков существуют и настоящие «художники», заставляющие насладиться красотой и элегантностью не только процесса, но даже самой идеи проникновения в систему. В мае 2013 г. появилась информация о том, что специалистам компании по сетевой безопасности Lookout Mobile удалось взломать очки-компьютер Google Glass при помощи QR-кода, а точнее, с помощью так называемых фотобомб, «взрывающихся» при фиксировании очками QR-кодов. Дело в том, что это устройство способно автоматически сканировать любую картинку с целью распознавания объектов, которые могут представлять интерес для владельца.

По уверениям Google, сейчас эта уязвимость устранена, но изначально в QR-кодах, которые используются для настройки очков, можно было зашифровать любые команды, в том числе и позволяющие получить полный удалённый доступ к устройству, незаметный для владельца. Кроме того, ранее можно было «заставить» очки подключиться ко взломанной точке доступа Wi-Fi или устройству с Bluetooth и перехватывать любую информацию, передаваемую как от очков, так и к очкам, – то есть, грубо говоря, можно было показать владельцу сфабрикованную картинку. В настоящее время возможность автоматического подключения к Wi-Fi

заблокирована, и очки Google Glass реагируют на QR-коды лишь в строго определённых режимах.

Как видим, собственно QR-коды не слишком подвержены взлому, поскольку в их спецификации изначально заложена система исправления ошибок на основе кода Рида – Соломона с четырьмя уровнями избыточности от 7 до 30 %, что позволяет, например, считывать даже повреждённый код, код с нанесённым изображением или использовать для этого смартфон с грязным либо поцарапанным объективом.

Однако в подавляющем большинстве случаев взлом самого кода (то есть теоретически возможное, но весьма трудоёмкое изменение каким-то образом оригинальной картинки) и не требуется. Гораздо большую опасность представляют подложные QR-коды, причём особенно уязвимы именно мобильные устройства в связи с самим характером их «полевого» использования.

Поэтому лучшим способом защиты от мошенничества остаётся старое сетевое правило: не открывайте подозрительные ссылки; в нашем случае оно звучит как «не сканируйте подозрительные QR-коды». Гораздо безопаснее приобрести какой-то товар в проверенном онлайновом или офлайновом магазине, чем иметь дело с виртуальными магазинами, расположенными в сомнительных местах, а тем более – рекламными проспектами ***(Как хакеры используют QR-коды для взлома систем // InternetUA (http://internetua.com/kak-hakeri-ispolzuuat-QR-kodi-dlya-vzloma-sistem). – 2014. – 1.04).***

***

Специалисты предупреждают о новой угрозе. Ее источником оказалась хорошо знакомая пользователям Windows программа WinRAR.

Израильский исследователь Д. Коэн сообщил, что обнаружил способ, позволяющий создавать файлы, которые выглядят как rar- или zip-архивы изображений или документов. Однако в действительности такие файлы являются исполняемыми и при открытии осуществляют загрузку опасных зловредов на компьютеры пользователей.

Данные Д. Коэна уже подтвердила компания IntelCrawler, уточнив, что уязвимость присуща всем используемым сегодня версиям WinRAR. Специалисты компании утверждают, что атака с использованием фальшивых архивных файлов началась 24 марта и в настоящее время в числе ее целей оказались несколько предприятий оборонного и аэрокосмического комплекса, дипломатических миссий и крупнейших мировых компаний из списка Fortune Global 500. Это позволяет предположить, что уязвимость WinRAR используется для масштабной кампании кибершпионажа.

Экспертам IntelCrawler удалось идентифицировать один из командных серверов киберпреступников, координирующих атаку. Он располагается в Турции, однако специалисты предполагают, что сервер был взломан и взят под контроль, а потому истинное происхождение кибершпионской кампании

остается пока неизвестным ***(WinRAR приглянулся кибершпионам // InternetUA (http://internetua.com/WinRAR-priglyanulsya-kibershpionam). – 2014. – 1.04).***

***

Пользователи Dropbox обвинили сервис во вмешательстве в личные данные юзеров, сообщает TechCrunch.

29 марта пользователь Twitter написал в своем микроблоге, что Dropbox обнаружил в его личной папке файл, нарушающий антипиратское законодательство. Твит очень быстро распространился и вызвал негодование пользователей по поводу действий Dropbox.

Администрации Dropbox пришлось оправдываться и объяснять, как именно работает антипиратская защита сервиса. Как объяснили представители сервиса, Dropbox не запрещает пользователям загружать и хранить пиратские файлы, если они закрыты для других юзеров. Но если документ становится публичным, то он может быть заблокирован по закону об авторском праве.

«Иногда мы получаем предписания по DMCA (Закон об авторском праве в цифровую эпоху) с требованием удались ссылки по причинам защиты авторских прав. Мы поступаем согласно закону и блокируем обнаруженную ссылку», – сообщила администрация Dropbox после обвинений в нарушении правил приватности.

Администрация сервиса объяснила, что она не просматривает содержание отправленных файлов, а проверяет их хеш-коды на совпадение с кодами документов, внесенных в черный список из-за нарушения антипиратского законодательства.

О принципах работы этого механизма компания объявляла еще в 2012 г., но стало известно, что отправка пиратских файлов конкретным пользователям тоже запрещена.

«У нас есть автоматическая система, которая препятствует тому, чтобы другие пользователи открывали доступ к идентичным файлам по другой ссылке Dropbox. Это делается при помощи сравнения хеш-кодов. Мы не просматриваем файлы в ваших личных папках и заинтересованы в том, чтобы ваши документы были защищены», – сообщили в Dropbox. При этом система не способна обнаружить пиратский файл, если он не был ранее внесен в список. К тому же, если документ был изменен, то он будет восприниматься сервисом как новый, разрешенный файл.

Сервис Dropbox начал работу в 2007 г.. Он является одним из самых популярных облачных хранилищ данных. Пользователи могут не только загружать файлы, но и делиться ими адресно или со всеми остальными пользователями. Dropbox пользуются более 200 млн человек по всему миру ***(Dropbox обвинили в нарушении правил приватности // InternetUA (http://internetua.com/Dropbox-obvinili-v-narushenii-pravil-privatnosti). – 2014. – 31.03).***

***

Хакеры из группировки Russian Cyber Command заявили, что им удалось получить доступ к персональным данным абонентов «Интертелекома». Они выложили в сеть несколько архивов, общим объемом около 2 Гб, в которых, по их словам, содержатся пароли доступа абонентов к сети, копии документов и договоров, IMEI-номера устройств и другие данные украинского провайдера сотовой связи. Всего, по словам хакеров, в архивах содержится информация о 100 тыс. абонентах. «Интертелеком» подтвердил факт утечки информации, но при этом у оператора отметили, что в архивах нет личных данных абонентов, а хакеры, скорее всего, взломали компьютеры региональных дилеров компании, пишет AIN.UA (http://ain.ua/2014/04/01/518108).

По информации AIN.UA, в опубликованных архивах действительно немало различных данных, как имеющих отношение к «Интертелекому», так и нет. Например, там можно найти скан-копии паспортов граждан Украины, договоров на подключение к Интернету, выписок из единого реестра, внутренние инструкции для дилеров «Интертелекома» и много другой информации.

В службе безопасности оператора пояснили, что файлы в формате Excel, которые были опубликованы в Интернете, на самом деле являются инструкцией для подключения абонентов, которая передается каждому официальному дилеру оператора при обучении. А скан-копии первого листа абонентского договора доступны на корпоративном сайте «Интертелекома».

«Все приведенные в скриншотах абонентские номера относятся к нумерации Хмельницкой области. Эти данные могли фиксировать на своем компьютере сотрудники официальных дилеров оператора при подключении новых абонентов», – говорит руководитель службы безопасности «Интертелекома» В. Украинец. По его словам, такие записи могут вести партнеры любой организации, предоставляющие услуги населению, и фиксировать результаты своей работы для дальнейшей сверки с организацией при проведении взаиморасчётов.

В «Интертелекоме» полагают, что хакеры могли получить доступ к файлам, хранящихся на компьютерах дилеров компании с помощью вирусного программного обеспечения. В то же время у оператора заверили, что персональные данные абонентов «Интертелекома» хранятся в базе данных оператора в другом формате, а специальные средства безопасности исключают возможность несанкционированного доступа к ним.

В последние несколько месяцев хакерские группировки регулярно совершают атаки на украинские ресурсы. Недавно антиправительственная организация «КиберБеркут» заблокировала работу информагентств Liga.net и Unian.net, веб-сайта А. Парубия Parubiy.org, западного портала zik.com.ua и ряда других онлайн-ресурсов. На днях те же злоумышленники взломали почтовые ящики региональных отделений партий УДАР и «Батькивщина» и

произвели ряд атак на телефоны украинских политиков и вербовщиков Национальной Гвардии.

Между тем американские и английские эксперты считают, что впридачу к военному вторжению в Крым Россия ведет против Украины кибервойну. По данным чиновников США, Россия уже нанесла серию кибердударов по украинским сетям коммуникаций в рамках кампании по интервенции в Крым ***(Хакеры выложили в Интернет информацию об абонентах «Интертелекома» // AIN.UA (http://ain.ua/2014/04/01/518108). – 2014. – 1.04).***

***

Как следует из сообщения исследователей безопасности из антивирусной компании Sucuri, ими был проведен подробный анализ распространяемых в сети «бесплатных версий» премиум-плагинов для популярной системы управления контентом WordPress.

Как выяснилось, в некоторых случаях созданные сторонними разработчиками дополнения содержат вредоносный код, предназначенный для захвата контроля над атакуемым ресурсом.

При этом приманкой для жертв служит тот факт, что официальный аналог такого дополнения стоит немалых денег. Желая сэкономить на оплате легитимного ПО многие владельцы интернет-сервисов используют их неофициальные аналоги или копии.

Отметим, что на проведение данного исследования экспертов вдохновило обнаружение «абсолютно бесплатного» плагина SEOPressor, который был установлен сразу на нескольких сайтах. Владельцы этих ресурсов обратились в Sucuri с просьбой очистить их от вредоносного ПО.

После установки данного дополнения у злоумышленника появляется возможность удаленно создать учетную запись с правами администратора и получить полный доступ к порталу.

«В случае, если скомпрометированный ресурс специализируется на торговле в сети Интернет, последствия такой атаки могут обойтись значительно дороже покупки легитиного плагина», – предупреждают эксперты ***(Сайты на WordPress взламывают через «бесплатные версии» премиум-плагинов // InternetUA (http://internetua.com/saiti-na-WordPress-vzlamivauat-cserez--besplatnie-versii--premium-plaginov). – 2014. – 2.04).***

***

Как сообщает исследователь безопасности из Securatary М. Личфилд, ему удалось обнаружить критически опасную уязвимость в решении разработчиков eBay, предназначенном для использования теми людьми, которые предпочитают вести собственную торговлю, нежели пользоваться услугами онлайн-аукциона. Речь идет о платформе eBay ProStore.

Указанная брешь, по заверениям М. Личфилда, позволяет удаленному злоумышленнику получить доступ к данным кредитной карты, используемой

для оплаты товаров и услуг на уязвимом ресурсе. В eBay, в свою очередь, подчеркивают, что в настоящее время неисправность устранена.

Согласно отчету исследователя, эта же уязвимость может быть проэксплуатирована с целью раскрытия конфиденциальной информации пользователей атакуемого ресурса. Эти данные включают имя, фамилию и прочую информацию, указанную при регистрации учетной записи.

«Мы могли совершать покупки от чужого имени и за чужой счет или даже создавать подарочные сертификаты», – подчеркивает М. Личфилд ***(Брешь в eBay ProStore позволяет похищать деньги покупателей // InternetUA (http://internetua.com/bresh-v-eBay-ProStore-pozvolyaet-pohisxat-dengi-pokupatelei). – 2014. – 3.04).***

***

Неизвестные хакеры заявляют, что получили доступ к базе данных с именами и почтовыми адресами пользователей Coinbase. База имеет определенную ценность, поскольку Coinbase – это финансовый сервис, цифровой кошелек для биткоинов. Другими словами, некто мог заполучить контактную информацию о значительной части пользователей Bitcoin.

Хакеры частично опубликовали базу на Pastebin. В файле указаны адреса и имена 2042 пользователей (1153 уникальных адреса электронной почты). Как сообщается, полный список гораздо больше.

Вероятно, базу можно выгодно продать, хотя в данном случае называется альтруистическая причина для взлома. «Coinbase передает всю историю ваших транзакций в ФБР, FinCEN и налоговую службу, – пишут анонимы. – Они находятся под подпиской о неразглашении».

Руководство Coinbase опубликовало комментарий в официальном блоге, в котором опровергает факт взлома и утечки базы данных пользователей. Тем не менее, они признают наличие «бага» в системе, который позволяет постороннему лицу получить список пользователей Coinbase. Впрочем, такой же «баг» присутствует во многих других веб-сервисах, которые сообщают каждому встречному, занят или нет аккаунт с определенным адресом электронной почты. Отображение имени и фамилии пользователя с определенным адресом электронной почты – тоже специальная функция Coinbase, реализованная для удобства при отправке денег конкретному адресату.

Руководство Coinbase подчеркивает, что на Pastebin опубликованы адреса и имена менее 0,5 % пользователей, и эту информацию хакеры получили не в результате взлома, а из неких иных источников. Возможно, с других сайтов bitcoin-тематики ***(Опубликованы имена и адреса части пользователей Coinbase // InternetUA (http://internetua.com/opublikovani-imena-i-adresa-csasti-polzovatelei-Coinbase). – 2014. – 3.04).***

***

Неизвестные взломали официальный сайт Координационного совета Севастополя sevispolkom.info, разместив на главной баннер с номером 565, по которому якобы можно узнать ряд вопросов, в том числе как без очереди получить российский паспорт.

Отметим, что номер 565 был выделен мобильными операторами для перечисления средств в поддержку украинской армии – за каждый звонок или смс у абонента со счета списывается 5 грн.

Так, хакеры разместили на сайте Координационного совета Севастополя следующее объявление: «Правительство РФ, специально для жителей Крыма, голосовавших на референдуме за присоединение к России, создан специальный круглосуточный номер 565».

На сайте уточняется, что по этому номеру можно узнать: как получить российский паспорт без очереди, что сделать для повышения пенсии в три раза, как сдать в аренду жилье богатым русским и т. д. Более того, по номеру 565 можно даже задать вопрос Путину, на который он обязуется ответить.

Сторонники присоединения Крыма к РФ также могут бесплатно заказать персональный дизель-генератор на 10кВТ (бензин обещают выдавать бесплатно).

Кроме всего прочего крымчанам предлагается не только звонить, но отправлять SMS. Однако на сайте Севастополя хакеры разместили примечание, что в одном звонке или СМС можно задать только один вопрос.

«Украинские националисты пробуют перехватить и перенаправить звонки в свои спецподразделения, но вы продолжайте звонить, пока вас не соединят с Москвой», – резюмируется на сайте Севастополя ***(Хакеры взломали сайт Севастополя для сбора денег в поддержку украинской армии // proIT (http://proit.com.ua/news/internet/2014/04/03/152312.html). – 2014. – 3.04).***

***

За последние несколько месяцев значительно увеличилось количество DDoS-атак через «DNS-отражение и усиление пакетов». Главной целью таких нападений были уязвимые домашние маршрутизаторы по всему миру. Такие атаки позволяют одновременно использовать десятки Гбит трафика для нарушения корректной работы интернет-провайдеров, предприятий и веб-сайтов в любой точке мира.

В последнем отчете компании Nominum указывается:

1. Более 24 млн маршрутизаторов, подключенных к Интернету, используют открытые DNS, что делает интернет-провайдеров уязвимыми к DDoS-атакам на DNS-серверы.

2. В феврале 2014 г. более 5,3 млн таких маршрутизаторов использовались для генерации трафика для осуществления атак.

3. В январе 2014 г. более 70 % от общего DNS-трафика, который поступал в сеть провайдера, были связаны с DNS-отражением.

4. В настоящее время DNS – наиболее популярный протокол для запуска атак с «отражением и усилением пакетов».

Эксперты отмечают, что DDoS-атаки через «DNS-отражение и усиление пакетов» набирают популярность, потому что они могут нанести жертве колоссальный ущерб. Помимо этого, в рамках подобных атак уязвимые домашние маршрутизаторы маскируют истинную цель нападения и провайдерам тяжело установить конечный пункт назначения и получателя огромного количества усиленного трафика ***(24 млн маршрутизаторов подвергают интернет-провайдеров DDoS-атакам // InternetUA (http://internetua.com/24-mln-marshrutizatorov-podvergauat-internet-provaiderov-DDoS-atakam). – 2014. – 4.04).***

***

Владельцы телефонов Apple, у которых установлена последняя версия операционной системы, рискуют навсегда расстаться со своим аппаратом при краже. Им не поможет даже функция поиска гаджета Find My iPhone, ведь злоумышленники смогут ее отключить и удалить профиль в iCloud даже без знания пароля. В этом им поможет баг, который недавно обнаружили в iOS 7.

Функция поиска телефона Find My iPhone позволяет по сигналу GPS и базовых станций определить местоположение гаджета и помогает вернуть устройство при утере или краже. Ведь чтобы отключить ее, нужно знать пароль к учетной записи Apple ID. Но из-за бага в iOS 7 злоумышленники могут обнулить профиль пользователя в iCloud, в котором также содержится пароль AppleID. После этого они смогут вернуть смартфон в заводское состояние, из-за чего хозяин уже не сможет его найти.

Чтобы удалить профиль iCloud, злоумышленникам достаточно выполнить простую последовательность действий. Сначала им нужно войти в настройки гаджета и выбрать «Удалить аккаунт». Одновременно с этим требуется отключить функцию Find My iPhone. Система попросит ввести пароль AppleID, но если зажать кнопку питания и перезагрузить смартфон, тогда можно будет удалить профиль iCloud без ввода пароля. После этого можно вернуть гаджет к заводским настройкам и привязать его к другой учетной записи.

Apple пока не исправила этот баг в своей ОС, поэтому рекомендуем пока не обновляться до iOS 7. Или, если вы уже выполнили апдейт, внимательней следите за своим мобильным гаджетом, чтобы его не украли ***(В iOS7 обнаружился идеальный для злоумышленников баг // Portaltele.com.ua (http://portaltele.com.ua/news/software/25498--ios7-----.html). – 2014. – 4.04).***

***

Эксперты «Лаборатории Касперского» обнаружили новый в своем подходе к незаконному обогащению троянец Waller – помимо отправки

платных SMS, зловред также пытается украсть деньги с электронного кошелька QIWI.

Попав на телефон пользователя, этот троянец обращается к своему управляющему серверу за командами, выполняя стандартные для таких программ действия: проверка баланса, отправка SMS, установка других вредоносных программых и прочее. Однако помимо этого Waller обладает еще несколькими возможностями, которые позволяют ему опустошать электронный кошелек QIWI, зарегистрированный на номер владельца зараженного смартфона. Получив соответствующую команду, троянец проверяет баланс счета QIWI-Wallet, отправляя SMS на короткий номер. Полученные в ответ сообщения троянец перехватывает и переправляет их злоумышленникам. В случае положительного баланса электронного кошелька троянец может начать переводить деньги со счета пользователя на другой счет QIWI-Wallet, указанный мошенниками. Для этого по команде троянец отправляет на короткий номер соответствующее SMS, в котором указаны номер кошелька злоумышленников и сумма перевода.

Подобные механизмы кражи денег с электронных кошельков дают злоумышленникам широкие возможности воровать деньги у пользователей даже в тех странах, где не действуют премиум-номера, так как платежный сервис QIWI работает на рынках еще семи стран помимо России. В их число входят Румыния, Бразилия, Казахстан, Беларусь, Молдова, Иордания, США, а в 15 других странах сервис представлен по модели франшизы.

«Пользователи, пребывающие в заблуждении, что вредоносные программы если и могут нанести финансовый ущерб, то незначительный, скорее всего, поменяют свою точку зрения после распространения подобных троянцев. В платежной системе QIWI в течение одного дня допускаются переводы общей суммой до 15 тыс. р. – а это серьезный удар по кошельку жертвы. И несмотря на то что Waller пока не очень популярен, в последнее время злоумышленники все активнее пытаются заражать мобильные устройства пользователей этим троянцем. Мы в очередной раз порекомендуем не включать на мобильных устройствах “Режим разработчика” и запретить возможность установки приложений из сторонних источников. Однако, если учесть, что способы кражи денег киберпреступниками становятся все более изощренными, единственной надежным средством защиты является установка защитного ПО», – отметил Р. Унучек, антивирусный эксперт «Лаборатории Касперского».

Троянец распространяется с сайтов злоумышленников под видом различных приложений, среди них – android universalnaya proshivka, media player classic dlya android, golosomenyalka na android. Кроме того, ссылки на Waller встречаются в SMS-спаме ***(Троянец Waller ворует деньги с Qiwi-кошельков // InternetUA (http://internetua.com/troyanec-Waller-voruet-dengi-s-Qiwi-koshelkov). – 2014. – 4.04).***

***

Немецкие правоохранители сообщили о проведении расследования по поводу похищения данных 18 млн пользователей сервисов электронной почты, которое стало самым масштабным за всю историю Германии. Так, прокуратура Вердена (Нижняя Саксония, Германия) устанавливает, каким образом злоумышленники получили доступ к пользовательской информации.

Жертвами хищения стали все клиенты всех провайдеров страны. Тем не менее, непонятно, почему все 18 млн учетных записей приписываются именно немецким пользователям, если некоторые из адресов находятся в домене .com, который является международным.

Стоит отметить, что за последние несколько месяцев это уже второе масштабное похищение данных пользователей. В январе нынешнего года эксперты по безопасности сообщали о том, что хакеры получили доступ к 16 млн учетных записей в сервисах электронной почты. Есть предпосылки считать, что эти два случая связаны между собой.

Прокуратура Вердена пока не сообщила, какое количество аккаунтов принадлежит пользователям из Германии ***(В Германии расследуется самый масштабный случай похищения пользовательских данных // InternetUA (http://internetua.com/v-germanii-rassleduetsya-samii-masshtabnii-slucsai-pohisxeniya-polzovatelskih-dannih). – 2014. – 5.04).***