СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(22.04–3.05)

2014 № 9

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(22.04–3.05)
№ 9

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 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 11
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 13
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 25
Інформаційно-психологічний вплив мережевого спілкування на особистість 25
Маніпулятивні технології 26
Зарубіжні спецслужби і технології «соціального контролю» 30
Проблема захисту даних. DDOS та вірусні атаки 36

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Аналитическая компания Shareholic представила отчёт по реферальному трафику восьми крупнейших социальных медиа за I квартал 2014 г.

Facebook, Pinterest, Twitter, StumbleUpon, Reddit и Google+ с начала года увеличили количество реферального трафика, в то время как у YouTube и Linkedin значение этого показателя ушло в минус.

Для исследования Shareholic отслеживала данные 400 млн пользователей. В сравнении с данными за 2013 г. реферальный трафик значительно возрос только у Facebook и Pinterest.

За I квартал 2014 г. процент реферальных переходов Facebook возрос с 15,44 % до 21,25 % (то есть на 37 %). Этот же показатель у Pinterest увеличился с 4,79 % до 7,1 % (на 48,36 %), в то время как у Twitter лишь на 1,59 % (с 1,12 % до 1,14 %). Другими словами, количество реферального трафика у Facebook и Pinterest растёт хорошими темпами, а у Twitter почти не меняется.

Изменения показателя у других представленных в исследовании сайтов хоть и велики в процентной составляющей, всё же малы в абсолютном выражении.

Половину реферального трафика Facebook получает от мобильных пользователей.

С конца 2013 г. Facebook намеренно начал снижать органический охват постов, изменив алгоритм сортировки ленты, чтобы администраторы страниц больше денег вкладывали в их продвижение. Социальная сеть уверяет, что это делается из-за того, что количество контента постоянно растёт, а места в ленте пользователей больше не становится, поэтому отдавать его нужно лучшим. Или тем, кто готов заплатить ***(С начала года Facebook стал раздавать на 37 % больше трафика // InternetUA (http://internetua.com/s-nacsala-goda-Facebook-stal-razdavat-na-37--bolshe-trafika). – 2014. – 22.04).***

***

Найбільша професійна соціальна мережа у світі LinkedIn повідомила про те, що загальна кількість її користувачів перевищила 300 млн осіб, пише Корреспондент.net (http://ua.korrespondent.net/world/3352319-chyslo-korystuvachiv-sotsmerezhi-LinkedIn-perevyschylo-300-mln-osib).

З початку поточного року кількість користувачів мережі збільшилася більш ніж на 23 млн осіб.

Число американських користувачів соцмережі також встановило рекорд, перевищивши позначку в 100 млн. Проте більшість користувачів – близько 67 % – перебувають за межами США. Наразі членами соцмережі є мешканці більше 200 країн.

Офіційний запуск сайту LinkedIn був здійснений 5 травня 2003 р. Соцмережа наразі підтримує 22 мови, у тому числі російську. Штат компанії перевищує 5 тис. співробітників, які працюють у 27 містах по всьому світу.

Користувачі LinkedIn шукають на сайті вакансії, наймають співробітників, звертаються за консультаціями до провідних галузевих експертів. Особисті сторінки можна створювати безкоштовно, але з 2005 р. соцмережа ввела платну підписку, яка забезпечує більше можливостей для пошуку кандидатів і професійного спілкування. Платна підписка забезпечує близько 70 % виручки компанії ***(Число користувачів соцмережі LinkedIn перевищило 300 млн осіб // Корреспондент.net (http://ua.korrespondent.net/world/3352319-chyslo-korystuvachiv-sotsmerezhi-LinkedIn-perevyschylo-300-mln-osib). – 2014. – 21.04).***

***

Twitter офіційно запустив оновлений інтерфейс профілів для користувачів у всьому світі. Twitter став схожим на соціальну мережу.

У результаті оновлення користувачі отримали можливість розміщувати великі за розміром фотографії (400x400 пікселів), новий допустимий розмір обкладинки тепер становить 1500x1500 пікселів.

Відтепер окремо відзначені твіти, які отримали найвищий рівень взаємодії, – ретвіти, відповіді та додаваня в улюблені. Такі твіти будуть мати більший шрифт і виділятись на фоні інших.

З'явилася можливість прикріпляти вгорі один із твітів. Аналогічна функція є для сторінок у Facebook.

Також нині можна обирати, який саме таймлайн бачити при потраплянні на профіль користувача – усі твіти (у т. ч. ретвіти), твіти з фото та відео, лише твіти та відповіді.

Щоб ввімкнути новий дизайн, необхідно скористатися цим посиланням: https://twitter.com/i/new_profile?ref=page ***(Новий дизайн Твітера став доступним для всіх користувачів // UkrainianWatcher (http://watcher.com.ua/2014/04/23/novyy-dyzayn-tvitera-stav-dostupnym-dlya-vsih-korystuvachiv/). – 2014. – 23.04).***

***

Крупнейшая в мире соцсеть Facebook анонсировала сервис FB Newswire, с помощью которого журналисты и медиаресурсы смогут отслеживать потенциально интересные им новости, которые публикуются и обсуждаются пользователями соцсети. Об этом говорится в сообщении Facebook.

Сервис по сути представляет собой новостной агрегатор, объединяющий материалы из сообщений пользователей соцсети.

Сервис доступен в виде сообщества на Facebook, а также в формате Twitter-аккаунта @FBNewswire. Новостные истории могут включать в себя фотографии, видеоролики, обновления статуса, цитаты из СМИ, ссылки на

веб-сайты. Кроме того, для каждой новости публикуются хэштеги, по которым можно отследить ее обсуждение, и контактное лицо, с которым можно связаться для получения дополнительной информации.

Новости для публикации на страничке сообщества отбираются и оформляются особой командой редакторов компании Storyful, чья технология используется в сервисе.

Среди таких новостей могут быть новые технологии, анонсированные в аккаунте компании в той или иной соцсети, сенсационные заявления знаменитостей, результаты спортивных матчей и вирусные видеоролики.

«Каждый день на Facebook появляются новости. Более миллиарда человек используют платформу, чтобы узнавать, изучать и принимать участие в значимых событиях по всему миру. FB Newswire агрегирует потенциально интересный новостной контент, который размещается на Facebook пользователями и организациями в публичном доступе», – пишет директор по медиапартнерствам Facebook Э. Митчелл.

Отслеживание новостного контента в социальных сетях стало привычной практикой для СМИ. Некоторые ньюсмейкеры выбирают онлайн-сервисы для заявления своей позиции по тем или иным вопросам, а также в соцсетях можно узнать о событиях от их непосредственных участников и свидетелей.

Это уже не первый сервис, который Facebook запускает для отслеживания новостей и интересных публичных дискуссий в соцсети. В январе этого года Facebook запустила блок публикации трендов, где размещаются наиболее обсуждаемые среди пользователей темы. Кроме того, в прошлом году соцсеть запустила кликабельные хэштеги, по которым можно обнаружить публикации, объединенные одной темой или событием ***(Facebook создала новостной агрегатор материалов пользователей соцсети // InternetUA (http://internetua.com/Facebook-sozdala-novostnoi-agregator-materialov-polzovatelei-socseti). – 2014. – 24.04).***

***

Facebook является лидером рефереального трафика, поступающего на сайты из социальных сетей и сервисов. Об этом свидетельствуют результаты исследования, проведённого платформой социальной аналитики Shareaholic. В ходе эксперимента была изучена статистика более чем 300 тыс. сайтов, месячная аудитория которых превышает 400 млн уникальных пользователей.

Цель эксперимента – выяснить, какой процент трафика поступает на сайты из восьми наиболее популярных социальных медиа.

В I квартале 2014 г. процент реферального трафика (переходов из социальных медиа, на которых размещается ссылка на страницу сайта), поступающего из Facebook, в общей доле трафика увеличился на 37,6 % в сравнении с Q4 2013 г. Только в марте текущего года доля реферального трафика на сайты из Facebook составила 21,25 % в общем объёме.

Следом за крупнейшей в мире социальной сетью с большим отрывом идет сервис увлечений Pinterest. Несмотря на то что в I квартале 2014 г. процент реферального трафика на сайты из Pinterest возрос на 48,4 %, доля переходов из социального сервиса на сайты в общем объёме составила 7,1 %.

Завершает тройку лидеров Twitter с долей переходов на сайты в 1,14 %. Важно отметить, что в минувшем квартале сервису микроблогов так и не удалось продемонстрировать значимого роста реферального трафика. Увеличение составило всего 1,6 %.

Социальные сервисы YouTube и Linkedin в I квартале 2014 г. показали отрицательную динамику. Процент реферального трафика на сайты из видеохостинга упал на 52,4 %, а из сообщества профессионалов – на 20, 8 %.

Также напомним, что в IV квартале 2013 г., по данным Shareaholic, социальный трафик на сайты из Facebook, Pinterest и StumbleUpon увеличился в среднем на 30 % ***(Исследование: около четверти реферального трафика соцмедиа поступает на сайты из Facebook // ProstoWeb (http://www.prostoweb.com.ua/). – 2014. – 25.04).***

***

Соцсеть «Одноклассники» внедрила сервис геолокации, позволяющий определять местонахождение пользователя. Об этом «Ленте.ру» сообщил пресс-секретарь соцсети И. Грабовский.

Как показало тестирование «Ленты.ру», отметку о месторасположении можно сделать вручную при написании поста в соцсети. Ресурс также стал запрашивать разрешение на определение местонахождения. При согласии пользователя его расположение определяется автоматически.

«Пользователи могут самостоятельно добавлять в базу данных геометок различные места: рестораны, офисы и т. д.», – прокомментировал И. Грабовский.

Сервис геолокации, по сообщению соцсети, основан на базе данных Open Street Maps, визуализация карт реализована с помощью «Яндекс.Карт».

В настоящее время возможность отмечать местоположение есть только в веб-версии «Одноклассников», но сделанные отметки отображаются и на мобильных устройствах. В ближайшее время сервис, по планам соцсети, будет внедрен в мобильной версии и приложениях.

Сегодня сервисы геолокации действуют в основных крупных соцсетях: «ВКонтакте», Facebook и Twitter ***(«Одноклассники» стали определять месторасположение пользователя // InternetUA (http://internetua.com/odnoklassniki--stali-opredelyat-mestoraspolojenie-polzovatelya). – 2014. – 25.04).***

***

Социальная сеть Google+ перестанет существовать как отдельный продукт, пишет портал TechCranch со ссылкой на собственные источники в

корпорации Google. При этом официальный представитель Google опроверг порталу данную информацию.

По словам двух источников издания, Google в настоящее время активно перестраивает кадровый состав, ранее занятый в развитии социальной сети, а также сервисов Hangouts и Photos. Речь идет более чем о тысячи работниках. На территории кампуса интернет-корпорации построен новый корпус, в который осуществляется переезд части команды работников социальной сети.

«Сегодняшняя новость (об уходе В. Гундотра с поста главы Google+. – Ред.) никак не повлияет на стратегию Google+. У нас есть талантливая команда, которая продолжит развивать сервисы Google+, Hangouts и Photos», – заявил TechCranch официальный представитель Google.

В рамках трансформации часть команды, занимавшейся развитием сервисов Google+, Hangouts и Photos, перейдет в подразделение Android.

Переход части команды Google+ в мобильное подразделение корпорации означает концентрацию Google на разработке мобильных решений, «виджетов», которые, по мнению руководства, окажутся более эффективными для компании, нежели разработка собственной социальной сети.

В. Гундотра, возглавлявший Google+, покидает свой пост после почти восьми лет работы в компании. В. Гундотра выступал за сохранение Google+ как отдельной платформы. В настоящее время соцсеть насчитывает около 29 млн пользователей ***(Социальная сеть Google+ прекратит свое существование // Marketing Media Review (http://mmr.ua/news/id/socialnaja-set-google-prekratit-svoe-suschestvovanie-39478/). – 2014. – 28.04).***

***

Компания Mail.Ru Group совместно с правообладателями запустит сервис бесплатного просмотра фильмов в соцсети «Мой Мир» по воскресеньям. Об этом «Ленте.ру» сообщили в компании.

В результате запуска сервиса «Воскресный кинотеатр» в этой соцсети впервые появится постоянная функция просмотра легальных копий фильмов.

В пресс-службе Mail.Ru сообщили «Ленте.ру», что новые фильмы будут появляться на платформе «Мой Мир» в полночь, начать просмотр фильма можно в любое время в течение всего воскресенья. Если пользователь начал смотреть фильм, например, в 23.30, то он может спокойно досмотреть картину, в полночь отключится лишь возможность начать просмотр.

В соцсети «Мой Мир» до сих пор поддерживался сервис с пользовательскими видеороликами «Видео@Mail.Ru», а легальные фильмы и сериалы можно смотреть в рамках сервиса «Афиша@Mail.Ru».

Ранее «Мой Мир» провела разовый эксперимент с размещением в соцсети авторского фильма П. Руминова «Я буду рядом» – за 48 часов фильм набрал 67 тыс. просмотров.

Работа «Воскресного кинотеатра» начнется 9 мая с показа военной драмы Ф. Бондарчука «Сталинград» ***(Соцсеть «Мой Мир» запустит бесплатный кінотеатр // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/39185/126/lang,ru/). – 2014. – 28.04).***

***

Социальная сеть «ВКонтакте» в течение месяца подпишет меморандум Роскомнадзора о легализации контента. Об этом «Известиям» рассказал источник в федеральной службе. Правообладатели связывают перемену в отношении руководства соцсети к пиратскому контенту с тем, что П. Дуров покинул пост ее генерального директора.

В декабре 2013 г. администрация «ВКонтакте» отказалась присоединиться к соглашению. «Пока не будем подписывать, мы не согласны с рядом пунктов», – заявлял «Известиям» И. Перекопский, которой в то время был вице-президентом «ВКонтакте». Однако, по словам источника в Роскомнадзоре, в настоящее время ситуация изменилась, и «ВКонтакте» подпишет меморандум. Пресс-службы «ВКонтакте» и Роскомнадзора от комментариев отказались.

В декабре 2013 г. представители 36 интернет-площадок и фирм-правообладателей договорились о сотрудничестве. Подготовленный Роскомнадзором и правообладателями меморандум предусматривает, что подписавшие его компании будут совместными усилиями пресекать распространение пиратских фильмов. Это позволит снизить нагрузку на суды. Подписавшие документ стороны обязуются содействовать доступу пользователей к легальным фильмам. Согласно меморандуму, администрация сайта в течение суток заблокирует размещенный пользователем пиратский фильм, если в жалобе точно указан адрес страницы. Если же правообладатель указал только адрес сайта, пиратский контент заблокируют «в разумное время». При этом представители интернет-площадок изучат возможности внедрения на своих ресурсах систем идентификации контента, позволяющих автоматически запретить повторное появление фильмов.

На сегодняшний день документ подписали ВГТРК, «Амедиа», «Мосфильм», «Каро Премьер», «ТНТ-Телесеть», интернет-компании Mail.Ru Group (владелец соцсетей «Одноклассники» и «Мой Мир»), RuTube, Ivi, Zoomby, Megogo и др. При этом, помимо «ВКонтакте», пока не присоединились к соглашению «Яндекс» и Google (которой принадлежит сервис YouTube). «Мы не подписали документ, поскольку при его подготовке не были учтены важные для интернет-компаний пункты: обязательность указания адреса страницы в обращениях правообладателей, недопустимость премодерации и т. д.», – сообщили в пресс-службе «Яндекса» ***(«ВКонтакте» подпишет антипиратский меморандум //***

InternetUA (http://internetua.com/vkontakte--podpishet-antipiratskii-memorandum). – 2014. – 29.04).

***

Спустя несколько недель после того как Facebook объявила, что messenger-функционал больше не встроен в мобильный клиент, компания обновила отдельное мобильное приложение Facebook Messenger, добавив в него ряд новых опций, а также возможность значительно более быстрой отправки медиа-файлов, в частности фото и видео. Кроме того, Facebook Messenger теперь получил возможность прямого получения мобильных фото и видео с камеры устройства.

Впрочем, у Facebook Messenger есть одна пользовательская недоработка – приложение почти мгновенно отправляет фото и видео, не оставляя пользователю возможности предпросмотра отправляемого материала, сразу передавая его получателю. Значительная часть остальных мессенджеров, в частности WhatsApp, Viber, Snapchat и другие, предлагают предпросмотр перед отправкой.

Среди остальных новшеств новый Messenger включает в себя улучшенный поиск, возможность скачивания стикер-паков и ряд функциональных улучшений. Новый Facebook Meggenger пока доступен только для iOS, однако в Facebook говорят, что новинка в ближайшее время появится и в Android-версии ***(Facebook выпустила обновленный Messenger // InternetUA (http://internetua.com/Facebook-vipustila-obnovlennii-Messenger). – 2014. – 29.04).***

***

Приложение для платформы iOS Secret запустилось в Великобритании, Ирландии, Австралии и Новой Зеландии. Об этом сообщило издание The next web.

Приложение Secret было создано и развивалось в США. По сути, оно является анонимной соцсетью, которая позволяет общаться с другими пользователями, подписываясь придуманными псевдонимами (никнеймами) или вообще без подписи. При этом с помощью адресной базы соцсети получатель сообщения может понять, знает ли он его автора, или анонимка пришла от знакомых его друзей.

В проекте говорят о значительном росте числа пользователей, не раскрывая конкретных цифр. Версия Secret для Android в настоящее время, по данным издания, тестируется и будет запущена в скором времени ***(Анонимная соцсеть Secret вышла за пределы США // InternetUA (http://internetua.com/anonimnaya-socset-Secret-vishla-za-predeli-ssha). – 2014. – 30.04).***

***

Сервис Twitter, похоже, собирается развивать между пользователям приватные обсуждения. Об этом в интервью Bloomberg сообщил исполнительный директор Twitter Д. Костоло.

Предполагается, что так называемый whisper mode («режим шепота») позволит пользователям легко делать приватными публичные беседы, не предпринимая каких-либо сложных действий. Вообще, Twitter был задуман как публичный сервис, что означает то, что публикуемый контент по умолчанию становится доступен и другим пользователям.

В то же время сервис предлагает и систему прямых сообщений (DM), но она не совершенная. Новая функция whisper mode должна стать чем-то вроде многопользовательской системы прямых сообщений. Тем не менее, как именно будет реализована новая «фича», пока не сообщается, и пользователям Twitter остается лишь строить собственные догадки ***(Twitter предложит «режим шепота» // ProTV.UA (http://protv.ua/news/internet/twitter_predlojit_rejim_shepota_/). – 2014. – 3.05).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Оказывается точно также как профессиональные дипломаты или министры, ведущие переговоры на государственном уровне, обычные граждане могут конструктивно общаться между собой на важнейшие общественные темы. Подтвердил выше изложенные выводы «Проект гражданской дипломатии», стартовавший в социальной сети в начале марта. Инициаторы решили на этом не останавливаться и провести 18 апреля круглый стол под названием «Роль гражданской дипломатии в поддержании общественной стабильности и согласия», который был в помещении Информационно-ресурсного центра.

И. Черный, который является основателем Центра гражданской дипломатии, сказал, что провести круглый стол является гражданской инициативой. В настоящее время всех волнуют некоторые проблемы общества и поэтому все участники решили мотивировать других людей для совершения определенных действий в решении этих проблем. Лично И. Черный заходит в известную социальную сеть «ВКонтакте», выбирает страну, город, возраст целевой аудитории и просто добавляет людей в свои друзья, а после общение. После этого следует сосредоточить внимание на особенностях. Потому что очень интересно общаться тогда, когда есть какие-либо разногласия. Самое первое – человек выражает свое мнение. Второе – он должен понять убеждения другой стороны. Третье – необходимо согласовывать позиции с собеседником посредством отказа от неважных ее составляющих и акцентированию внимания на действительно важных вещах.

Благодаря такому общению получается, что в «Проекте гражданской дипломатии» находятся люди из самых разных уголков Украины, России, Беларуси, Польши и они все находят много общего. А общее это можно увидеть в жизненных позициях, в мнениях, в действиях, в стремлениях и все они получают объективную информацию о тех противоречивых событиях, которые разворачиваются сегодня в мире.

Для того чтобы пообщаться вживую, привлечь к проекту совершенно новых активных людей организовали «круглый» стол с гражданской дипломатией. Лозунг мероприятия звучал так: «Вместе мы можем создать сильное и счастливое общество, необходимо просто договориться между собой». Важно отметить, что среди участников присутствовали и предприниматели, и юристы, и историки, и веб-дизайнеры и т. п.

…Таким образом, новый совершенно непохожий на другие проект под названием «Проект гражданской дипломатии» является чем-то манящим и весьма перспективным в развитии. Сейчас украинцы хотят сплотиться, но не полностью понимают друг друга из-за того, что видят информационную войну, поэтому пообщаться поближе, и даже во время встречи очень удобно полезно и необходимо. Данный проект способен научить человека выслушивать чужое мнение, понимать, что оно имеет право жить, и искать пути соприкосновения и согласования. Только после прохождения очередных этапов кировоградец/любой украинец может овладеть настоящими основами дипломатии и стать соответственно дипломатом. Нужно только желание и время для общения ***(Кировоградцы становятся настоящими дипломатами в социальных сетях // Городской портал Кировограда (http://kr.ua/news/news/1355/). – 2014. – 23.04).***

***

Ідентифіковані профілі в соцмережах озброєних сепаратистів, що захопили адмінбудівлі в Слов'янську. Про це на своїй сторінці у Facebook написав активіст Євромайдану О. Уманець.

«Завдяки допомозі блогерів ідентифіковані дані злочинців, що захопили Слов'янськ. Як з'ясувалося багато хто з них мають профілі в соцмережах і навіть ведуть там активне життя», – написав активіст і оприлюднив посилання:

Александр Ганичев http://vk.com/spets80

Евгений Пономарев http://vk.com/dingo31

Игорь Георгиевский http://vk.com/garry_san

Сергей Анастасов http://vk.com/anastasovserg

Тихон Каретный http://vk.com/id243374106

Евген Злой http://vk.com/id229685502 ***(В соцмережах поширюють контакти слов'янських терористів // Espreso.tv (http://espreso.tv/news/2014/04/23/v_socmerezhakh_poshyryuyut_kontakty_slovyanskykh_terorystiv). – 2014. – 23.04).***

Согласно документации по продажам, пишет Ad Age, социальная сеть предлагает своим крупнейшим рекламодателям сегмент пользователей, выразивших интерес к чемпионату мира по футболу, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-vpervye-predlozhit-reklamodateljam-auditoriju-pod-televizionnoe-sobytie-39399/).

Впервые Facebook построил сегмент аудитории под крупное телевизионное событие, но если тестовый запуск пройдет хорошо, то данный вид рекламы распространится на Олимпийские игры, Суперкубок и церемонию Оскара, сообщает лицо, знакомое с планами Facebook.

В настоящее время маркетологи могут таргетировать рекламу по таким интересам, как «футбол» или даже «чемпионат мира по футболу» (сегмент содержит почти 45 млн человек, согласно данным сервиса объявлений Facebook). Отличие нового тестового сегмента в том, что он будет обновляться ежедневно, чтобы включать людей, которые не обязательно являются преданными поклонниками футбола, но оказались затронуты волной чемпионата и стали публиковать статусы или ссылки на истории, связанные с турниром.

Facebook стремится продемонстрировать рекламодателям, как социальная активность телевидения работает на практике. Для начала социальная сеть в январе сотрудничала с компанией SecondSync, чтобы оценить шумиху вокруг ТВ, которая разворачивалось в большей части аккаунтов на Facebook, где пользователи включили настройки конфиденциальности, но Twitter впоследствии купил эту компанию.

Размер сегмента не раскрывается, но у него есть огромный потенциал. Глобальная аудитория чемпионата мира превышает базу пользователей Facebook: согласно исследованию FIFA, более 3,2 млрд человек смотрели прямую трансляцию турнира в течение, по крайней мере, минуты в 2010 г. У Facebook, по состоянию на конец прошлого года, было 1,23 млрд ежемесячных пользователей.

В документации Facebook не встречается упоминание полного названия чемпионата мира, так как FIFA известна стремлением защитить свою интеллектуальную собственность, и использование имени турнира компаниями, не являющимися спонсорами, запрещено.

Сегмент «глобальной футбольной аудитории» станет доступным в конце мая перед турниром, который пройдет в Бразилии в июне и июле 2014 г. Помимо всего прочего, к нему можно будет применить и демографический принцип таргетирования ***(Facebook впервые предложит рекламодателям аудиторию под телевизионное событие // Marketing Media Review (http://mmr.ua/news/id/facebook-vpervye-predlozhit-reklamodateljam-auditoriju-pod-televizionnoe-sobytie-39399/). – 2014. – 22.04).***

***

Издание ЦП не один раз рассматривал тему снижения органического охвата постов на Facebook – и это на фоне последней статистики о том, насколько сильно возрос реферальный трафик, отдаваемый этой соцсетью. Создатели страниц на Facebook оказались серьёзно обеспокоены: всё шло к тому, что единственный способ увеличить охват постов – заплатить за раскрутку записей.

С. Матиста из компании Pagemodo размышляет о том, к чему это ведёт. Платное продвижение определённо увеличит охват постов и даст преимущество перед теми конкурентами, которые пока не торопятся платить. Но это не значит, что у тех, чей бюджет сильно ограничен, нет шансов. Если взглянуть на ситуацию объективно, то общие правила ведения страницы не меняются; меняются лишь количество людей, которые видят эти посты.

В том случае, если количество просмотров записей по умолчанию снижается, нужно как можно больше вовлекать тех людей, которые всё-таки продолжают видеть ваши записи. Гораздо выгоднее иметь сотню пользователей, которые совершают какие-то действия на странице, чем десять тысяч «мёртвых душ», которые, может быть, и читают, но при этом ничего не делают.

Создание грамотной стратегии и контента может помочь повысить охват, не заплатив ни копейки (хотя если несколько свободных копеек имеется в наличии, то лучше их потратить на раскрутку поста).

Приёмы, которые С. Матиста приводит в своём посте:

1. Повысьте качество контента. Если вы хотите, чтобы больше людей увидело ваш пост, нужно сделать так, чтобы его друзьям захотелось его расшарить. Эксперт М. Хайат предлагает внедрять следующие вещи:

Мощные заголовки – списки, провокационные вопросы, лайфхаки;

Релевантные и приемлемые изображения – никаких картинок из фотобанков или приевшихся фотографий;

Контент, которым легко поделиться – социальные кнопки на страницах сайта, призывы к действию и т. п.

2. Следите за трендами. Когда в Facebook появился блок Trending Topics, администраторам и маркетологам стало гораздо проще следить за тем, что люди обсуждают прямо сейчас. Если в этом списке нет того, что может подойти вашей аудитории, следите за обновлениями через Feedly, Google Alerts или Flipboard – если грамотно настроить список источников и ключевых слов, можно быстро и точно ловить популярные именно сейчас темы. Именно их ваши подписчики будут лайкать, комментировать и репостить особенно усердно.

3. Отвечайте подписчикам. Система EdgeRank внимательно следит за взаимодействием между подписчиками и страницей, которое определяет параметр Affinity Score. Чем больше вы общаетесь с подписчиками, тем более релевантной и активной выглядит страница в глазах алгоритма.

Соответственно, её посты будут чаще попадать в ленту новостей. Именно поэтому с подписчиками нужно общаться в комментариях.

4. Отмечайте другие бренды в постах. Недавно на Facebook появилась функция, позволяющая отмечать бренды на страницах других компаний. Так можно попытаться достучаться до подписчиков другой страницы, просто упомянув её у себя. Безусловно, не стоит с этим переусердствовать – для каждого такого упоминания должна быть подходящая ситуация и/или причина.

5. Продвигайте посты выборочно. Как утверждалось выше, все эти приёмы помогут увеличить органический охват, но нет ничего зазорного в том, чтобы немного приплатить. Особенно в тех случаях, когда пост на самом деле может зацепить подавляющее большинство читателей. Одним из самых популярных среди подписчиков типов контента являются конкурсы, так что если вы хотите проверить работу системы проплаченных постов, попробуйте организовать некое состязание.

Да, это раздражает, но Facebook – не благотворительная организация и не школьный проект. Компании необходимо что-то зарабатывать, чтобы развиваться. И поскольку многие администраторы страниц и маркетологи начали разочаровываться в Facebook, самое время взять всё в свои руки и сделать рывок, пока конкуренты не понимают, что происходит ***(5 приёмов ведения страницы в Facebook: как победить снижение органического охвата // Marketing Media Review (http://mmr.ua/news/id/5-priemov-vedenija-stranicy-v-facebook-kak-pobedit-snizhenie-organicheskogo-ohvata-39396/). – 2014. – 22.04).***

***

Нью-йоркський департамент поліції (The New York City Police Department) 22 квітня попросив людей публікувати у Twitter фотографії з поліцейськими із хештегом #myNYPD. Відповідь громадян виявилася неочікувано негативною, повідомляє CNN.

Користувачі Twitter почали завантажувати під хештегом #myNYPD фото, що демонструють жорстокість та негідну поведінку поліції.

На запитання щодо кампанії представниця нью-йоркської поліції почала її захищати: «NYPD створює нові шляхи ефективної комунікації з громадою. Twitter забезпечує відкриту платфому для нецензурованого обміну думками. Цей відкритий діалог на користь нашому місту».

Серед учасників кампанії були і такі, які захищали поліцію, нагадували про те, що «є багато хороших копів».

CNN зауважує, що це не перший випадок провалу рекламної кампанії у соцмережах. 2012 р. McDonald’s створив хештеш #McDstories і поросив споживачів ділитися найкращими спогадами про їхній заклад. Через кілька годин кампанію зупинили через жахливі історії користувачів про отруєння їжею, а також нігті та комах ***(Twitter-кампанія на підтримку поліції Нью-Йорка переросла в акцію протесту // Громадська організація***

«Телекритика» (http://osvita.mediasapiens.ua/material/29897). – 2014. – 23.04).

***

Чистий прибуток компанії Facebook Inc. в I кварталі 2014 р. зріс у 2,9 рази – до 642 млн дол., порівняно з 219 млн дол. роком раніше. Про це йдеться в опублікованому квартальному звіті компанії, повідомляє Корреспондент.net (http://ua.korrespondent.net/business/financial/3353666-chystyi-prybutok-Facebook-v-I-kvartali-2014-zbilshylasia-vtrychi).

Виторг Facebook Inc. в I кварталі зріс в 1,7 раза. Показник становив 2,502 млрд дол. (роком раніше – 1,458 млрд дол.). Доходи від реклами збільшилися на 82 % і досягли показника 2274 млрд дол. ***(Чистий прибуток Facebook в I кварталі 2014 збільшилася втричі // Корреспондент.net (http://ua.korrespondent.net/business/financial/3353666-chystyi-prybutok-Facebook-v-I-kvartali-2014-zbilshylasia-vtrychi). – 2014. – 24.04).***

***

Убытки «ВКонтакте» за 2013 г. снизились на 35 % и составили 137 млн р., сообщается в отчете Mail.ru Group за I квартал 2014 г. и итоги 2013 г.

Общая выручка соцсети в 2013 г. возросла на 14,6 % и составила 3,825 млрд р. Значительную часть доходов компании принес запуск новых рекламных продуктов. В 2013 г. «ВКонтакте» запустила биржу рекламы для сообществ. До этого владельцы пабликов не платили соцсети никаких отчислений с доходов от рекламы.

Mail.Ru Group является основным акционером соцети. В марте компания приобрела 12 % «ВКонтакте» и увеличила свою долю до 52 %. В соответствии этим убытки соцсети за 2013 г. обошлись Mail.ru в 55 млн р. ***(«ВКонтакте» отчитался об убытках // InternetUA (http://internetua.com/vkontakte--otcsitalsya-ob-ubitkah). – 2014. – 24.04).***

***

Сеть микроблоггинга Twitter замедляет рост пользовательской базы и пока не может наладить бизнес-модель, которая бы позволила этой компании получать стабильные доходы от своей деятельности. Такие выводы следуют из опубликованного 1 мая компанией квартального отчета.

Twitter заявила, что количество ее участников в I квартале достигло 255 млн, что на 25 % больше, чем годом ранее. Фактический темп роста говорит о замедлении регистраций, так как ранее Twitter не показывала результатов прироста ниже 30 % за год. На фоне этой статистики бумаги компании просели на торгах на 11 %, даже несмотря на то что компания более чем удвоила продажи, доведя их квартальный уровень до 250 млн дол.

Аналитики говорят, что в настоящее время Twitter уже точно не дорастет до масштабов Facebook, а вдобавок к этому Twitter получает множество новоиспеченных конкурентов, таких как Snapchat, которые

понемногу оттягивают аудиторию. После публикации квартальных данных акции Twitter упали в цене до уровня 37,79 дол., что стало минимальным ценовым уровнем с момента размещения компании на бирже.

М. Гупта, финансовый директор Twitter, в рамках пресс-конференции сообщил, что компания пока не планирует проводить вторичную продажу акций на открытом рынке.

В отчетном квартале компания расширила убыток до 132,4 млн дол. или 23 центов на акцию, против 27 млн дол. или 21 цента на акцию годом ранее. Без учета операционных статей расхода Twitter получила убыток в 3 цента на акцию. В отчете компании также сказано, что компания за I квартал обработала более 157 млрд просмотров, что на 15 % больше показателей годом ранее.

Гендиректор Twitter Д. Костоло говорит, что он сейчас занят подстройкой компании под меняющиеся требования рынка и ориентирован на возвращение роста пользовательской базы. Он также отметил, что компания будет добиваться роста пользовательской базы, главным образом, на промышленно-развитых рынках, главным образом, в Европе и США.

В текущем квартале компания ожидает выручку в 270–280 млн дол., тогда как по итогам года этот показатель ожидается на уровне 1,2–1,25 млрд дол. ***(Twitter вновь в убытках // InternetUA (http://internetua.com/Twitter-vnov-v-ubitkah). – 2014. – 1.05).***

***

Буквы являются мощным оружием, и публикация нескольких десятков может иметь значительные последствия. Сила социальных медиа сегодня такова, что может значительно поднять популярность компании, но ее же может и разрушить. Достаточно лишь одного неосторожного высказывания, например, в Twitter.

На прошлой неделе это доказал финансист и миллионер Н. Ротшильд, который фривольно высказался в сервисе микроблогов о своем бизнес-партнере А. Бакри в горнодобывающей компании Asia Resource Minerals (ARMS). «Хотя твой отец является злым гением, – написал в Twitter отпрыск банковской династии Ротшильдов, – ходят слухи о твоей чрезмерной глупости».

Это сообщение взорвало социальные медиа по всему миру, ведь в корпоративных пресс-релизах такой стиль сообщения не используется и выбивается из привычного шаблона. Для Н. Ротшильда это высказывание открыло дорогу к развитию и возобновило интерес общественности к его долгой борьбе против индонезийской семьи миллионеров А. Бакри. Финансист обвиняет их в обвале стоимости предыдущей до основания ARMS компании. Уже через сутки число читателей Twitter Ротшильда возросло с 200 человек до 1700.

Однако не всегда резкие высказывания ведут к светлому будущему. Например, создатель Twitter Д. Костоло сам пострадал от неосторожного

высказывания, когда сравнил американского академика В. Вадху с известным комедиантом Carrot Top. Опрометчивый твит заставил Д. Костоло пересмотреть состав совета директоров Twitter.

«Если вы не желаете, чтобы ваше высказывание оказалось на передовицах газет и интернет-сайтов, вам не стоит этого говорить», – рассказывает управляющий директор корпоративного направления в пиар-агентстве Weber Shandwick М. Уэнман.

Социальные медиа как рычаг давления

О возможностях соцсетей влиять на компании уже знают некоторые инвесторы и успешно их используют в своих целях. Например, несколько месяцев миллиардер К. Икан писал в Twitter о том, что Apple необходимо выкупить обратно больше акций. А затем его инвесткомпания в феврале официально предложила Apple программу на 14 млрд дол. по выкупу акций.

Н. Ротшильд, который говорит, что его высказывание об А. Бакри было инстинктивным, тоже присоединился к Twitter не просто так, а по стратегическим причинам. «Я заинтересован в Индонезии и своих инвестициях, некоторые из которых имеют серьезное судебное разбирательство, – говорит он. – Я хочу быть уверенным, что люди будут следить за ситуацией».

Правительства стран уже осознали силу, которой обладают социальные медиа, в частности Twitter, над компаниями. Так, в США лишь в прошлом году разрешили публиковать в этом сервисе маркетинговые новости корпораций. А в Великобритании это до сих пор под запретом.

Сами представители компаний и бизнес-консультанты считают, что благодаря Twitter бизнес может быстрее сообщать новости и реагировать на события. «Вы можете видеть, насколько медленными являются традиционные системы распространения информации: письма по электронной почте и пресс-релизы, – отмечает основатель пиар-агентства Powerscourt Р. Годсон. Именно он посоветовал Н. Ротшильду завести аккаунт в Twitter. – Он не подходит каждому, но для Натаниеля Twitter позволяет быстро реагировать на события и получить глобальную поддержку».

Нужно знать, когда остановиться

Пока одни только осваивают Twitter или пожинают плоды неосторожных высказываний, некоторые поставили этот инструмент себе в работу. Среди них – Р. Мердок и Р. Бренсон, которых аналитики считают мастерами высказываний на 140 символов. Первый, например, имеет в Twitter 500 тыс. подписчиков, а второй – 4 млн.

Еще одним ТОП-менеджером, который использует Twitter для продвижения бизнеса, является Д. Джоэррес. Он работает исполнительным директором рекрутинговой компании Manpower и имеет более 7 тыс. подписчиков в этом сервисе микроблогинга. По его словам, социальная сеть сегодня является полезным инструментом, который позволяет большому бизнесу обрести человеческое лицо. Он также отметил, что при этом нужно осознавать границы допустимого.

«Вы должны вложить немного персональности и воображения в сообщения, но не стоит перегибать палку. Это мой личный аккаунт, но при этом он еще и корпоративный. Я говорю от лица компании, – говорит он. Людям стоит волноваться, только когда они сделают что-то глупое».

Одним из ярких случаев, когда социальные сети помогают сгладить большим компаниям даже громкие провалы в своей работе, является история британского банка TSB Bank. В январе у него случился крупный сбой банкоматов, что вызвало резкое недовольство пользователей и множество гневных отзывов. Директор финансового заведения П. Пестер лично извинялся перед клиентами в Twitter. Его персональные разъяснения пользователям банка помогли сгладить кризис.

Другие ТОП-менеджеры тоже считают, что социальные сети уже стали для них частью работы. «Точно так же, как исполнительный директор любой компании, входящей в список FTSE 100 [Футси 100 – лондонский биржевой индекс. Рассчитывается независимой компанией FTSE Group, которой совместно владеют агентство Financial Times и Лондонская фондовая биржа. Считается одним из наиболее влиятельных биржевых индикаторов в Европе – прим. ред.], должен давать интервью и брифинги аналитикам, он теперь должен иметь профиль в социальных медиа, – говорит директор пиар-компании Weber Shandwick М. Уэнман. – Это нормальная часть бизнес-жизни» ***(Как 140 символов помогают строить и разрушать компании // InternetUA (http://internetua.com/kak-140-simvolov-pomogauat-stroit-i-razrushat-kompanii). – 2014. – 24.04).***

***

Сервис микроблогов Twitter анонсировал запуск нового формата рекламных блоков Website card, призванного существенно увеличить число переходов пользователей на сайт рекламодателя, пишет Marketing Media Review (http://mmr.ua/news/id/novye-reklamnye-bloki-twittera-uvelichat-chislo-perehodov-polzovatelej-na-sajt-39475/).

«Новый рекламный формат – уникальная возможность для рекламодателей продвинуть собственный контент при помощи твитов и обеспечить приток релевантного трафика на каждую страницу сайта. Будь то: домашняя страница, страница товара или страница поста в корпоративном блоге», – комментируют представители Twitter.

Формат рекламы Website card подразумевает под собой публикацию в твите блока контента со страницы сайта с добавлением кнопки Read more. Данное решение заставит заинтересовавшегося пользователя перейти на ресурс рекламодателя и продолжить чтение.

«Управляя функциями и инструментами таргетинга, которые основываются на анализе сигналов о пользователях, таких как: интересы, ключевые слова, взаимосвязи, знаниях о посещении пользователями сайтов рекламодателей, – маркетологи смогут при помощи формата Website Card нацеливать на свою аудиторию правильный контент в наиболее подходящее

время. Новый вид рекламы может стать еще более эффективным, если использовать его параллельно с функцией отслеживания вовлечённости пользователей во взаимодействие с брендом и последующим измерением количества конверсий», – комментирует запуск менеджер по продукту Д. Дьюкс ***(Новые рекламные блоки Twitter'а увеличат число переходов пользователей на сайт // Marketing Media Review (http://mmr.ua/news/id/novye-reklamnye-bloki-twittera-uvelichat-chislo-perehodov-polzovatelej-na-sajt-39475/). – 2014. – 28.04).***

***

Facebook официально запустил Business Manager, инструмент, который позволит агентствам и компаниям управлять несколькими кампаниями с помощью одного интерфейса, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-novyj-instrument-dlja-kompanij-business-manager-39492/).

Инструмент позволяет назначать роли людям, работающим с разными кампаниями. Facebook также обещает, что инструмент позволит агентствам и клиентам безопасно делиться материалами кампании. Business Manager позволяет компаниям добавлять или удалять рекламные аккаунты, связанные с компанией и отменять разрешение для людей, используя их аккаунты.

Инструмент также должен предоставлять операции, которые помогут разграничить личные и бизнес взаимодействия в Facebook. Пользователи могут использовать свой логин в Facebook для доступа к рекламным аккаунтам и Страницам не будучи друзьями с другими пользователями для получения доступа.

Как отметили в компании Business Manager не будет конкурировать с программой Preferred Marketing Developers ***(Facebook запустил новый инструмент для компаний Business Manager // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-novyj-instrument-dlja-kompanij-business-manager-39492/). – 2014. – 29.04).***

***

Сегодня продвижение в социальных сетях является неотъемлемой частью развития бизнеса. Всё большее число компаний заводят страницы в социальных сетях. Но главные сложности начинаются, когда они начинают думать, что же туда постить. Взять, к примеру, производителей еды и напитков. Какой контент им размещать, чтобы привлекать покупателей?

В данной статье собрано несколько примеров контент-стратегий продуктовых брендов, реализованные в Facebook. Возможно, некоторые идеи вам покажутся интересными, и вы захотите их взять на заметку.

Придерживайтесь единого стиля

Nutella – производитель популярной по всему миру шоколадной пасты. Какие идеи бренд может реализовать в Facebook кроме публикации видео и изображений с открытой банкой и пастой, намазанной на хлеб?

«Начните день с Nutella», – призывает компания. Этот девиз мы видим на обложке страницы бренда.

Эта идея, так или иначе, присутствует и в каждом посте. Благодаря этому потребители во время завтрака всегда знают, что Nutella – их «лучший друг».

Кстати, на бренд подписано более 18 млн человек.

Вывод: придерживайтесь единого стиля, используйте одну и ту же тему на обложке и в своих сообщениях, чтобы потребители точно понимали, какую идею вы хотите до них донести.

Поддерживайте необычные события

Кто не знает Nescafe? Даже те, кто не любит кофе, прекрасно осведомлены о бренде. Но как удалось этого добиться? В том числе и благодаря грамотной маркетинговой стратегии.

Одна из стратегий заключается в том, что бренд поддерживает нетипичные для себя события, которые никак не связаны с продуктом. Это позволяет Nescafe выйти за пределы обычного целевого рынка.

Nescafe приглашает потребителей на дегустацию напитка во время Парада Роз. Нечто подобное делает и M&M's, приглашая одиноких людей найти себе пару. Кто бы мог подумать, что шоколадные конфетки будут заниматься сводничеством?

Вывод: поддержите мероприятия, которые привлекут внимание людей, не относящихся напрямую к вашей целевой аудитории. Так вы станете более привлекательны и сумеете заполучить новых клиентов.

Привлекайте пользователей к участию в жизни бренда

Ваши потребители – ключ к успеху вашего бизнеса. Привлекайте их к участию в жизни сообщества в социальных сетях.

Например, Dunkin Donuts предлагает пользователям рассказать свою историю.

Для привлечения большего внимания бренд использует специальный хэштег #mydunkin.

Вывод: привлекайте потребителей к участию в жизни бренда и созданию контента. Это существенно повысит популярность вашей страницы и решит проблему «А что размещать?».

Используйте приложения

Ещё один способ сделать бренд более привлекательным – предложить потребителям пользоваться приложениями. Посмотрим на пример Dominoes. На обложке своей страницы Facebook бренд предлагает воспользоваться приложением для заказа пиццы онлайн.

Кроме того, у компании есть приложение для желающих получить работу в сети пиццерий. Таким образом, Dominoes не просто привлекает фанов и увеличивает продажи, но и воспитывает лояльность потребителей к бренду.

Вывод: используйте приложения в социальных сетях для проявления своей индивидуальности и решения маркетинговых задач.

Следите за трендами

Каждый год маркетологи делятся своими прогнозами относительно трендов на ближайшее время. Почему бы не начать им следовать?

Например, два главных SMM-тренда 2014 г. – видеоконтент и обучение потребителей вместо сосредоточения на конверсии. Этих трендов придерживается Nestle. Объединяя обучение и видео, бренд публикует посты с хэштегом #healthybytes24, рассказывая о здоровой пище на своей странице в Facebook.

Вывод: следите за трендами и следуйте им, чтобы получать преимущества перед конкурентами ***(Как продуктовые бренды продвигаются в Facebook? // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kak_produktovye_brendy_prodvigayutsya_v_facebook). – 2014. – 29.04).***

***

Социальные сети существуют не только для того, чтобы постить котиков. Предприниматели могут извлечь из них пользу для своего бизнеса, правильно выбрав инструменты для работы с соцмедиа. Редакция ЦП изучила онлайн-сервисы, предлагаемые журналом Entrepreneur, пишет Marketing Media Review (http://mmr.ua/news/id/poleznye-smm-instrumenty-dlja-predprinimatelej-39499/).

Инструменты для работы с аудиторией в Рунете

1. Visually’s Google Analytics.

Google Analytics – мощная платформа для сбора и анализа данных об аудитории сайта. Но данные на этой платформе представлены неочевидно. Советуем попробовать приложение Visually’s Google Analytics. С его помощью можно создать инфографику о показателях работы сайта, в которой будут отражены все ключевые показатели. Отдельно выделены метрики, по которым у сайта наметилось улучшение в работе с аудиторией. Делать такую инфографику можно в автоматическом режиме с обязательной отправкой готового отчета по email. Приложение бесплатно и доступно всем желающим.

2. TweetDeck.

Бесплатный и удобный клиент для работы с несколькими учетными записями в Twitter. Поддерживает отображение нескольких колонок с основной лентой, упоминаниями, личными сообщениями. Не новый инструмент, но достаточно удобный для того, кто только начал осваивать работу с микроблогами для продвижения своих товаров и услуг.

3. HootSuite.

Бесплатный «комбайн» для работы с различными социальными сетями в едином интерфейсе: здесь есть поддержка профилей и потоков в Twitter, Facebook, LinkedIn, Google+, Foursquare и целом ряде соцсервисов. Позволяет не просто общаться или ретранслировать контент с основного сайта, но и

смотреть статистику посещаемости, уровень вовлечения и оценивать эффективность работы SMM-специалиста своей компании.

Базовая версия бесплатна, а вот за расширенный анализ данных и дополнительные инструменты придется доплатить. В бесплатной учетной записи вы сможете вести до пяти профилей в разных соцсетях и транслировать до двух потоков RSS. За 6–100 профилей в соцсетях и коллективную работу до девяти сотрудников вашей компании с Hootsuite придется заплатить 8,99 дол./мес.

4. Edgerank Checker.

У Facebook есть собственная платформа и набор инструментов для оценки вовлеченности и охвата. Но в интерфейсе Facebook Insights достаточно легко заблудиться. Чтобы не пришлось выискивать информацию по оценке ключевых метрик для Facebook-страницы, советуем использовать Edgerank Checker. Здесь даже есть возможность мониторинга постов в реальном времени. Инструмент бесплатный для получения базовой информации по EdgeRank. Для дополнительного ранжирования и анализа постов, просмотра данных по негативному фидбеку и другой информации надо заплатить по 15 дол. за одну Facebook-страницу в месяц.

5. Buffer.

Простой и эффективный инструмент для публикации контента в Facebook, Twitter, LinkedIn и Google+. Подойдет для малого бизнеса, у которого нет времени или финансовых ресурсов на регулярное ведение своих страниц в социальных сетях вручную. Если в компании SMM-специалист, контент-менеджер и коммьюнити-менеджер – это один и тот же человек, то с помощью Buffer можно распланировать контент для разных каналов в течение дня. Также предлагается ряд расширений для браузеров: есть расширения для быстрой публикации контента (ссылки, страницы, сайты) для Chrome, Firefox и Safari.

Бесплатная версия позволяет работать с двумя профилями и публиковать до 10 постов в каждом профиле в день. Если же заплатить 10 дол. в месяц, то ограничений по числу публикаций не будет, а число профилей возрастет до 12.

Инструменты для работы с иностранной аудиторией

1. Sprout Social.

По аналогии с Hootsuite платформа Sprout Social позволяет отслеживать и управлять учетными записями компании в разных соцсетях. Весь контент и ленты разделены на шесть вкладок. Можно подключить Facebook, Google+ (только страницы), LinkedIn, Twitter. Посты можно планировать и публиковать с заданной периодичностью. Инструмент платный: 39 дол. за пользователя в месяц – для управления 10 профилями, мониторинга в реальном времени и создания сравнительных отчетов. За 59 дол. в месяц за одного пользователя можно получить до 20 профилей, интеграцию с Helpdesk и Google Analytics. Для самых активных предпринимателей, активно работающих с зарубежными соцсетями и разными страницами, есть

тариф 99 дол. за пользователя в месяц. За эти деньги вы сможете управлять сеткой из 50 профилей, оптимизировать посты по уровню вирусного охвата, настраивать интерфейс платформы, получать расширенные отчеты о посещаемости и взаимодействию с контентом.

2. Crowdbooster.

Инструмент для стриминга новых постов и контента в Twitter и Facebook, который помимо планирования и отложенной публикации контента, позволяет также отслеживать статистику взаимодействий с фолловерами и лидерами мнений. Инструмент платный: 9 дол. в месяц – за одну Facebook-страницу, один Twitter-профиль и одного пользователя. За 49 дол. в месяц можно получить 10 аккаунтов, возможность зарегистрировать до 8 пользователей. А за 119 дол. в месяц – 30 учетных записей в соцмедиа и до 30 пользователей, которые их администрируют.

3. Twitter Showdown.

Онлайн-сервис для сравнения двух аккаунтов в Twitter, с помощью которого наглядно можно сравнить собственный профиль и контент в микроблогах с конкурентами. Число фолловеров, уровень вовлечения для опубликованного контента, число упоминаний, время публикации контента, частота обновления и репостов – всё это можно получить при помощи данного бесплатного инструмента.

4. SocialBro.

Специальный сервис для Twitter, позволяющий анализировать вовлечение и таргетинг публикаций в микроблогах. Лучше всего данный сервис работает в паре с Buffer или Hootsuite. Предлагается бесплатный период на 15 дней. А стоимость полной версии сервиса начинается с 13,95 дол./мес. (обрабатывает до 29 тыс. контактов в 5 профилях Twitter).

5. Postling.

Этот инструмент подойдет для расширения охвата аудитории в разных соцсетях. Собирает дайджест из текущей активности, репостов и лайков в ваших профилях и страницах бренда в Facebook, Twitter, LinkedIn, в блогах, в Yelp, YouTube и Flickr. Первые 30 дней обойдутся в 1 дол., далее надо будет заплатить 10 дол. в месяц за пять профилей в соцмедиа.

6. Tailwind.

Интернет-сервис для работы с социальной сетью Pinterest. Помимо анализа вовлеченности, можно подключить Google Analytics и отслеживать конверсии по опубликованным картинкам. Инструмент бесплатен для базового использования; расширенные функции и работа с архивом контента, конкурентами и пользователями обойдется от 29 дол./мес.

7. Social Mention.

Бесплатная платформа для поиска и мониторинга активности бренда в соцмедиа в режиме реального времени. Работает с пользовательским контентом. Выдает метрики по релевантным результатам, охвату, ключевым словам, лидерам мнений ***(Полезные SMM-инструменты для предпринимателей // Marketing Media Review***

(http://mmr.ua/news/id/poleznye-smm-instrumenty-dlja-predprinimatelej-39499/). – 2014. – 29.04).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Исследователи университета Виргинии, США, убеждены, что при помощи анализа сообщений в сети микроблогов Twitter можно предсказывать совершение преступлений.

Своё утверждение исследователи подкрепляют аналитическим алгоритмом, который успешно срабатывает в прогнозировании от 19 до 25 видов преступлений. Система может предсказать кражу, разбойное нападение, домогательство и драку на бытовой почве.

Руководитель исследовательской группы М. Гербер проясняет суть проекта: сегодня в социальных сетях люди постоянно отчитываются о своих прошлых и будущих повседневных действиях.

Если несколько человек, территориально находящихся поблизости друг от друга, собираются вечером весело провести время с алкоголем, вероятность возникновения конфликтных ситуаций повышается. Что легко может привести к правонарушениям и преступлениям.

Приведённый пример является весьма грубым и схематичным, тем не менее, учёные считают, что анализ сообщений Twitter – а в перспективе, и социальных сетей вообще – позволит правоохранителям предугадывать правонарушения, и реагировать на них заранее.

Напомним, не так давно учёные из Университета Калифорнии, США, при помощи сети микроблогов Twitter построили визуальную модель распространения вирусных или бактериальных болезней по всему миру ***(По сообщениям в Twitter можно предугадывать преступления // InternetUA (http://internetua.com/po-soobsxeniyam-v-Twitter-mojno-predugadivat-prestupleniya). – 2014. – 26.04).***

***

Исследователь Р. Ландерс из Университета Олд-Доминион, штат Вирджиния, США, доказал, что, ориентируясь на страницу пользователя в социальной сети, можно предсказать, насколько будет высок уровень производительности труда того или иного соискателя.

Активность человека в социальных сетях наиболее ярко проявляет две его личностные характеристики: добросовестность и экстраверсию.

Под добросовестностью исследователь подразумевает общую организованность человека, его пунктуальность, умение выполнять работу вовремя. Это главная черта, помогающая определить успешность потенциального сотрудника.

Экстраверсия – склад личности с активностью, направленной преимущественно на внешний мир и социальные отношения.

Для своих исследований Р. Ландерс с помощниками опросил 146 человек. Испытуемые проходили специальный психологический тест. Тем временем, другая группа учёных оценивала личностные качества участников теста на основе их профилей в Facebook.

Полученный в результате анализа страницы в социальной сети психологический профиль оказался точнее, и позволил узнать о людях больше, чем говорили они сами о себе во время теста.

Кроме того, изучение учётных записей в Facebook позволяет узнать достоверные факты о том, как вели себя участники опроса в прошлом ***(Профиль в социальной сети расскажет, насколько хорош потенциальный сотрудник // InternetUA (http://internetua.com/profil-v-socialnoi-seti-rasskajet--naskolko-horosh-potencialnii-sotrudnik). – 2014. – 3.05).***

Маніпулятивні технології

«Информационная война» – это термин, который обозначает процесс манипуляции информацией с целью достижения тех или иных целей. Цели могут быть от самых мелочных, до мирового масштаба.

Ещё некогда сам У. Черчелль утверждал, что «Кто владеет информацией – тот владеет миром», – британского политика нельзя упрекнуть в том, что он был не прав. Однако на сегодняшний день данное изречение немного меняет свое значение.

В настоящее время информационное пространство стало настолько доступным для любого рядового гражданина, что уже не информация ценится, как источник знаний и истины, а умелое использование, внедрение дезинформации является ценным инструментом манипулирования общественным мнением. Термин «Информационная война» также видоизменился и со временем приобрел совсем иное значение, чем это было когда-то.

Информация в цифрах

Не менее сотни тысяч журналов выходят ежегодно на 60 языках мира. Эксперты подсчитали, что с 1950 г. количество информации в мире удваивалось каждые 10 лет, в 70-х – раз в пять лет, а теперь информационное пространство разрастается каждый год. К чему приведет информационный бум, существует множество теорий.

С какой целью мы распространяем и получаем информацию

Сегодня информация является полноценным продуктом, который имеет свою цену. Люди покупают, продают, обменивают и даже спекулируют информацией, и многие ученые уже пришли к неутешительному выводу, что информация для людей, как источник знаний для саморазвития и духовного возвышения отошла на второй план. Более того, сейчас сведения и информация – это верный инструмент для заработка денег.

Современные источники информации

Конечно же, более доступной для широких масс информация стала с появлением Интернета. Сегодня мы черпаем знания, сведения, новости, справочную информацию из социальных сетей, читаем о событиях насущных на интернет-сайтах различной тематики. Также в сети можно найти литературу обширной тематики – от художественной до научных пособий.

Кроме того, граждане активно обмениваются информацией, взятой из непроверенных источников, от человека к человеку, что зачастую запускает механизм активации информационного вируса…

Сарафанное радио

Сарафанное радио – это, пожалуй, один из самых древних способов добычи и распространения информации. Такой подход к получению сведений дает отличный инструмент манипулирования общественным мнением.

Психологический фактор таков, что обычному человеку интереснее получить информацию методом «из уст в уста», нежели из официального источника. Многие специалисты считают, что большую роль в формировании такого психоэмоционального влияния играет устройство нашего общества, культура общения нации и уровень доверия граждан к властям своей страны.

Кроме того, человек сам по себе склонен к преувеличению, поэтому не стоит удивляться, что изначально новость о мухе, в конце концов, станет сенсацией «слоновьих размеров» – это в действии так называемый испорченный телефон.

Примеров можно привести массу. Взять хоть 2007 г., когда в Интернете расползлись слухи о взрыве на Волгодонской АЭС. Однако можно и не заглядывать так глубоко назад, ведь прямо на глазах у всей планеты разворачивается драма, начавшаяся с Евромайдана в Киеве.

Как известно, сегодня настоящий очаг вооруженного конфликта образовался на востоке Украины, а очень большую роль в развитии событий, в частности в эскалации насилия, сыграла двусторонняя дезинформация.

Информационная война в Украине

Справедливо можно сказать, что информационная война в нашей стране сейчас ведется по нескольким фронтам: между Россией и Украиной (международный масштаб), между украинскими властями и гражданами (локальный характер).

Сегодня опасный вирус дезинформации – это главное оружие в такой войне. И даже скептики молчат, ведь понимают, что слово бывает порою острее ножа. Умелые ораторы веками разжигали войны с трибун, сегодня масштабы поля брани разрослись до невообразимых размеров.

В Украине информационная война уже давно вышла за рамки блогосферы, хоть и стоит признать, что социальные сети остались самым влиятельным инструментом передачи и распространения информации.

Как начиналась информационная война в Украине

Кольцо «боевых действий» начало туго смыкаться вокруг информационного поля Украины ещё в минувшем году. Тогда Россия начала освещать события Майдана и преподносить их своему зрителю под «Кремлевским соусом», однако нельзя говорить и о незаангажированности всех украинских СМИ – ситуация примерно такая же.

Итак, оппоненты начали пестреть критикой в адрес друг друга, занялись распространением информации и начали мешать друг другу.

Хронология событий в начале

Нацсовет Украины по теле- и радиовещанию сначала робко, а потом уже в форме ультиматума потребовал прекратить трансляцию в Украине нескольких российских каналов. Конечно, провайдеры кабельного ТВ противились как могли. Главный аргумент – пользователи проплатили определенную услугу, пакет каналов, которая включает трансляцию конкретных телевизионных каналов. Однако Нацсовет и СНБО были неумолимы, поэтому 11 марта около половины от всех действующих в Украине кабельных провайдеров прекратили трансляцию ряда российских каналов. В опале оказались такие каналы как ОРТ, РТР-планета, Россия 24, Вести и НТВ мир.

Тем временем в оккупированном Крыму

А в Крыму ждать не стали и отключили все украинские каналы, заменив их российскими, конечно. Поначалу пользователям говорили, что такая мера введена из-за технических неполадок, потом начали говорить о задолженности со стороны Украины за эксплуатацию эфирных установок и ретрансляторов.

Конечно, не обошлось без «слепых фактов», людям говорили, что в Крыму кабельным операторам угрожали оружием, заставляя отключить украинские каналы. Ранее В. Лутковская заявляла, что эпицентр информационной войны развернулся именно в Крыму.

По итогам, мы имеем пострадавшую сторону – крымчане, ведь именно их лишили возможности получать информацию из альтернативных источников, а значит, лишили права на другую точку зрения. Близится время, когда Россия начнет и фильтрацию интернет-пространства крымчан, ведь в самой стране-агрессоре эта схема уже давно введена и работает. Российскую цензуру в действии испытали на себе такие медиа-гиганты, как социальная сеть «ВКонтакте», и практически уничтоженный Кремлем телеканал Дождь.

Недавние исследования, результаты которых активно используются в различных аналитических статьях, говорят о том, что 70 % россиян не отрицают, что правительство их страны практикует политику строгой цензуры.

Россия, конечно же, не остановится ни на фронте реального захвата Украины, ни на поле боя информационной войны, поэтому паниковать начинают европейцы.

Так, в СМИ заговорила Польша, власти которой считают, что Россия начала действовать и на их информационном пространстве, разжигая искру ненависти между украинцами и поляками. Не нужно быть социологом, чтобы сделать такие выводы, стоит только открыть любую статью в польских СМИ о происходящем в Украине и прочесть комментарии под тестом – растет количество антиукраинских и антипольских высказываний. Это яркий пример влияния информации на сознание и мнение каждого отдельного гражданина.

Как фильтровать информацию обычному украинцу

Прежде чем поверить, проверь или «Доверяй, но проверяй» – известное и ценное выражение. Во-первых, стоит оговориться, что человеческий разум не может отличить присутствие истины от её отсутствия – это факт, с которым стоит считаться.

В сегодняшних условиях максимальную пользу гражданам принесет тактика получения информации из нескольких источников. Не стоит слепо доверять одному источнику информации, ведь даже самые надежные детали иногда дают сбой.

Научитесь сопоставлять факты, проверять реальность услышанного ***(Ржевская В. Украина на острие информационной войны. Стратегия выживания // NovostiUA.net (http://novostiua.net/stati/55618-ukraina-na-ostrie-informacionnoy-voyny-strategiya-vyzhivaniya.html). – 2014. – 26.04).***

***

США создавали социальные сети наподобие Twitter для «развития открытой политической дискуссии» в странах Азии и Африки, сообщает New York Times со ссылкой на администрацию президента Б. Обамы.

В Белом доме сообщили, что проекты действовали в десятках стран с 2010 г. Большая часть проводилась в тайне от правительств этих государств, поэтому администрация президента не раскрывает данные о них. В Афганистане, Пакистане и Кении информация об этих программах была частично открыта.

В частности, в Пакистане Госдепартамент США работал над сервисом Humari Awaz («Наши голоса») совместно с правительственными и телекоммуникационными организациями страны. Программа была закрыта из-за недостатка финансирования. Кенийский проект Yes Youth Can создан Агентством США по международному развитию и существует до сих пор.

Также в Белом доме сообщили, что планировалось создать подобные сервисы в Нигерии и Зимбабве.

В начале апреля в администрации президента США сообщили о попытке развития такого же проекта на Кубе. Соцсеть ZunZuneo существовала с 2008 г. и была закрыта в середине 2012 г. из-за проблем с финансированием. Максимальное количество пользователей сервиса достигало 40 тыс. пользователей. Американские власти скрывали, что они являются организатором этого проекта.

В 2010 г. в арабских странах прошла волна протестных выступлений, которая получила название «Арабская весна». По мнению политологов, большую роль в ее распространении сыграли социальные сети, особенно Twitter. В связи с этим власти Египта и Ливии пытались полностью ограничить доступ к Интернету ***(Белый дом рассказал о секретных «твиттерах» в недемократических странах // InternetUA (http://internetua.com/belii-dom-rasskazal-o-sekretnih--tvitterah--v-nedemokraticseskih-stranah). – 2014. – 29.04).***

Зарубіжні спецслужби і технології «соціального контролю»

Міжнародна конференція з інтернет-безпеки NetMundial, яка відбулася в Сан-Паулу (Бразилія), запропонувала визнати стеження за користувачами кримінальним злочином в усьому світі.

Про це повідомляє Укрінформ із посиланням на інформаційну службу Бі-Бі-Сі.

Конференцію ініціювала президент Бразилії Д. Русеф, за якою тривалий час стежили спецслужби США.

У конференції взяли участь 600 делегатів із 85 країн світу. Прийнято резолюцію, яка засуджує всі форми шпигунства в Інтернеті. Однак її не було схвалено одноголосно. Росія, зокрема, виступила проти – вона вважає, що цей документ обмежує суверенітет держави в законодавчій галузі ***(Міжнародна громадськість вважає стеження за користувачами кримінальним злочином // Західна інформаційна корпорація (http://zik.ua/ua/news/2014/04/25/mizhnarodna_gromadskist_vvazhaie_stezhennya_za_korystuvachamy_kryminalnym_zlochynom_482543). – 2014. – 25.04).***

***

Російський парламент прийняв пакет «антитерористичних законів», згідно з якими закордонні компанії будуть зобов’язані зберігати інформацію про активність своїх користувачів на території Росії і мінімум протягом шести місяців.

Як пише Lenta.ru в короткому аналізі нових законодавчих ініціатив Думи РФ, обмеження можуть торкнутись таких популярних сервісів, як Skype та Gmail. Переписка користувачів цих мессенджерів (як і Яндекса чи

«ВКонтакте», наприклад) повинна буде зберігатись на серверах у Росії. Описана процедура створена нібито для захисту російських громадян від тероризму – а потенційні терористи також можуть бути користувачами популярних соцмереж та сервісів.

Водночас, за словами експертів та юристів, опитаних виданням, єдиним практичним застосуванням цього закону у разі, якщо іноземні компанії відмовляться зберігати переписку в Росії, стане повне їх блокування на території федерації. Іншого дієвого способу забезпечити виконання нових законів немає.

Представники Google, Facebook, Microsoft поки що утрималися від коментарів на цю тему ***(В Росії можуть заборонити Skype і Gmail // UkrainianWatcher (http://watcher.com.ua/2014/04/22/v-rosiyi-mozhut-zaboronyty-skype-i-gmail/). – 2014. – 22.04).***

***

Президент России В. Путин считает, что Интернет возник как проект ЦРУ.

«Все это возникло как спецпроект ЦРУ США, так и развивается», – сообщил российский лидер на заседании Медиафорума в Санкт-Петербурге.

По его словам, в России необходимо размещать серверы крупных национальных интернет-ресурсов и защищать хранящуюся там информацию, поскольку в США, через которые проходит основной поток данных, все контролируется.

Ранее, отметил В. Путин, у российских компаний не было возможности для таких капиталовложений, но в настоящее время они появляются ***(Путин заявил, что интернет – это проект ЦРУ // InternetUA (http://internetua.com/putin-zayavil--csto-internet---eto-proekt-cru). – 2014. – 25.04).***

***

Роскомнадзор закрыл доступ к ряду сайтов, где якобы украинцы призывали устроить массовые акции протеста в России

«Роскомнадзором ограничен доступ к более чем 10 информационным ресурсам, содержащим призывы интернет-сообществ украинских националистов к массовым акциям протеста в России», – говорится в сообщении Генпрокуратуры по Сибирскому федеральному округу.

О каких конкретно сообществах идет речь, прокуратура не уточняет ***(РФ закрыла доступ к ряду украинских сайтов // InternetUA (http://internetua.com/rf-zakrila-dostup-k-ryadu-ukrainskih-saitov). – 2014. – 28.04).***

***

Совет Федерации РФ одобрил закон, обязывающий блогеров, интернет-страницы которых ежедневно посещают более 3 тыс. пользователей, выполнять требования, предъявляемые к СМИ.

Документ также обязывает организаторов распространения информации в сети – поисковые системы, социальные сети и форумы – уведомлять профильный регулятор (Роскомнадзор) о начале своей деятельности и хранить данные в течение шести месяцев, за неисполнение этих требований предусмотрены штрафы до 500 тыс. р. (14 тыс. дол.) ***(Совфед РФ обязал соцсети хранить данные // InternetUA (http://internetua.com/sovfed-rf-obyazal-socseti-hranit-dannie). – 2014. – 29.04).***

***

Российские власти обсуждают комплекс мер по ужесточению контроля за интернет-провайдерами, пишет «Коммерсант» со ссылкой на источник. Соответствующие предложения по нормативно-правовому регулированию в сфере инфраструктуры связи готовятся рабочей группой при администрации президента РФ. Как следует из предложений, в России необходимо принудительно ввести три уровня сетей передачи данных: местный, региональный, общероссийский. Далее – наложить запрет на присоединение региональных и местных сетей передачи данных к зарубежным. Пропуск всего трафика региональных и местных операторов предлагается осуществлять только через сети общероссийских операторов. На всех уровнях всех сетей передачи данных вводится фильтрация контента, а также запрет на размещение DNS-серверов доменов .RU и .РФ за пределами территории России. Кроме того, предлагается лишить полномочий Координационный центр доменов .RU и .РФ, который разрабатывает правила регистрации доменных имен в зонах .RU и .РФ, и передать его функции уполномоченному федеральному органу исполнительной власти. Рабочая группа предлагает сохранить требования по лицензированию сетей передачи данных и сетей телевещания и в то же время сделать предметом лицензирования сети связи и деятельность по переводу URL-адресов в IP-адреса и обратно.

Введение иерархии сетей передачи данных приведет к росту стоимости доступа в Интернет и снижению его качества, так как операторы не смогут выбирать оптимальные маршруты трафика, считает один из участников рынка. По его мнению, запрет на размещение DNS-серверов .RU и .РФ приведет к тому, что в этих зонах перестанут регистрироваться, а предложение оставить в качестве предмета лицензирования сети передачи данных и телевизионного вещания сейчас невозможно реализовать: голосовую связь нельзя перевести полностью в IP, так как часть сетей в России до сих пор аналоговые. Предложение ввести государственное лицензирование деятельности по переводу URL-адресов в IP-адреса и обратно собеседник издания расценивает как «фактическое отключение страны от Интернета» ***(Российские власти намерены ужесточить***

контроль за интернет-провайдерами // InternetUA (http://internetua.com/rossiiskie-vlasti-namereni-ujestocsit-kontrol-za-internet-provaiderami). – 2014. – 29.04).

***

Совет национальной безопасности и обороны Украины (СНБО) рассматривает вопрос об отключении некоторых российских интернет-ресурсов. Об этом во время пресс-конференции заявила заместитель секретаря СНБО В. Сюмар, передает «Обозреватель» со ссылкой на РБК-Украина (http://obozrevatel.com/politics/34829-snbo-mozhet-zablokirovat-rossijskie-sotsialnyie-seti.htm).

«Россия заблокировала доступ к 10 украинским сайтам. Для нас этот вопрос так же актуален, он сейчас находится в состоянии разработки. Мы, как страна, никогда не использовали блокирование интернет-ресурсов. Но, очевидно, что коммуникация террористов сейчас проходит в российских социальных сетях. Но блокировать интернет-ресурсы это – опасный прецедент», – рассказала В. Сюмар.

По ее словам, в настоящее время идет рассмотрение и изучение этого вопроса. «Тут нужно все взвесить», – подчеркнула В. Сюмар ***(СНБО может заблокировать российские социальные сети // «Обозреватель» (http://obozrevatel.com/politics/34829-snbo-mozhet-zablokirovat-rossijskie-sotsialnyie-seti.htm). – 2014. – 29.04).***

***

Жителям Нью-Йорка следует быть осторожнее, поскольку их частные разговоры может подслушать обычная лампа, причем местонахождение шпионского гаджета неизвестно, пишет британская газета The Daily Mail.

Лампа под названием Conversnitch подслушивала разговоры горожан уже несколько месяцев и транслировала отдельные реплики в специально созданный аккаунт в Twitter.

Подробности об устройстве раскрыли его создатели. 23 апреля художники К. МакДональд и Б. Хаус, которые задумали Conversnitch как арт-проект, призванный заставить обывателей задуматься о том, что в современном мире практически невозможно гарантировать конфиденциальность. На создание устройства художников вдохновил поток новостей о слежке, которую годами вели американские и британские спецслужбы.

Conversnitch состоит из мини-компьютера Raspberry Pi, микрофона, светодиода, а в качестве корпуса для этой техники используется обычный пластиковый цветочный горшок. Устройство помещается на место обычной лампы и записывает разговоры находящихся поблизости людей. При помощи публичных сетей Wi-Fi записи передаются. Затем файл в краудсорсинговый сервис Amazon Mechanical Turk, работники которого расшифровывают

запись и публикуют ее отрывки в Twitter. Стоимость одного такого устройства составляет примерно 100 дол.

К. МакДональд и Б. Хаус также опубликовали видео, из которого следует, что они установили несколько ламп Conversnitch по всему городу: в кафе, в офисе на улице, в библиотеке и в чьей-то спальне ***(Лампа-шпион подслушивает разговоры нью-йоркцев и транслирует их в Twitter // InternetUA (http://internetua.com/lampa-shpion-podslushivaet-razgovori-nua-iorkcev-i-transliruet-ih-v-Twitter). – 2014. – 26.04).***

***

Американские интернет-сервисы отныне обязаны при соответствующем запросе передавать властям США пользовательские данные, даже если эта информация хранится на зарубежных серверах. Как сообщает Reuters, такое решение на судебном заседании в Нью-Йорке принял федеральный судья Д. Фрэнсис.

Постановление суда касалось требования спецслужб к корпорации Microsoft открыть доступ к переписке одного из ее клиентов. Защита утверждала, что эта информация хранится на сервере в Дублине и компания не обязана раскрывать ее.

Однако суд вынес решение, что ордер на выдачу цифрового контента регулируется законом «О хранении информации» и распространяется за пределы территории его юрисдикции. Адвокаты корпорации собираются обжаловать это постановление в окружном суде.

Решение Д. Фрэнсиса стало прецедентом и, по американскому законодательству, может распространяться на другие аналогичные дела. Теперь ни Microsoft, ни Google, ни любая другая американская интернет-компания не имеет права отказать спецслужбам США в предоставлении информации о своих пользователях, даже если эти данные хранятся на иностранных серверах ***(Судебный прецедент обязал компании США раскрывать данные иностранных пользователей // InternetUA (http://internetua.com/sudebnii-precedent-obyazal-kompanii-ssha-raskrivat-dannie-inostrannih-polzovatelei). – 2014. – 27.04).***

***

Как сообщило издание Reuters, китайские спецслужбы в течение года читали переписку австралийских парламентариев. Осуществляемые ими кибератаки на компьютерную сеть парламента в 2011 г. позволяли получать доступ к личной переписке его членов.

По данным издания, эти атаки были более «обширными», чем предыдущие, и «эффективно предоставляли контроль над целой системой». «Это было подобно золотой жиле. У них был доступ ко всему», – цитируют издание неназванные источники.

Стоит отметить, что парламентская компьютерная сеть является незасекреченной внутренней системой, которой пользуются федеральные законодатели, персонал и советники для частных обсуждений.

Находясь в системе, помимо переписки, хакеры также имели доступ к спискам контактов и другим данным, хранящимся в сети. Это позволяло Китаю лучше понять политические, профессиональные и социальные связи австралийского правительства, в том числе, конфиденциальные обсуждения между законодателями и их сотрудниками.

Уязвимость была обнаружена в 2011 г. Кроме того, сообщалось, что хакерам удалось похитить проекты многомиллионных штаб-квартир австралийской разведки, а также информацию Министерства иностранных дел и торговли Австралии.

Напомним, что правительство Т. Эбботта, занявшего пост премьер-министра в прошлом году, поддержало запрет на участие китайской компании Huawei Technologies Co Ltd в 38-миллионном тендере по развитию национальной сети National Broadband Network из соображений кибербезопасности ***(Китайские спецслужбы в течение года читали переписку австралийских парламентариев // InternetUA (http://internetua.com/kitaiskie-specslujbi-v-tecsenie-goda-csitali-perepisku-avstraliiskih-parlamentariev). – 2014. – 28.04).***

***

Співробітники ЦРУ перехопили записи закритих розмов московських урядовців, які давали вказівки терористам на Сході України

Про це заявив держсекретар США Д. Керрі на закритому засіданні тристоронньої комісії у Вашингтоні, пише Еспресо.TV з посиланням на американське видання The Daily Beast.

«Корпорація Intel зараз виготовляє записані на плівку розмови розвідників, яким віддають накази з Москви, і всі можуть вказати різницю в акцентах, ідіомах, у мові. Ми точно знаємо, хто віддає ці накази, ми знаємо, де вони і звідки», – сказав Д. Керрі.

При цьому він не назвав конкретних російських чиновників, які фігурують у записах, але стверджує, що перехоплена інформація свідчить про те, що росіяни навмисно розпалюють протистояння на сході України і брешуть про це офіційним особам зі США та громадськості.

«Це не випадково, що є деякі люди, яких ідентифікували і у Криму і в Грузії і які зараз знаходяться у східній Україні», – сказав держсекретар. «Це образа для будь-якої розвідки, не кажучи вже про наші уявлення того, як ми повинні себе поводити у XXI столітті. Це бандитизм, це шахрайське державництво», – наголосив він ***(Керрі: ЦРУ перехопило вказівки кремлівських чиновників терористам на сході України // Espreso.tv (http://espreso.tv/news/2014/04/29/kerri_cru_perekhopylo_vkazivky_kremlivskykh_chynovnykiv_terorystam_na_skhodi_ukrayiny). – 2014. – 29.04).***

***

Обнаружение Heartbleed уязвимости спровоцировало новую волну дебатов по поводу того, должна ли спецслужба держать бреши в тайне.

В понедельник, 28 апреля, координатор по кибербезопасности Белого Дома США М. Дениэл пролил свет на то, в каких случаях Агентство национальной безопасности держит информацию об уязвимостях в тайне, а в каких раскрывает.

«Сбор огромного запаса нераскрытых брешей, при этом оставляя Интернет уязвимым, а американцев – незащищенными, не входит в интересы нашей национальной безопасности – заявил М. Дениэл. – Но это не означает, что мы должны полностью отказаться от их использования при сборе информации в целях защиты нашей страны в долгосрочной перспективе».

Напомним, что в начале нынешнего месяца была обнаружена Heartbleed уязвимость, эксплуатация которой позволяла похищать учетные данные пользователей, а также информацию их кредитных карт. Данная брешь затронула около 500 тыс. сайтов, в том числе Google, Facebook, Yahoo и многие другие.

Ранее сообщалось, что АНБ знала об уязвимости, но не раскрыла ее общественности, однако ведомство сразу же отвергло эти обвинения. М. Дениэл также подтвердил информацию о том, что АНБ было неизвестно о бреши.

«Несмотря на то, что мы не знали о существовании Heartbleed уязвимости, этот случай спровоцировал новые дебаты по поводу того, должно ли правительство скрывать от общественности информацию о брешах», – отметил эксперт.

По словам М. Дэниела, в большинстве случаев правительство раскрывает уязвимости. Тем не менее, в некоторых случаях лучше эту информацию держать в тайне, добавил эксперт. Например, для препятствования террористическим атакам или краже национальной интеллектуальной собственности ***(Эксперт пояснил, в каких случаях АНБ не раскрывает информацию об уязвимостях // InternetUA (http://internetua.com/ekspert-poyasnil--v-kakih-slucsayah-anb-ne-raskrivaet-informaciua-ob-uyazvimostyah). – 2014. – 30.04).***

Проблема захисту даних. DDOS та вірусні атаки

Количество DDoS-атак за год возросло в среднем на 47 %, причем средняя интенсивность атаки за тот же период возросла на 133 %, что говорит об увеличении доступности сетевых ресурсов, находящихся в распоряжении хакеров. Об этом говорится в последнем отчете компании Prolexic, поставляющей услуги защиты от DDoS-атак.

В отчете компании сказано, что организаторы атак в I квартале 2014 г. чаще других злоупотребляли такими сетевыми протоколами, как Character

Generator (CHARGEN), Network Time Protocol (NTP) и Domain Name System (DNS). Еще одним опасным трендом в организации DDoS-атак специалисты называют атаки класса reflection and amplification, распространенность которых за год возросла на 40 %.

По данным компании, за последний год нагрузка не сети фильтрации трафика возросла в среднем вдвое, что говорит о фактическом увеличении доступности сетевых ресурсов в распоряжении хакеров. За счет традиционных бот-сетей, а также техник отражения трафика и манипуляции с DNS, организаторам атак удалось организовывать сетевой поток мощностью до 200 Гбит/сек с информационной нагрузкой до 53,5 Мп/с (миллионов сетевых пакетов в секунду).

В Prolexic говорят, что примерно четверть DDoS-атак были организованы на сайты-СМИ и сайты развлекательных направлений. В целом компания отмечает, что организаторы атак чаще стали использовать для DDoS-атаки с участием сетевого уровня (Layer 3 и 4), тогда как DDoS на уровне приложений (Layer 7) снизились за год на 21 %.

В отчете сказано, что каждый раз организаторы DDoS руководствовались разными мотивами, но в целом их стратегия заключалась в следующем: используй как можно меньше ресурсов, создавая как можно бОльший урон. Это привело к формированию черного рынка DDoS-инструментов и DDoS-сетей, которые позволяют организовать систему DDoS-as-a-service для потенциальных клиентов DDoSсеров ***(Количество DDoS-атак за год выросло на 47 % // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/04/22/Prolexic-report.html). – 2014. – 22.04).***

***

Мы неоднократно слышали о том, что пользователи операционной системы Android подвержены большей опасности получения на свои устройства вредоносного программного обеспечения, способного передавать злоумышленникам персональные данные и деньги пользователей, чем владельцы гаджетов от Apple. Однако один из пользователей ресурса Reddit обнаружил вредоносное приложение, которое работает в фоновом режиме на iOS-устройствах. Данное приложение пересылает своему разработчику Apple ID устройств, на которые он установлен. Однако опасность заражения присутствует только в том случае, когда на устройстве установлен Jailbreak, а пользователь устанавливает из ненадежных источников некоторые приложения.

Вредоносное приложение называется «Unflod Baby Panda» и распространяется через китайские сайты со взломанными приложениями для iOS. Немецкая компания по безопасности SektionEins сообщает, что данное приложение отслеживает SSL-трафик и информацию об учётной записи Apple ID. Компания уверена, что приложение способно установить и другие

файлы на заражённые устройства. В то же время сообщается, что удалить вредоносное ПО с устройства можно вручную.

В настоящее время Jailbreak-сообщество считает, что удаление Unfold.dylib и изменение пароля Apple ID достаточно, чтобы избавиться от проблемы. Однако вредоносное приложение полностью не исследовано, и неизвестно о каких-либо дополнительных его особенностях. Поэтому мы считаем, что единственным способом обезопасить себя является полное восстановление устройства.

Стоит ещё раз отметить, что угроза касается только тех пользователей, кто установил Jailbreak и пользуется приложениями из ненадежных источников ***(Вирусы для iOS всё же существуют // InternetUA (http://internetua.com/virusi-dlya-iOS-vs--je-susxestvuuat). – 2014. – 22.04).***

***

Учетные записи пользователей Steam очень часто становятся целью киберпреступников, которые разрабатывают очень изощренные методы взлома. Для защиты клиентов Valve создала функцию Steam Guard, однако в своем текущем виде ее оказалось недостаточно – недавно систему научились обходить фишеры.

Благодаря Steam Guard пользователи получают на электронную почту код подтверждения каждый раз, когда осуществляется попытка авторизации с нового компьютера. Это означает, что даже если у злоумышленника есть логин и пароль, он не может украсть учетную запись без доступа к почтовому ящику жертвы.

Исследователи из Malwarebytes заявили, что взломщики нашли способ обойти механизм защиты с помощью фишинговой атаки. При посещении специально сформированной страницы у игрока спрашивают логин и пароль Steam-аккаунта, после ввода которого отображается следующее сообщение:

«Мы заметили, что вы заходите в Steam из нового браузера или нового компьютера. Возможно, вас просто давно здесь не было… В качестве дополнительной меры безопасности вам придется обеспечить доступ через этот браузер, передав определенный файл ssfn* из папки Steam… Файл ssfn* содержит ваш ID и расположен в одном из разделов папки Steam (…/Program Files/Steam/ssfn*)».

Дело в том, что при авторизации в Steam из нового устройства Steam Guard создает SSFN-файл, который подтверждает, что устройство действительно принадлежит владельцу аккаунта. Получив данный файл, злоумышленники могут очень легко войти в игровой сервис под именем жертвы, не вводя дополнительный код защиты.

Данный метод фишинга активно используется уже приблизительно месяц, из-за чего многие пользователи жалуются на потери коллекционных карточек и прочего.

Администрации Steam известно о данной угрозе – на странице технической поддержки Steam Guard появилось уведомление,

предупреждающее пользователей ***(Фишеры научились взламывать учетные записи в Steam, невзирая на Steam Guard // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/04/22/phishers-bypass-steam-guard-protection.html). – 2014. – 22.04).***

***

Согласно предоставленному компанией Verizon отчету – Data Breach Investigations Report – в двух из трех инцидентов безопасности хакеры использовали краденные или скомпрометированные данные. «Попытки получения правдивых учетных данных – часть многих видов атак, – заявляет Д. Джейкобс, старший аналитик Verizon и соавтор доклада. – Проникновение в систему при помощи прошедших проверку подлинности учетных данных открывает намного больше возможностей. Не нужно компрометировать каждый ПК в системе отдельно. Нужно просто авторизоваться».

В отчете содержатся данные от 50 организаций из 95 различных стран, включая Секретную службу США, польскую и латиноамериканскую команды быстрого реагирования на киберугрозы. Специалисты проанализировали около 1367 подтвержденных инцидентов. В общей сложности в 2013 г. было зафиксировано 63 437 нарушений безопасности.

В 2013 г. около 422 инцидентов безопасности произошли посредством использования украденных учетных данных. Далее следуют случаи использования вредоносного ПО, нацеленного на кражу информации (327), фишинг-атаки (245), сканирования POS-систем (223), а также применение бэкдоров (165). Помимо этого, были также зафиксированы случаи использования бэкдоров в C&C-серверах (152), шпионского ПО (149) и загрузчиков вредоносного ПО (144).

В отчете указывается, что 75 % инцидентов безопасности в финансовом секторе проводились через атаки на веб-приложения, DDoS-атаки и скимминг. 54 % нападений в промышленном секторе проводились при помощи методов кибершпионажа и DDoS-атак. Интересно, что сектор розничной торговли также чаще страдал от DDoS-атак (33 %), нежели от нападений на POS-терминалы. Популярность последних значительно падает, отмечают в Verizon ***(Хакеры используют украденные учетные данные для осуществления взломов компьютерных систем // InternetUA (http://internetua.com/hakeri-ispolzuuat-ukradennie-ucsetnie-dannie-dlya-osusxestvleniya-vzlomov-kompuaternih-sistem). – 2014. – 23.04).***

***

Среди пользователей Android-устройств распространяется вредоносное приложение iBanking, замаскированное под мобильную версию Facebook. Об этом CNews сообщили в антивирусной компании Eset.

При входе в аккаунт на Facebook пользователь видит на экране окно установки бота iBanking под видом «мобильного приложения Facebook». Не

заметив подмены и выполнив указания приложения, он загружает вредоносное ПО. Решения Eset NOD32 детектируют iBanking как Android/Spy.Agent.AF, рассказали в Eset.

Такой метод установки вредоносного ПО (веб-инъекция) достаточно распространен, но ранее использовался только для компрометации онлайн-банкинга. Теперь он нацелен на невнимательных или новых пользователей Facebook, которые не могут отличить от подделки настоящее мобильное приложение и систему двухфакторной аутентификации, указали в компании.

После заражения устройства iBanking обеспечивает злоумышленникам широкие возможности слежки за пользователем. Среди функций бота – переадресация входящих вызовов на заданный номер, отправка SMS на любой номер втайне от владельца устройства, захват входящих и исходящих SMS, кража списка контактов, захват аудиоконтента с помощью микрофона устройства и др. Подобное шпионское ПО чаще всего применяется для кражи данных, необходимых для онлайн-платежей.

Окно установки iBanking, замаскированного под мобильное приложение Facebook

«iBanking демонстрирует реализацию более сложных функций, нежели ранее обнаруженные мобильные вредоносные программы, – отметил А. Баранов, ведущий вирусный аналитик Eset Russia. – Он может быть использован в сочетании с любым ПО, внедряющим вредоносный код в веб-страницу и заинтересованным в обходе двухфакторной аутентификации. В дальнейшем можно прогнозировать появление новых мобильных компонентов, нацеленных на другие популярные интернет-сервисы».

Эксперты вирусной лаборатории Eset рекомендуют пользователям мобильных устройств на Android устанавливать приложения только с надежных площадок, просматривать отзывы о программе и разработчике, а также защитить смартфон и планшет мобильным антивирусом ***(Программа-шпион маскируется под Android-приложение Facebook // InternetUA (http://internetua.com/programma-shpion-maskiruetsya-pod-Android-prilojenie-Facebook). – 2014. – 23.04).***

***

США и Россия являлись источниками почти 45 % хакерских атак по итогам 2013 г., говорится в исследовании «Лаборатория Касперского», презентованном на форуме «РИФ+КИБ».

При этом США находятся на первом месте с долей 25,54 %, а Россия – на втором с долей 19,44 %.

Из первой десятки стран – источников веб-атак выбыл Китай, который ранее занимал первое место в рейтинге.

«Властям Китая удалось убрать из локального киберпространства множество вредоносных хостингов, в то же время были ужесточены правила регистрации доменов в зоне .cn.», поясняется в исследовании.

Таким образом по итогам 2013 г. КНР заняла лишь 21-е место в рейтинге. Всего число атак с интернет-ресурсов, размещенных в разных странах, в 2013 г. увеличилось на 7 % по сравнению с 2012 г., до 1,7 млрд ***(США и Россия являлись в 2013 году источниками 45 % веб-атак // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/04/24/attacks-stats.html). – 2014. – 24.04).***

***

В сети зафиксирована активность ботнета из устройств, зараженных версией банковского трояна Zeus. Особенностью этого варианта вредоносного ПО является его установка руткита, который предотвращает его распознавание антивирусными решениями, сообщает К.Чен из Fortinet.

По словам ИБ-эксперта, перед началом своей активности новый вредонос также сканирует компьютер в поисках уже установленной версии 0x38 трояна ZeuS. Затем он заменяет ее бинарными файлами версии 0X3B.

«Каждый бинарник P2P Zeus (ред. – название ботнета) извлекает номер версии из пакета обновления и сравнивает его с номером, который жестко указан в коде» для того, чтобы подтвердить удачную установку апдейта, подчеркивает К. Чен.

В Fortinet говорят, что единственным отличием новой версии P2P Zeus от предыдущих является то, что он размещает файл драйвера руткита в папку %SYSTEM32%\drivers. Более ранние варианты трояна устанавливали его вместе со всем функционалом.

Руткит значительным образом усложняет не только процесс обнаружения вредоноса, но и его удаление с зараженной системы.

Вполне вероятно, что инфицировать боты удалось при помощи вредоносной кампании с использованием поддельных писем от Sturbucks.

Напомним, ранее стало известно о том, что банковский троян ZeuS распространяется с подлинной подписью приложения ***(Новый вариант P2P Zeus содержит руткит // InternetUA (http://internetua.com/novii-variant-P2P-Zeus-soderjit-rutkit). – 2014. – 23.04).***

***

Последнее время специалисты наблюдают, как SMS-троянцы расширяют географическую зону своего присутствия. В рейтинге самых часто выявляемых «Лабораторией Касперского» мобильных вредоносных программ в настоящее время первую строчку занимает троянец, способный отправлять SMS на премиум-номера в 14 различных странах мира. Однако это не предел: зафиксирован новый SMS-троянец FakeInst.ef, который угрожает пользователям 66 стран, в том числе США – в этой стране подобные вредоносные программы ранее не были замечены «Лабораторией Касперского».

Этот троянец был обнаружен специалистами «Лаборатории Касперского» в феврале 2013 г. и с тех пор получил продолжение еще в 14 разных версиях. Первые модификации умели отправлять премиум SMS только в России, но в конце первого полугодия 2013 г. появилась поддержка еще 64 стран, среди которых были государства Европы, СНГ, Латинской Америки и Азии. Согласно данным облачной инфраструктуры Kaspersky Security Network, наибольшее количество случаев заражения FakeInst.ef встречается в России и Канаде.

Троянец выдает себя за приложение для просмотра порнографического видео и просит пользователя подтвердить отправку SMS в качестве оплаты за возможность просмотра платного контента. Однако после успешной отправки сообщения FakeInst.ef просто перенаправляет пользователя на сайт, содержимое которого находится в открытом доступе.

Для отправки SMS из разных стран троянец расшифровывает свой конфигурационный файл, в котором хранятся необходимые номера и префиксы для международной связи. В этом файле FakeInst.ef выбирает подходящие значения в соответствии с мобильным кодом страны пользователя, после чего производит отправку сообщения. Кроме этого, вредоносная программа периодически обращается к управляющему серверу за указаниями. Среди команд, которые она может получить, хотелось бы выделить отправку SMS с заданным текстом на указанный в команде номер и перехват входящих сообщений. Причем FakeInst.ef может просто воровать все входящие SMS, а может удалять их или отвечать на них.

«Мы полагаем, что троянец был создан русскоязычными злоумышленниками, так как ранние версии этого троянца были рассчитаны на работу только в России. К тому же все C&C-сервера зарегистрированы и пользуются услугами хостинга в России. Практически во всех версиях FakeInst.ef используется один из двух управляющих серверов, зарегистрированных на имя человека, указавшего московский адрес и российский номер телефона. Но несмотря на свое происхождение троянец стал настоящим космополитом и теперь угрожает пользователям мобильных устройств на всех континентах. И не он один – именно поэтому смартфонам и планшетам необходима надежная защита», – отметил Р. Унучек, антивирусный эксперт «Лаборатории Касперского» ***(Обнаружен SMS-троянец, способный работать сразу в 14 странах // InternetUA (http://internetua.com/obnarujen-SMS-troyanec--sposobnii-rabotat-srazu-v-14-stranah). – 2014. – 25.04).***

***

Лидер хакерской группировки Lulzsec по кличке Sabu пару лет назад заложил всех своих товарищей ФБР. Но, оказывается, на этом дело не кончилось. Как пишет The New York Times, этот человек координировал серию кибератак ФБР против ресурсов других стран.

Сотни таких атак были проведены против государственных сайтов Ирана, Сирии, Бразилии, Нигерии, Турции и Пакистана. Насколько напрямую замешано в них ФБР – сказать сложно.

Однако известно, что существует список, в котором перечислено около двух тысяч уязвимых правительственных сайтов других стран. Под руководством Sabu (настоящее имя – Г. Монсегюр) его сообщник Д. Хаммонд собирал информацию о логинах. Она поступала в ФБР, и бюро не приходилось марать в этом руки.

Интересно, что как только Д. Хаммонд стал не нужен, его осудили и посадили в тюрьму за преступления против США. Г. Монсегюра же пока оставили на свободе, но где он – неизвестно ***(Лидер хакерской группировки Lulzsec помогал ФБР США взламывать сайты других государств // InternetUA (http://internetua.com/lider-hakerskoi-gruppirovki-Lulzsec-pomogal-fbr-ssha-vzlamivat-saiti-drugih-gosudarstv). – 2014. – 27.04).***

***

Пользователи социальной сети Facebook сообщили о сбое в работе ресурса, в результате которого из их новостных лент исчезли все записи. Сбой коснулся как мобильных приложений Facebook, так и версии соцсети для браузеров.

По данным издания The Next Web, проблемы с отображением новостной ленты наблюдаются у пользователей по всему миру.

Жалуются на недоступность новостной ленты и пользователи из России. Некоторые сообщают, что найти посты друзей на сайте все-таки можно, если пролистать вниз несколько пустых разделов. Часть пользователей пишет, что какое-то время лента действительно была недоступна, однако потом ее привычный вид вновь был восстановлен.

Представители социальной сети уже принесли извинения пользователям за доставленные неудобства и заявили, что в целом сбой устранен. О том, что стало причиной неожиданного исчезновения из новостных лент всех записей, в компании не уточнили.

В Facebook ранее уже сталкивались с похожим сбоем. В декабре 2013 г. некоторые пользователи соцсети вместо постов в ленте стали видеть сообщения со словами, что в настоящий момент записей для отображения нет. Тогда, правда, сбой коснулся только браузерной версии социальной сети. Новостные ленты в мобильных приложениях Facebook продолжали отображаться без каких-либо ошибок ***(Сбой в Facebook опустошил новостные ленты у части пользователей // InternetUA (http://internetua.com/sboi-v-Facebook-opustoshil-novostnie-lenti-u-csasti-polzovatelei). – 2014. – 27.04).***

***

Соцсеть «ВКонтакте» долгое время не могла выпустить обновление клиента под iOS 7. Релиз состоялся в конце декабря. Причина, по которой апдейт не выходил в App Store, – изменение политики Apple в отношении нелегального контента. Спустя почти пять месяцев приложение пропало из онлайн-магазина. Вместе с ним из App Store исчезли и другие клиенты, использующие API социального сервиса.

Официальное приложение «ВКонтакте» для iOS 7 исчезло из App Store 26 апреля. В настоящее время клиент недоступен для загрузки как на смартфонах iPhone, так и на планшетах iPad. По словам пресс-секретаря «ВКонтакте» Г. Лобушкина, социальная сеть знает о проблеме.

Как рассказал создатель популярного клиента «ВКонтакте» под названием «Мята», его приложение также пропало из App Store. «Сегодня утром по Мск из App Store сняли нас, официальное приложение ВК и ряд других приложений для ВК. У VK app это уже второй раз, первый был в феврале», – написал Дмитрий. Apple сообщила, что программа разработчика нарушает пункты правил App Store, запрещающие распространение нелегального контента.

«Мы выяснили, что ваше приложение Мята содержит функциональность для загрузки музыки или видео, которые не удовлетворяют пунктам правил App Store с номерами 22.1 и 22.4.

22.1: Контент в приложении должен удовлетворять требованиям в отношении соблюдения авторских прав. Это относится ко всем регионам, в котором оно доступно для пользователей. Обязанность разработчика – соблюдать местные законы.

22.4: Приложения, которые предусматривают возможность обмена нелегальными файлами, будут удалены из App Store.

По этой причине, ваше приложение удалено из App Store».

Что интересно, что еще в ноябре прошлого года Apple перестала пропускать обновления для приложений, использующих API «ВКонтакте», из-за наличия на сервисе пиратского контента. Как сообщил один из разработчиков, в 2014 г. американская корпорация будет еще строже относиться к «ВКонтакте» и неофициальным клиентам.

Смогут ли авторы приложений для «ВКонтакте» решить проблемы с App Store и вернуть клиенты в магазин, покажет время. Есть мнение, что блокировка могла произойти из-за жалобы кого-то из правообладателей ***(Apple начала блокировать клиенты «ВКонтакте» для iOS из-за доступа к нелегальному контенту // InternetUA (http://internetua.com/Apple-nacsala-blokirovat-klienti--vkontakte--dlya-iOS-iz-za-dostupa-k-nelegalnomu-kontentu). – 2014. – 28.04).***

***

Глава отдела информационной безопасности медицинской компании Essentia Health С. Эрвен провёл исследование медицинского оборудования и софта. Его заключение таково: оборудование, которое используют врачи,

настолько плохо защищено, что провести атаку, которая смешает все их планы, совершенно несложно.

Уязвимостям подвержено всё оборудование – от имплантированных инсулиновых помп и дефибрилляторов до хирургических роботов и аппаратов МРТ. С. Эрвен и его коллеги обнаружили, что госпитали полны абсолютно незащищённых устройств, и дело тут даже не в традиционных уязвимостях софта, а в банальном несоблюдении безопасности на фундаментальном уровне – например, очень простые стандартные пароли. Или, скажем, хирургические роботы оборудованы собственным файерволом, который можно обойти безумно простым способом: достаточно просто запустить сканер уязвимостей, и он «упадёт», оставив устройство незащищённым.

Резервные копии хранилищ рентгеновских снимков зачастую вообще не защищены паролями. Имплантированные автоматические помпы для доставки медикаментов легко перепрограммировать через Интернет, дефибрилляторы можно заставить давать постоянные электрические разряды.

Не составит труда получить доступ к рецептам и изменить их, можно вмешаться в операцию... Можно сделать буквально всё что угодно. Конечно, такая ситуация будет сохраняться, пока подобные «дыры» наконец не используют во зло. Тогда все засуетятся, но будет поздно ***(Практически любое медицинское оборудование очень легко взломать // InternetUA (http://internetua.com/prakticseski-luaboe-medicinskoe-oborudovanie-ocsen-legko-vzlomat). – 2014. – 29.04).***

***

Интернет-компания AOL объявила о том, что «десяткам миллионов» держателей адресов электронной почты на серверах компании придется сменить пароли и контрольные вопросы, после того как на серверы компании была совершена хакерская атака, скомпрометировавшая не менее 2 % аккаунтов.

Компания говорит, что работает с правоохранительными органами над расследованием. Уже удалось установить, что хакерами были получены email-адреса пользователей, их почтовые адреса, зашифрованные пароли и ответы на контрольные вопросы, необходимые для сброса паролей. Также в AOL говорят, что у компании нет данных о расшифровке хакерами защищенных паролей.

В компании не сообщили, сколько всего адресов электронной почты у AOL зарегистрировано ***(AOL стала жертвой хакерской атаки // InternetUA (http://internetua.com/AOL-stala-jertvoi-hakerskoi-ataki). – 2014. – 29.04).***

***

Компания Digital Security 28 апреля сообщила о появлении критичной уязвимости в Apache Struts2, Java-фреймворке с открытым исходным кодом.

Фреймворк Apache Struts сегодня очень распространен. Он не только используется для построения крупных веб-сайтов, но и является частью приложений корпоративного уровня. Кроме того, Apache Struts применяется во многих платежных веб-приложениях, включая банк-клиенты. В частности, его используют некоторые ведущие российские финансовые организации.

24 апреля 2014 г. на китайских форумах появилось сообщение о 0-day уязвимости в Apache Struts2. Основная ее опасность в том, что она может привести к отказу в обслуживании, а в некоторых условиях может вызвать произвольное выполнение кода.

Подвержены все версии 2-ой ветки (2.0.0-2.3.16). Добиться произвольного выполнения кода возможно через манипуляцию с подстановкой классов (изменение значения ClassLoader, используя специальные запросы к серверу). Сама атака возможна вследствие некорректного регулярного выражения, которое было добавлено в качестве защиты для закрытия уязвимости, найденной в декабре 2013 г. (S2-020, http://struts.apache.org/release/2.3.x/docs/s2-020.html). То есть фактически все это время уязвимость так и не была до конца исправлена).

Пользователям Apache Struts2 срочно необходимо обновить конфигурацию Struts, следуя официальному заявлению разработчиков по ссылке http://struts.apache.org/announce.html#a20140424 до выхода обновления, которое будет доступно в течение 72 часов ***(В Apache Struts 2 выявлена критическая уязвимость // InternetUA (http://internetua.com/v-Apache-Struts-2-viyavlena-kriticseskaya-uyazvimost). – 2014. – 28.04).***

***

У всіх версіях браузера Internet Explorer виявлена надзвичайно небезпечна вразливість. Вразливість дає змогу зловмисникові встановити майже повний контроль над комп’ютером користувача. За інформацією Microsoft уразливість наявна у всіх існуючих на ринку версіях браузеру Internet Explorer, із 6 версії до 11 версії. На ці версії браузера IE припадає понад половина світового ринку браузерів.

Скориставшись уразливістю, хакери можуть отримати адміністративні права в системі і мати можливість встановлювати програми, переглядати або видаляти дані і виконувати інші маніпуляції. Для цього досить заманити користувача на спеціальний сайт.

Скористатися вразливістю хакери можуть тоді, коли користувач залогінений у систему з правами адміністратора. Уже зафіксовані випадки хакерських атак з використанням цієї вразливості.

Очікується, що незабаром Microsoft випустить оновлення для Internet Explorer, яке усуне вразливість. Проте слід зазначити, що кілька тижнів тому була припинена підтримка операційної системи Windows XP, тому вона не отримає оновлення. Користувачам, які працюють із цією ОС, рекомендується перейти на альтернативні браузери ***(У всіх версіях браузера Internet Explorer виявлена надзвичайно небезпечна вразливість // UkrainianWatcher***

(http://watcher.com.ua/2014/04/29/u-vsih-versiyah-brauzera-internet-explorer-vyyavlena-nadzvychayno-nebezpechna-vrazlyvist/). – 2014. – 29.04).

***

Аналитики Arbor Networks представили результаты мониторинга угроз в начале 2014 г.

Как сообщает Help Net Security со ссылкой на компанию Arbor Networks, по итогам I квартала 2014 г. количество DDoS-атак, мощностью свыше 20 ГБ/с, увеличилось в 1,5 раза (в сравнении с аналогичным периодом в прошлом году). Такие данные аналитикам удалось получить благодаря собственной системе мониторинга интернет-угроз ATLAS.

Результаты анализа, представленные экспертами в ходе конференции Infosecurity Europe 2014, также свидетельствуют о том, что все большее число злоумышленников отдают предпочтение такому виду DDoS, как NTP отражение/усиление.

За отчетный период наиболее масштабные атаки проводились на веб-ресурсы США и Франции. В то же время объектом частых, но маломощных нападений становились серверы различных компаний Австралии.

Отметим, что NTP представляет собой UDP-протокол, предназначенный для синхронизации часов с помощью компьютерной сети. Для злоумышленников любой UDP-сервис (в том числе DNS, SNMP, NTP, chargen и RADIUS) представляет собой потенциальный вектор атаки, поскольку протокол не требует установки соединения, а IP-адрес источника атаки легко может быть подменен.

Привлекательным для хакеров также является то, что DDoS-атаки с использованием NTP имеют довольно высокую степень амплификации. При этом необходимые вредоносные инструменты легко доступны в сети, что делает данный вид нападений легко выполнимым ***(NTP значительно повышает опасность DDoS-атак // InternetUA (http://internetua.com/NTP-znacsitelno-povishaet-opasnost-DDoS-atak). – 2014. – 30.04).***

***

Как сообщает издание BBC со ссылкой на французского исследователя безопасности под псевдонимом Steven K, нашумевшая Heartbleed-уязвимость сыграла злую шутку со злоумышленниками. Брешь была использована для получения доступа к подпольным форумам и раскрыть хранившуюся там информацию.

«Речь идет о ситуации в которой “кто к нам с мечом пришел, тот от меча и пострадал”», – констатировал специалист.

Вместе с тем, по словам специалиста, «потенциал этой уязвимости, затрагивающей сервисы black-hat, просто огромен», поскольку взлому уже подверглись такие известные веб-сайты криминальной направленности, как Darkode и Damagelab.

Стоит также отметить, что наравне с инцидентами в преступном сегменте сети, появление Heartbleed-уязвимости спровоцировало объединение флагманов интернет-индустрии. Так, ряд крупных компаний (включая Cisco, Dell, Facebook, Intel, Microsoft, VMware, IBM, Google) сообщили о готовности совместно вкладывать деньги в наиболее важные проекты с открытым исходным кодом. Предполагается, что это снизит риск появления критических уязвимостей, подобных бреши в OpenSSL ***(Heartbleed-уязвимость сыграла против злоумышленников // InternetUA (http://internetua.com/Heartbleed-uyazvimost-sigrala-protiv-zloumishlennikov). – 2014. – 2.05).***

***

Очередное вредоносное ПО на платформе Android обнаружила компания Eset. Вирус под именем Android/Samsapo.A, попадая на устройство пользователя, стремится получить доступ к списку контактов для своего дальнейшего распространения.

Приложение способно скачивать другие вредоносные файлы, получать доступ к персональной информации (например, содержимому текстовых сообщений) и блокировать звонки. Пользовательские данные отправляются на домен, зарегистрированный на прошлой неделе.

Распространяется программа через отправку текстовых сообщений с фразой «Это твоё фото?» на русском языке и ссылкой на файл формата .apk, который и является копией Samsapo. Файл называется com.android.tools.system v1.0, маскируясь под системное приложение, не имеет пользовательского интерфейса и собственной иконки. Исследователи считают такую технику распространения новой для Android, хотя на Windows она давно в ходу.

Совет даётся стандартный для подобных случаев: скачивать приложения из официального магазина Google Play Store (хотя и это не даёт 100 % гарантии безопасности) и с особой тщательностью относиться к программам, запрашивающим разрешения, вроде доступа к чтению и записи текстовых сообщений ***(Новая вредоносная программа атакует пользователей Android // InternetUA (http://internetua.com/novaya-vredonosnaya-programma-atakuet-polzovatelei-Android). – 2014. – 2.05).***

***

Порядка 99 % кибератак в I квартале 2014 г. были направлены на Android-устройства. Об этом свидетельствуют результаты «Отчета по мобильным угрозам», опубликованного F-Secure Labs.

Всего за первые три месяца текущего года ИБ-эксперты обнаружили 277 новых семей и вариантов вредоносного ПО, 275 из которых были предназначены для осуществления атак на устройства под управлением ОС от Google. Еще два вируса были созданы для атак на iOS и Symbian. Стоит

отметить, что за аналогичный период прошлого года стало известно только о 149 вредоносах и их семьях, 91 % из которых предназначались для Android.

Кроме того, в I квартале специалисты зафиксировали активность первого Android-вируса, который используют для генерации криптовалюты Litecoin. Также замечен буткит Oldboot, который затрагивает первые этапы начальной загрузки устройства. Эксперты говорят, что этот вирус чрезвычайно сложно обнаружить и удалить.

В этот же период для Android появились троян, распространяющийся через Tor, и банковский троян Droidpak.

В F-Secure говорят, что в I квартале текущего года наибольшее количество атак на Android-устройства было совершено в Великобритании (пострадал один из 500 пользователей). США и Германия разместились на второй строчке с 5–10 атакованными пользователями из 10 тыс.

Наиболее часто атаки осуществлялись с целью отправки sms-сообщений на короткие номера, скачивания или установки вредоносных файлов, отслеживания местоположения устройства, слежки за пользователем при помощи аудио и видео, соединения с веб-сайтами для увеличения количества посетителей, похищения данных и пр. ***(99 % кибератак в первом квартале 2014 года были направлены на Android-устройства // InternetUA (http://internetua.com/99--kiberatak-v-pervom-kvartale-2014-goda-bili-napravleni-na-Android-ustroistva). – 2014. – 3.05).***

***

Как сообщает TorrentFreak со ссылкой на пресс-релиз компании Intelligent Content Protection, 90 % наиболее популярных пиратских торрент-сайтов содержат множество вредоносного и нежелательного ПО. Более того, две трети таких порталов связаны с мошенниками, специализирующимися на краже данных кредитных карт.

Данную статистику удалось собрать путем проведения подробного анализа 30 наиболее посещаемых нелегитимных файлообменных сервисов в сети.

Эксперты также отмечают, что в большинстве случаев администрация пиратских ресурсов перенаправляет своих пользователей на инфицированные сайты при помощи баннеров с кнопками «скачать» или «играть». При этом попытки каким-либо образом навредить своим посетителям не предпринимает лишь один из 30 торрент-сайтов.

Из отчета Intelligent Content Protection также следует, что сами веб-сайты могут не содержать вирусов, а лишь размещать небезопасные ссылки. Так, один из торрентов даже использует службу Google SafeBrowsing.

«Мы не сталкивались с автоматическими инъекциями вредоносного кода при посещении тех сайтов, которые были отсканированы. Во всех случаях, пользователь должен самостоятельно скачать и запустить исполняемый файл с вирусом», – заключают специалисты ***(Пиратские торрент-сайты кишат вредоносным ПО и мошенниками // InternetUA***

(http://internetua.com/piratskie-torrent-saiti-kishat-vredonosnim-po-i-moshennikami). – 2014. – 3.05).