СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(5–26.08)

2013 № 16

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(5–26.08)
№ 16

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 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Лига безопасного Интернета в сентябре запустит социальную сеть для активистов по борьбе с онлайн-преступлениями и противоправным контентом. Этот ресурс станет площадкой для взаимодействия кибердружинников лиги и правоохранительных органов в противодействии сайтам с противоправной информацией.

«У участников социальной сети будет возможность делиться информацией и содействовать очищению Рунета от опасного контента, возможность развиваться в рамках движения "Кибер-дружины", – отметил он, добавив, что за работу дружинники будут получать внутреннюю валюту, которую смогут менять на скидки в реальной жизни.

«С помощью сети дружинники смогут оперативно сообщать об опасных сайтах и пополнять список "белых", безопасных интернет-ресурсов. Они получат возможность через соцсеть напрямую общаться с правоохранительными органами и представителями госвласти», – пояснил представитель лиги.

По словам Скусова, соцсеть создается, в первую очередь, по просьбам самих активистов, которые устали работать в рамках существующих нетематических сетей. «В новой сети мы очерчиваем границы, вводим разделы, доступные для разных уровней пользователей, – рассказал собеседник агентства. – Так, новичок не может получить полного доступа к информации, опубликованной в рамках социальной сети, а, например, "тысячник" уже может видеть все, контролировать и координировать работу участников сети более низкого ранга». Сеть, по его словам, позволит «сократить расстояние между активистами и реальными исполнителями: оперативниками, которые привлекают киберпреступников к ответственности».

Стать участником новой социальной сети смогут все желающие. Общение в рамках ресурса будет защищено от разного рода хакерских атак. «Мы серьезно отнеслись к вопросам безопасности: ее повышенный уровень будет достигнут специальным программным обеспечением, установленным на серверах, где будет находиться сеть».

Лига безопасного Интернета была создана в начале 2011 г., в нее вошли такие крупные игроки интернет-индустрии, как операторы «Билайн», «Мегафон» и МТС, национальный оператор связи «Ростелеком», почтовый сервис Mail.ru и «Лаборатория Касперского». Среди главных задач этого партнерства – борьба с детской порнографией и проявлениями экстремизма. За минувший год кибер-дружинники, по данным лиги, помогли раскрыть 319 преступлений в Интернете ***(В России запустят соцсеть активистов-«кибердружинников» Лиги безопасного Интернета // IT Expert (http://itexpert.in.ua/rubrikator/item/28588-v-rossii-zapustyat-sotsset-aktivistov-kiberdruzhinnikov-ligi-bezopasnogo-interneta.html). – 2013. – 5.08).***

***

YouTube сообщила, что теперь ведущие каналов со 100 и более подписчиками могут использовать функцию потокового вещания. Этот шаг открывает небольшим независимым авторам широкие возможности на крупнейшем сайте видеовещания. Еще недавно подобная привилегия была открыта только для каналов, у которых не менее тысячи подписчиков, причем предыдущее снижение требований состоялось в мае.

Доступ к сервису будет разворачиваться постепенно, поэтому удовлетворяющие критерию пользователи могут получить новую функцию не сразу, а в течение ближайших дней. Когда это станет возможно, в настройках функций аккаунта напротив YouTube Live появится кнопка «Включить».

Новой категории авторов будет предоставлена возможность добавлять оригинальный значок на видео и встраивать в аннотации ссылки на веб-сайты и даже онлайн-магазины, но, как и прежде, она будет доступна только для premium-пользователей YouTube. Также теперь для объединенных плейлистом видеозаписей YouTube автоматически покажет зрителям следующее видео в серии и ссылку на весь список воспроизведения.

Как видно, Google продолжает активно превращать YouTube в сервис вещания для более успешной конкуренции с телевидением ***(YouTube снизил ограничение функции потокового вещания // Четверта Влада (http://4vlada.net/smi/youtube-snizil-ogranichenie-funktsii-potokovogo-veshchaniya). – 2013. – 6.08).***

***

Сервис Instagram добавил в свой арсенал возможность вставлять фотографии и видеоролики в социальную сеть «ВКонтакте». Теперь это можно сделать начиная с новой версии приложения, Instagram 4.1. Об этом сообщает IT Expert со ссылкой на запись в официальном аккаунте сервиса на Facebook.

При выборе российской социальной сети при помощи опции «Поделиться» снимок или видео из Instagram появится в ленте новостей пользователя «ВКонтакте». Помимо этого, у пользователя отныне появится возможность поиска других пользователей Instagram среди друзей в социальной сети.

Помимо интеграции с «ВКонтакте», версия Instagram 4.1 содержит ряд других обновлений, в частности, возможность загрузки ранее отснятых видеороликов из галереи мобильного телефона.

Ранее пользователи Instagram могли автоматически делиться фотографиями в социальных сетях Facebook, Flickr, Twitter, Tumblr и Foursquare.

Сервис Instagram был запушен в октябре 2010 г. Он позволяет размещать с мобильных устройств на iOS и Android фотографии, а также короткие видеоролики. Ежемесячная аудитория сервиса составляет 130 млн человек ***(Instagram добавил интеграцию с «ВКонтакте» // IT Expert***

(http://itexpert.in.ua/rubrikator/item/28676-instagram-dobavil-integratsiyu-s-vkontakte.html). – 2013. – 8.08).

***

Соцсеть Facebook анонсировала нововведения в своей новостной ленте. По замыслу компании, обновления должны подстегнуть активность пользователей и отбить часть аудитории у Twitter – главного конкурента ресурса.

Нововведение – это «Пропихивание новостей» (Story bumping). Теперь Facebook будет поднимать в ленте пользователей новости, который он пропустил при предыдущем чтении. Разумеется, если эти новости интересны с точки зрения соцсети, и собрали много «лайков» и комментариев. Эта система напоминает вкладку «В курсе», существующую в Twitter.

«Пропихивание новостей» уже заработало для некоторых пользователей в веб-версии Facebook, в ближайшее время нововведение доберется и до мобильных платформ. Отметим, что Story bumping не распространяется на рекламные посты и проплаченные сообщения.

Facebook отмечает, что во время тестирования новой фунции пользователи стали чаще «лайкать» новости, комментировать и «расшаривать» их.

В ближайшее время Facebook внедрит еще одно нововведение – функцию Last Actor, которая будет поднимать в ленте новости от последних 50 людей, с которыми пользователь поддерживал контакт в Facebook.

Чуть позже в соцсети может появиться фунция «Хронологии по действующему лицу» (Chronological by Actor), которая сможет упорядочивать новости по определенной теме. Таким образом, последовательность постов о каком-либо событии будет отображаться не в порядке уменьшения популярности сообщений, а в хронологическом порядке.

Многие эксперты полагают, что, реформируя ленту новостей, Facebook пытается стать более похожей на Twitter, чтобы переманить обратно утекающую в сеть микроблогов молодую аудиторию. Twitter считается куда более оперативным ресурсом получения информации, и детище Цукерберга хочет сразиться с соцсетью за звание лучшего информатора ***(Интересные записи от Facebook // IT Бизнес (http://itua.info/business/36459.html). – 2013. – 9.08).***

***

Специалисты по программированию из Рочестерского университета разработали приложение, помогающее избежать интоксикации. Сервис, получивший название nEmesis, проводит анализ твитов пользователей соцсети, публикует названия заведения, где посетители столкнулись с низким качеством блюд, пишет NovostiUA (http://novostiua.net/obschestvo/42699-tvitter-podskazhet-v-kakoe-kafe-luchshe-ne-hodit.html).

За четыре месяца своей работы в текущем году программа уже доказала свою актуальность и состоятельность. Схема программы очень проста. Если какой-нибудь житель Нью-Йорка посещает одно из 25 тыс. кафе, находящихся в городе, в течение нескольких следующих дней приложение мониторит сообщения этого пользователя на предмет ключевых слов о пищевом отравлении.

За период тестирования программа проанализировала в общем числе около 3,8 млн различных твитов. шесть тыс. из них содержали слова о состоянии желудочно-кишечной системы. В итоге, программисты смогли составить список из 120 мест, которые имели связь с хотя бы одним случаем острого кишечного отравления. Причем, рейтинг кафе, который составляет nEmesis, близок к оценкам экспертов из департамента здравоохранения Нью-Йорка.

Пока сервис обслуживает лишь один город. Но вскоре поле его деятельности может значительно расшириться. В ноябре создатели программы отправляются на конференцию в Калифорнию, где сервис представят ученым.

Единственным недостатком программы остается то, что пользователи могут специально негативно отзываться о каком-либо кафе ***(Twitter подскажет, в какое кафе лучше не ходить // NovostiUA (http://novostiua.net/obschestvo/42699-tvitter-podskazhet-v-kakoe-kafe-luchshe-ne-hodit.html). – 2013. – 8.08).***

***

Кожну публікацію користувачів Facebook бачать в середньому 35 % їхніх друзів, показало дослідження Стенфордського університету.

Дослідження показало, що публікації, які не отримують коментарів та лайків, менш видимі – їх усередньому бачать 28,9 % друзів автора. Протягом місяця у кожного з досліджуваних користувачів була хоча б одна популярна публікація – яку в середньому побачили 61 % їхніх друзів (щоправда, досліджування проводилося до зміни алгоритму відображення контенту в стрічці новин).

Дослідження виявило, що користувачі, як правило, недооцінюють свою аудиторію у Facebook. Досліджувані користувачі вірили, що в середньому кожен їхній пост бачать приблизно 60 друзів – водночас реально бачать у середньому 99 друзів. Крім того, виявилося, що пости 95 % досліджуваних протягом місяця лайкали менш ніж 40 друзів, коментували менш ніж 18.

Під час дослідження вивчали пости 220 000 користувачів за червень 2012 р., у кожного в середньому було по 266 друзів. «Побаченим» вважався пост, який був у видимій частині стрічки новин когось із друзів хоча б 900 мілісекунд ***(Ваші пости у Facebook бачить лише кожен 3-й друг // UkrainianWatcher (http://watcher.com.ua/2013/08/13/vashi–posty–u–facebook–bachyt–lyshe–kozhen–3–y–druh/). – 2013 – 13.08).***

***

Крупнейшая в мире соцсеть Facebook начала тестировать в США функцию отображения популярных на данный момент тем (трендов), пишет техноблог Mashable.

Отслеживание трендов является типовой функцией Twitter – сервис микроблогов в реальном времени обновляет десятку наиболее обсуждаемых тем, пользователей и хэштегов, позволяя фильтровать их географически. Компания Google также поддерживает список трендов в своей соцсети Google+, и кроме того позволяет просмотреть список быстрорастущих запросов к своему поисковику и наиболее популярные YouTube-ролики.

«Сегодня мы начинаем ограниченное тестирование функции, которая отображает тренды Facebook», – сообщил Mashable представитель соцсети. По его словам, функционал сейчас доступен лишь небольшому числу пользователей в США, которые пользуются мобильным веб-сайтом Facebook. Соцсеть отмечает, что инструмент находится на ранней стадии разработки, и отказалась сообщить, планируется ли более широкий запуск.

Пользователи, которые вошли в тестовую группу, увидят в ленте новостей выделенный блок с одним или несколькими трендами (именами людей, событиями, названиями фильмов и т. д.). При нажатии на любой из них он увидит записи с упоминанием этой темы от других пользователей, включая тех, на обновления которых он не подписан.

В июне этого года Facebook сообщила о планах запуска серии функций, которые позволят отследить интересные публичные дискуссии о крупных событиях, известных людях или «горячих» темах. Первым из таких инструментов стали кликабельные хэштеги. Запуск таких функций может свидетельствовать об усиливающейся борьбе между Facebook и Twitter за время, проводимое пользователями на сайте, за внимание знаменитостей к ресурсу, а также за рекламные бюджеты компаний ***(Facebook начала тестировать функцию отслеживания трендов в США // Marketing Media Review (http://mmr.ua/news/id/facebook-nachala-testirovat-funkciju-otslezhivanija-trendov-v-ssha-35767/). – 2013. – 9.08).***

***

Социальная сеть Facebook приобрела технологии и команду питтсбургской Mobile Technologies, разработчика приложения Jibbigo, способного распознавать устную речь и переводить ее на другие языки. Последняя покупка Facebook могла бы помочь пользователям из разных стран общаться, несмотря на языковой барьер, сообщает телеканал «Россия 24».

Приложение, позволяющее записать голосовое сообщение на одном из 20 возможных языков и перевести его на другой, было запущено в 2009 г. Jibbigo. Разработанное для iOS и Android, оно оказалось полезным спутником для путешественников и быстро стало серьезной мобильной альтернативой классическим разговорникам.

Монетизация Jibbigo заключалась в возможности приобрести платную оффлайн-версию приложения, позволяющую понимать иностранную речь без необходимости подключения к Интернету.

По данным издания TechCrunch, члены команды Mobile Technologies присоединятся к команде разработчиков Facebook, однако в компании отказались уточнять, сколько конкретно человек перейдут в соцсеть. Также не разглашаются и прочие условия сделки.

Крупнейшая в мире социальная сеть может сделать многое, используя новую технологию. Когда-нибудь может появиться мультиязычный чат, голосовой перевод для путешествующих пользователей Facebook или возможность перевода постов на другие языки.

Ранее в американской социальной сети использовались технологии Bing от Microsoft. Внедрение новой технологии сможет дать больший контроль, необходимый, чтобы сделать функцию перевода более важной частью Facebook.

Миссия социальной сети включает в себя установление более тесной связи между людьми по всему миру. Серьезным препятствием здесь является разнообразие языков, на которых мы говорим и пишем. И, похоже, в Facebook нашли способ, как его преодолеть ***(Языковой барьер в Facebook исчезнет: Соцсеть купила переводчика с устной речи // Подробности.UA (http://podrobnosti.ua/internet/2013/08/13/923386.html). – 2013. – 13.08).***

***

Социальная сеть Facebook тестирует специальный мобильный клиент, предназначенный только для звезд. Об этом сообщает All Things Digital.

По данным издания, некоторые знаменитости уже получили доступ к VIP-приложению. Оно позволяет им следить за обсуждением своей личности в соцсети и отвечать фанатам.

Приложение, отмечает All Things Digital, является частью кампании Facebook по увеличению активности звезд в соцсети. Представители Facebook подтвердили изданию, что новое приложение действительно тестируется на небольшой группе пользователей. Подробности они пообещали рассказать позднее.

Как указывает All Things Digital, у конкурента Facebook, сервиса микроблогов Twitter общение с фанатами устроено проще – звездам достаточно открыть отдельную вкладку с ответами. Кроме того, существует стороннее приложение WhoSay, позволяющее знаменитостям следить за обсуждением своей личности сразу в нескольких соцсетях – Facebook, Twitter, Instagram и Tumblr ***(СМИ узнали о VIP-приложении Facebook // Версии.com (http://www.versii.com.ua/news/284840/). – 2013. – 15.08).***

***

Сервис микроблогов Twitter запустил новый блок, позволяющий отслеживать ссылки от СМИ на твиты. Блок получил название «связанные

темы». Об этом сообщили в блоге компании.

Теперь пользователи, ретвитнувшие запись на своей странице, увидят, какие СМИ ранее делились этим же твитом. Блок будет виден только по постоянной ссылке, а не в самой ленте Twitter.

В Twitter надеются, что с появлением функции связанных тем, новостные сюжеты станут полнее. По мнению разработчиков, нововведение позволит поместить новость в медиа-контекст.

Twitter активно интегрирует свои тенхнические возможности со средствами массовой информации. Например, в декабре 2012 г. Twitter запустил систему измерений телерейтинга в сотрудничестве с компанией Nielsen. В мае же этого года в тестовом режиме был представлен сервис, который отслеживает популярные в данный момент у пользователей телепередачи ***(Twitter запустил сервис отслеживания ссылок // InternetUA (http://internetua.com/Twitter-zapustil-servis-otslejivaniya-ssilok). – 2013. – 20.08).***

***

На початку серпня Facebook презентував нову опцію – можливість вставляти пости з соцмережі на сторонні сайти.

У Facebook також повідомили, що тепер вони додали можливість програвати відео, вставлене у пост на сторонньому сайті. Такий пост має ті самі характеристики й можливості, що й базовий запис у Facebook. Ви можете лайкнути його, поділитись, залайкати сторінку. Проте для коментування вас буде перенаправлено на сайт.

Вставляти можна лише записи, які мають публічний статус. Якщо запис має якісь обмеження (наприклад, бачити його можуть лише друзі) – вставити його буде не можливо.

Можливість вставляти пости з Facebook на сторонніх сайтах стала доступною для всіх користувачів. Щоб вставити запис, необхідно натиснути на «галочку» у правому верхньому кутку і у випадаючому меню обрати embed post (опція для більшості наразі недоступна). Далі скопіювати html-код, та вставити в себе на сайті.

Аналогічна технологія була реалізована у Twitter ще в 2010 р., а потім скопійована у Instagram ***(Можливість вставляти пости з Facebook на сторонніх сайтах стала доступною для всіх користувачів // UkrainianWatcher (http://watcher.com.ua/2013/08/22/mozhlyvist-vstavlyaty-posty-z-facebook-na-storonnih-saytah-stala-dostupnoyu-dlya-vsih-korystuvachiv/). – 2013. – 22.08).***

***

Після того, як Facebook запустив відео в Instagram, кількість розшарених відео з Vine (відео-сервіс від Twitter) зменшилася майже втричі.

Нагадаємо, у січні 2013 р. Twitter запустив мобільний сервіс Vine, який дозволяє користувачам створювати та поширювати короткі (до шести

секунд) циклічні відео, схожі на GIF-зображення. У червні цього року в Instagram додали можливість записувати відео до 15 сек., застосовувати до нього різні фільтри та публікувати точно так само, як і фото.

Одразу було зрозуміло, що відео в Instagram стане прямим конкурентом Vine, але невідомо було, хто стане успішнішим і на скільки. Наразі можна стверджувати, що, принаймні тимчасово, але відео в Instagram успішно витісняє з ринку відео з Vine ***(Костинян М. Запуск відео в Instagram таки сильно вдарив по Vine // UkrainianWatcher (http://watcher.com.ua/2013/08/15/zapusk-video-v-instagram-taky-sylno-vdaryv-po-vine/). – 2013. – 15.08).***

***

Социальная сеть «Одноклассники», проект Mail.Ru Group, объявила об обновлении своего приложения для iOS-устройств до версии 4.0.

Основные изменения коснулись навигации в приложении и просмотра фотографий. После обновления в приложении «Одноклассников» появилось боковое меню, вызвать которое можно как с помощью кнопки, так и с помощью простого жеста вправо. В боковом меню сосредоточены все разделы сайта. Там же расположен новый музыкальный мини-плеер, с помощью которого можно управлять музыкой, не отвлекаясь от общения с друзьями или просмотра ленты.

Также был улучшен просмотр фотографий. Галерея с альбомами получила абсолютно новый дизайн. Открыв альбом, пользователь увидит все фотографии в виде плитки. Перемещаться между фотографиями можно с помощью жестов, а комментировать и «Классить!» фотографии стало легче и удобнее.

Кроме того, при скролле содержимого в любом из разделов нижняя и верхняя панели навигации исчезнут с экрана, предоставляя больше пространства для просмотра интересного контента.

«Приложения для мобильных устройств, как и мобильная версия “Одноклассников”, всегда были для нас одними из самых приоритетных продуктов. С каждым днем все больше людей используют мобильные устройства для входа в социальную сеть. Именно поэтому мы подходим к работе над этими продуктами столь тщательно. В ближайшее время мы обновим наши приложения и для других мобильных платформ», – сказал руководитель бизнес-подразделения «Социальные сети» Mail.Ru Group И. Широков ***(«Одноклассники» обновили приложение для iOS // InternetUA (http://internetua.com/odnoklassniki--obnovili-prilojenie-dlya-iOS). – 2013. – 23.08).***

***

Социальная сеть Foursquare запустила функцию сбора деловой информации с помощью вопросов, появляющихся после чекина, сообщает компания.

Сервис Foursquare позволяет не только отмечаться в определенных местах, но и предоставляет краткую контактную информацию общественных мест, например телефон и адрес. Кроме того, пользователи могут оставить общедоступные подсказки и советы о заведении, которое они посетили.

В рамках нового функционала Foursquare будет задавать пользователю вопросы о посещенных местах, например, имеет ли ресторан открытую веранду, принимает ли кредитные карты и насколько быстро производит доставку. Вопросы будут появляться по одному и не всегда сразу после чекина, чтобы не утомлять пользователей.

Данные, собранные таким образом, дополнят профили организаций внутри самого приложения Foursquare. Информация, наряду с отметкой на карте и контактами, будет отображаться над пользовательскими подсказками.

Обновление было представлено пользователям Android несколько дней назад и теперь доступно для iOS.

База пользователей Foursquare на сегодня составляет 35 млн человек, однако рост количества чекинов резко замедлился. Пользователи продолжают использовать Foursquare для получения информации о заведениях, но интерес к чекинам и «войнам за должность мэра» снизился. Компания сообщала о пяти миллионах чекинов ежедневно – показатель не изменился с прошлого года.

Ранее американский конкурент Foursquare сервис Yelp, предоставляющий информацию о заведениях поблизости, запустил возможность оставлять комментарии с мобильных устройств. Подобные сервисы от Google, Square, Groupon и Facebook также фокусируются на сборе информации от пользователей, посетивших общественные места.

Foursquare (сокращённо 4sq) – социальная сеть с функцией определения геопозиции, предназначенная для работы с мобильных устройств. Сервис доступен не только для устройств с GPS-навигацией, но и для любых сотовых телефонов ***(Foursquare будет собирать бизнес-информацию после чекина // InternetUA (http://internetua.com/Foursquare-budet-sobirat-biznes-informaciua-posle-csekina). – 2013. – 23.08).***

***

Социальная сеть для делового общения LinkedIn откроет возможность регистрации для школьников. Новый раздел – University Pages – объединит студентов, выпускников вузов и старшеклассников. По мнению создателей, площадка LinkedIn теперь поможет найти свое призвание молодым людям. Колледжи и университеты, которые хотели бы рассказать о своей работе абитуриентам, студентам и сообществу выпускников, разместят информацию о себе в подрубрике University Pages. На «стене» учебного заведения в соцсети можно будет «побродить» по аудиториям и коридорам вуза, почитать новости от выпускников и узнать о предстоящих мероприятиях ***(В LinkedIn пустят учеников средней школы // InternetUA***

(http://internetua.com/v-LinkedIn-pustyat-ucsenikov-srednei-shkoli). – 2013. – 23.08).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Администрация Президента Украины открыла свою официальную страницу в социальной сети Facebook. Официальное представительство доступно по адресу: https://www.facebook.com/president.gov.ua, сообщает пресс-служба главы государства.

«Для персонализации страницы в Facebook выбран штандарт Президента Украины с изображением золотого трезуба. Заглавное фото на странице будет меняться. Сегодня на его месте – поздравление с Днем Независимости Украины», – отмечается в сообщении.

На странице опубликовано видеообращение Президента по случаю Дня Независимости, материалы с сегодняшних торжественных мероприятий при участии Президента, информационные сообщения и инфографика основных шагов Украины в направлении евроинтеграции.

В специальном приложении «Доступ к публичной информации» на Официальном представительстве АПУ в Facebook предусмотрена возможность оформления запроса на получение публичной информации в режиме онлайн. Все запросы автоматически передаются в Главное управление доступа к публичной информации, которое в законодательно определенные сроки рассмотрит их и даст ответ.

В приложении «Обращения граждан» пошагово описывается законодательно утвержденная процедура оформления обращений граждан к главе государства в письменном виде.

Сопровождение официальной страницы будет осуществлять Главное управление пресс-службы и коммуникаций Президента Украины ***(Администрация Президента Украины появилась в сети Facebook // InternetUA (http://internetua.com/administraciya-prezidenta-ukraini-poyavilas-v-seti-Facebook). – 2013. – 24.08).***

***

Самыми активными пользователями соцсетей среди мэров украинских городов являются городские головы Харькова, Днепропетровска, Одессы, Львова и Сум. Об этом свидетельствуют результаты исследования корреспондентов Укринформа, пишет «Обозреватель» (http://tech.obozrevatel.com/news/07649-nazvanyi-samyie-aktivnyie-v-sotssetyah-meryi-ukrainskih-gorodov.htm).

Г. Кернес, И. Куличенко, А. Костусев, А. Садовый и Г. Минаев имеют в соцсетях по 18, 15, 10, и 7,5 тыс. друзей соответственно. Такая интегрированность в интернет-пространство позволяет чиновникам

размещать больше информации, в том числе неофициального характера, вести дискуссии, получать вопросы и замечания пользователей, в конце концов, знать, что о них люди думают...

В соцсетях у харьковского городского головы Г. Кернеса появляются три–четыре оригинальных фотоснимка, на которых городской голова сфотографирован с друзьями, в семейном кругу, во время занятий спортом или на отдыхе. В комментариях харьковчане довольно часто просят Г. Кернеса помочь в решении той или иной проблемы.

Большой активностью в соцсетях отличается городской голова Одессы А. Костусев. Он единственный мэр, на страницу которого в Facebook можно попасть не из поисковой системы, а просто с сайта городского совета. Самой любимой темой одесского головы является снос незаконных зданий, расположенных на берегу моря. А. Костусев охотно участвует в таких операциях, размещая фоторепортажи.

На страницах главы Днепропетровска И. Кулиниченко размещены преимущественно новости культурной жизни города с фотографиями, а также анонсы рабочих совещаний и событий, есть сообщения, содержащие полезную для горожан информацию относительно медицинской реформы, ЖКХ. Однако личное присутствие мэра незаметно. Очевидно, что ведет страницу не он сам, а его пресс-служба.

Городской глава Львова А. Садовый использует свою страницу в Facebook для обнародования как официальной так и личной информации, .

У мэра Сум Г. Минаева есть своя страница в Facebook, «ВКонтакте», персональный сайт и аккаунт в Twitter. Особенно активно использует Facebook, где ежедневно по несколько часов общается с пользователями на различные темы. С целью привлечения к соцсети чиновников горисполкома Г. Минаев нередко общается со своими подчиненными именно при помощи Facebook.

У мэра Тернополя С. Надала целых два аккаунта в Facebook. Активность на персональной странице высокая, во всяком случае мэр пытается комментировать наиболее характерные вопросы и давать ответы на письма отдельных посетителей. Другую страницу – также под его именем – создали в начале марта этого года, потому что у предыдущей иссяк лимит друзей (их было 5 тыс.). Хотя к администрированию этой страницы приобщаются работники пресс-службы мэрии, уточнила пресс-секретарь городского совета.

У мэра Луганска С. Кравченко в Facebook 2172 друга. Все записи сделаны от первого лица, но судя по тому, что все они посвящены официальным событиям, то, скорее всего, заполняет страницу пресс-служба мэра. Обратной связи к комментариям нет, но и комментариев немного.

Собственную страницу месяц назад открыл Симферопольский городской голова В. Агеев. На сегодняшний день у него 1706 друзей. Записи пользователей касаются жалоб на плохие дороги, ЖЭКи и тому подобное.

Недавно персональную страницу в Facebook создал городской голова

Житомира В. Дебой и личную, без указания должности – городской голова Ривне В. Хомко. У одного зарегистрированы 143 друга, у другого – 69. В. Дебой размещает на странице главным образом поздравления с праздниками, но и те – нерегулярно: последнее поступило 6 июня, на День журналиста. Небольшое количество друзей господин В. Хомко объясняет фильтрацией.

Винницкий мэр В. Гройсман хоть и не имеет страниц в соцсетях, однако утверждает, что общается с винничанами онлайн 24 часа в сутки. По словам мэра, чаще всего винничане жалуются на коммунальные проблемы, есть пожелания и благодарности.

В то же время 12 мэров не имеют ни одного аккаунта, предпочитая общаться со своими избирателями через официальные страницы городских советов. Это городские головы Луцка, Донецка, Ужгорода, Запорожья, Ивано-Франковска, Кировограда, Николаева, Полтавы, Херсона, Хмельницкого, Черновцов, Чернигова. Все они говорят о нехватке времени ***(Названы самые активные в соцсетях мэры украинских городов // Обозреватель (http://tech.obozrevatel.com/news/07649-nazvanyi-samyie-aktivnyie-v-sotssetyah-meryi-ukrainskih-gorodov.htm). – 2013. –6.08).***

***

Вісім голів облдержадміністрацій і два голови облрад мають свої акаунти та сторінки в соцмережах. Найактивніші користувачі – С. Татусяк, М. Вишиванюк і М. Добкін. Про це повідомляє Укрінформ за результатами моніторингу в регіонах.

За кількістю друзів – більше як 4 тис. – лідирує голова Вінницької облради С. Татусяк. Він присутній в усіх популярних соцмережах. Йому можна написати в «Одноклассники», «ВКонтакте», Facebook і Twitter. Глава депутатського корпусу виставляє свої фотографії з численних поїздок по Європі, де спілкується з друзями Вінницької області, починає нові проекти, налагоджує контакти із зарубіжними фондами. З його віртуальних сторінок можна дізнатися, що він любить слухати В. Цоя, цінує мистецтво кіно та обожнює висловлювання великих і просто мудрих людей. На його стіні розміщено 15 найкращих цитат, що змінили життя, 50 звичок сильних людей, п’ять простих правил та ін. С. Татусяк часто коментує сторінки друзів, «лайкає» на їх коментарі і новині, робить це з душею, а головне, сам, без допомоги прес-служби.

Більш як 3 тис. друзів має у Facebook голова Івано-Франківської облдержадміністрації М. Вишиванюк. Інформація тут більш офіційна, але відвідувачі можуть залишити критичні зауваження, що стосуються стану шкіл, доріг тощо.

Близько 3 тис. друзів зареєстровано у голови Харківської ОДА М. Добкіна в Twitter. Судячи із записів, він пишається командою «Металіст», реагує на резонансні події в країні («врадіївську ходу», волинську трагедію, проблеми з міліцією). Останні записи – з риболовлі в Астрахані. Тут же розміщено фото

з сомом, який дістає М. Добкіну до плеча.

Голова Львівської ОДА В. Шемчук має свій акаунт у Facebook, на якому зареєстровано 2273 друзів. Тут чиновник регулярно розміщує свої фотографії з різних подій. Їх більш як 6 тис. Остання фотосесія – з Підгородецького замку, нинішній стан якого вимагає багатьох коштів і державної уваги. «Така краса! Образливо … Але не безнадійно:-)» – прокоментував підбірку В. Шемчук.

Близько тисячі послідовників має сторінка голови Луганської облради В. Голенка у Facebook. Ведеться вона від першої особи, але всі теми офіціозні, безпосередньо пов'язані з діяльністю в обласній раді. Коментарів під записами небагато, серед них зустрічаються як схвальні, так і гнівні. Коментаторам В. Голенко, як правило, не відповідає.

Голова Луганської облдержадміністрації В. Пристюк також має сторінку у Facebook. Тут викладається офіційна інформація про поїздки В. Пристюка, його прийоми населення, гарячу лінію тощо. Активність 316 друзів при цьому невисока – два–п'ять коментарів під кожним записом, в основному, позитивні, з похвалами на адресу губернатора.

Голова Сумської ОДА Ю. Чмирь має свою сторінку у Facebook, яка подобається 645 користувачам. Пише на ній більш-менш регулярно про найбільш резонансні події в області, проте в полеміку не вступає. Має також свій персональний сайт.

Акаунти у Facebook мають голови Закарпатської ОДА О. Леліда та Рівненської ОДА В. Берташ. У першого – 104 друзів і останнє оновлення – 8 травня. У другого, крім офіційного портрета і 176 друзів, нічого не представлено.

Голова Одеської ОДА Е. Матвійчук має персональний сайт, де дублюються повідомлення з сайту облдержадміністрації.

У соцмережах не зареєстровані ні голова Верховної Ради АРК В. Константинов, ні голова Ради міністрів АРК А. Могильов.

Не представлені там також чиновники Волинської, Донецької, Дніпропетровської, Житомирської, Запорізької, Кіровоградської, Миколаївської, Полтавської, Тернопільської, Чернігівської, Черкаської, Чернівецької, Херсонської, Хмельницької областей ***(Татусяк, Добкін та Вишиванюк – найактивніші обласні чиновники в соціальних мережах // ВінницяОk (http://vinnitsaok.com.ua/dobkin-tatusyak-ta-vyshyvanyuk-najaktyvnishi-oblasni-chynovnyky-v-sotsialnyh-merezhah-114448.html). – 2013. – 14.08).***

***

«Группа в поддержку Андрея Шкиля» создана в социальной сети Facebook. Авторы новой странички призывают всех неравнодушных зайти на нее и оставить свой лайк – виртуальную подпись в поддержку обращения к властям Франции о предоставлении А. Шкилю политического убежища, пишет «Обозреватель» (http://obozrevatel.com/politics/71963-na-fejsbuke-

sozdana-gruppa-v-podderzhku-shkilya.htm).

«Обозреватель» не раз писал о судьбе этого политика. В конце 2012 г. А. Шкиль был вынужден покинуть Украину, так как после завершения депутатской каденции он стал уязвимым для преследований со стороны правоохранительных органов. Дело в том, что еще в 2001 г. против А. Шкиля было возбуждено уголовное дело за участие в движении «Украина без Кучмы». Тогда, он был арестован и провел 13 месяцев в тюрьме. В 2002 г. его освободили в связи с избранием его народным депутатом. Однако последующее десятилетие не изменило юридической судьбы его уголовного дела: оно по-прежнему существует и в любой момент ему может быть дан ход.

Понимая это, А. Шкиль выехал за границу, пополнив, таким образом, ряды политэмигрантов последнего поколения. На сегодняшний день политик находится в Париже и ожидает решения французских властей. А интернет-общественность демонстрирует ему свою поддержку.

«Друзі! Ті, кому не байдужа доля А. Шкіля, створили цю сторінку та запрошують вас відвідати її. Кожен ваш лайк може перехилити шальки терезів у необхідний Андрієві бік. Ми просимо про моральну підтримку, яка є неоціненною у данній ситуації.

Почнемо відразу з головного: А. Шкіль перебуває у Франції, де чекає на рішення місцевої влади з приводу надання йому політичного притулку. Наше завдання, зібравши якомога більше підписів на підтримку А. Шкіля, довести Франції, що небезпека для нього існує», – говориться в обращении, размещенном на страничке «Группы поддержки».

За первые три дня существования «Группа в поддержку А. Шкиля» собрала около 400 подписей ***(На Facebook создана группа в поддержку Шкиля // Обозреватель (http://obozrevatel.com/politics/71963-na-fejsbuke-sozdana-gruppa-v-podderzhku-shkilya.htm). – 2013. – 6.08).***

***

Продовження «ямної» історії у соцмережах – цілком логічне після розмальовування вибоїн на дорогах у Черкасах і Горлівці. Там активісти обмальовували та ставили загородження біля особливо капосних і роками не латаних дірок. Тут треба віддати належне мешканцям російського Єкатеринбурга – саме вони першими почали малювати карикатури на чиновників прямо на дорогах міста. Комунальники реагували оперативно – вже на наступний день усе латалося та кроїлося… Щоправда, нашим активістам у Горлівці штраф «упаяли» за самоуправу…

Але ж тепер народні умільці знайшли дешевий та абсолютно не витратний спосіб. Головне – можливості невичерпні! Не прибирають сміття у дворі – відкривай сторінку для Купи Бруду. Немає гарячої води другий місяць – сфотографуй домашню сантехніку та підпиши: «Сумую за теплом!» Машини паркуються на дитячому майданчику – створюємо спільноту «А колись тут катался на гойдалці!». Єдиний нюанс – не забувати запрошувати до

спільноти керівників комунальних служб і чиновників вищого рангу. Правда, є імовірність, що всі вони незабаром закриють свої сторінки в соцмережах, коли кількість друзів-ям перевищить живих людей… Але хоч якусь частину дірок залатати встигнемо! ***(У комунальників – новий головний біль: соцмережі оголосили їм війну // ПІК (http://www.pic.com.ua/u-komunalnykiv-novyj-holovnyj-bil-sotsmerezhi-oholosyly-jim-vijnu.html). – 2013. – 5.08).***

***

Новый посол США в Украине Д. Пайетт пообещал регулярно отвечать на вопросы украинцев в своем видеоблоге. Об этом он заявил в видеоролике, который подготовило киевское посольство США специально для того, чтобы познакомить украинцев с новым послом, пишет «Обозреватель» (http://obozrevatel.com/politics/68507-novyij-posol-ssha-budet-obschatsya-s-ukraintsami-v-facebook.htm).

В видеоролике Д. Пайетт рассказал о своей семье, родном штате Калифорния и увлечениях.

«Я мечтаю увидеть Крым, про который мне рассказывали, что он столь же удивительный (как и его родной штат. – Ред.). Я люблю кататься на лыжах и ходить пешком. И планирую уже очень скоро исследовать склоны Карпатских гор», – признался Д. Пайетт.

Новый посол, за спиной которого 24 года дипломатической службы, заявил, что намерен оберегать стратегическое партнерство Украины и США, а также поддерживать демократические стремления украинского народа.

«Я хочу выяснить, как мы можем использовать социальные медиа, чтобы развивать наши отношения. Мне понравилась подборка на Facebook посольства США, которая рассказывает об известных американцах украинского происхождения. Я хочу услышать вас и приглашаю задать свой видеовопрос на странице Facebook посольства. Я буду регулярно отвечать на вопросы в моем видеоблоге», – сказал Д. Пайетт… ***(Новый посол США будет общаться с украинцами в Facebook // Обозреватель (http://obozrevatel.com/politics/68507-novyij-posol-ssha-budet-obschatsya-s-ukraintsami-v-facebook.htm). – 2013. – 7.08).***

***

Государственной судебной администрацией Украины создана страница «Судебная власть Украины» на Facebook.

Председатель Государственной судебной администрации Украины Р. Кирилюк: «Глобальная информатизация и, как следствие, значительное расширение коммуникационных возможностей в деятельности различных общественных институтов, сделали насущной необходимостью создания на Facebook страницы “Судебная власть Украины”.

Сегодня общественные интересы и предпочтения перешли в плоскость социальных сетей, и активность их пользователей побудили нас создать свой аккаунт.

Уже несколько лет существует профессиональная социальная сеть “Фемида”, созданная для судей, работников аппаратов судов, собственно, для специалистов судебной власти. Вместе с тем, по нашему мнению, пора выйти на более широкий круг потребителей новостей, видений, событий судебной власти Украины.

Интересным является и то, что Facebook имеет много интересных возможностей, в частности, проведение опросов, измерения “популярности” страницы, учета предпочтений пользователей, другое.

Сейчас Facebook является одной из самых массовых и популярных социальных сетей мира. Сегодня 1,2 млрд пользователей зарегистрировали здесь свои профили. Надеемся, что какая-то часть из них заинтересуется страницей “Судебная власть Украины”, ведь это отличный способ распространить правдивую, адекватную, точную и своевременную информацию о деятельности судебной власти» ***(Государственной судебной администрацией Украины создана страница «Судебная власть Украины» на Facebook // Судебно-юридическая газета (http://sud.ua/news/2013/08/07/52855-gosydarstvennoj-sydebnoj-administratsiej-ykraini-sozdana-stranitsa-sydebnaya-vlast-ykraini-na-facebook). – 2013. – 7.08).***

***

Премьер-министр Н. Азаров в ближайшее время посетит Луганскую и Ивано-Франковскую области, а с осени готовится целый ряд поездок в регионы. При этом он будет планировать поездки в регионы с учетом сообщений пользователей Facebook, сообщил Премьер на своей странице в соцсети.

«Готовится моя поездка в Луганск и Ивано-Франковск. Они состоятся в ближайшее время. Я хотел бы знать мнение своих корреспондентов из этих областей о том, на какие проблемы они бы советовали мне обратить больше всего внимания. На осень будет запланирован целый ряд поездок по стране, и я буду всех заранее информировать, чтобы можно было строить план поездки с учетом тех критических моментов, на которые вы мне укажете. Я вам заранее благодарен за эту помощь», – отметил Премьер-министр ***(Азаров будет совещаться по поводу своих поездок с фейсбучными френдами // Провокация (http://provokator.com.ua/2013/08/11/azarov-budet-soveshhatsya-po-povodu-svoih-poezdok-s-feysbuchnyimi-frendami/). – 2013. – 11.08).***

***

Сегодня в мире насчитывается около 500 млн пользователей Twitter, и это число продолжает неуклонно расти. Журналистка Foreign Policy М. Хэннан воспользовалась аналитическими сервисами Klout (оценивает степень влиятельности пользователя по реакции на его твиты), TweepsMap (определяет географию фолловеров), TweetPsych (сравнивает твиты пользователя со среднестатистическими) и TopTweet (определяет самый популярный твит), чтобы получить полное представление о Twitter-аккаунтах

восьми самых влиятельных политических деятелей мира.

Самым влиятельным политиком в Twitter оказался Б. Обама. Его результат в Klout – 99, что выше, чем у таких «тяжеловесов», как Д. Бибер (96) и Леди Гага (95). Судя по активности в микроблоге, Б. Обама – трудоголик, он пишет о работе и занятости в 3,38 раза чаще, чем среднестатистический пользователь, приводит статистику автор исследования.

Сервис TopTweet ошибочно называет самым популярным твитом американского президента запись «Да, мы можем», сделанную в марте 2010 г. после принятия закона «О доступной медицинской помощи». На самом деле, наибольшую известность приобрел твит «Еще четыре года», сделанный после переизбрания Б. Обамы на второй срок.

Британскому премьеру Д. Кэмерону до Б. Обамы еще далеко: показатель его влиятельности равен 92, говорится в статье. При этом для главы британского правительства регистрация в Twitter стала суровым столкновением с реальностью. Отныне все замечания о его политике и лишнем весе критики направляют прямо ему. Некоторые комментарии попадают даже в передовицы британских газет. «Интернет-тролли – мои новые любимцы», – пошутил Д. Кэмерон перед журналистами.

Если верить докладу «Твипломатия» (Twiplomacy), самый влиятельный лидер Twitter-вселенной – Папа Римский Франциск. Показатель влиятельности его англоязычного аккаунта всего 89, однако следует учесть, что у него также есть учетные записи на немецком, французском, польском, испанском, итальянском, арабском языках, а также на латыни.

Самым популярным твитом понтифика стала самая первая запись. «Дорогие друзья, сердечно вас благодарю и прошу продолжать молиться за меня», – написал он вскоре после того, как конклав избрал его главой Католической церкви.

После прошлогоднего скандала, когда гражданская жена Ф. Олланда нелицеприятно отозвалась в микроблоге о его бывшей супруге, французский президент забросил свой аккаунт в Twitter. Тем не менее, показатель влиятельности хозяина Елисейского дворца равен 87, сообщает журналистка.

Самый популярный твит Ф. Олланд опубликовал сразу после победы над Н. Саркози на президентских выборах 2012 г. «Моя миссия, мой долг – служить Республике, служить Франции!» – написал на радостях новоизбранный президент.

Премьер-министр Израиля Б. Нетаньяху пишет не часто, зато использует хэштеги. Его результат – 87. Б. Нетаньяху – единственный лидер в списке, у которого за рубежом больше фолловеров, чем в родной стране. Самая популярная запись в микроблоге появилась во время последнего вооруженного противостояния Израиля с палестинцами в Секторе Газа. «#Террористы из #Газы совершают двойное #военное #преступление. Они стреляют по израильскому мирному населению и прячутся за #палестинскими мирными жителями», – написал он в ноябре 2012 г.

Д. Медведев – активный пользователь социальных сетей с аккаунтами в

Twitter, Facebook и Instagram. «Помните, даже если вы читаете российского премьер-министра в Twitter, это еще не значит, что вы с ним друзья», предостерегает читателей журналистка, намекая на мартовское заявление его пресс-секретаря. «Он вам не Димон, – раскритиковала тогда интернет-пользователей Н. Тимакова. – Он – глава правительства».

Влиятельность Д. Медведева сервис Klout оценил в 86 баллов. Его лучший товарищ в сети – А. Шварценеггер. Приятели даже обсуждали в Twitter планы совместного отпуска на горнолыжном курорте. TwitterPsych показал, что Д. Медведев часто пишет о «контроле». Возможно, сказывается политическая жизнь в тени В. Путина, строит догадки журналистка.

Еще один активный пользователь Twitter – президент Аргентины К. Фернандес де Киршнер. Однажды она написала 161 твит за девять часов, сообщает Хэннан. По меткому выражению журналистов The Economist, ограничение в 140 знаков для нее – часть системы сдержек и противовесов.

Замыкает список премьер-министр Индии М. Сингх. Руководителя индийского правительства иногда критикуют за боязнь камер и необщительность, однако в Twitter его дела не так уж и плохи, говорится в статье: имея 700 тыс. подписчиков микроблога, он может похвастаться уровнем влиятельности в 80 баллов ***(Названы самые влиятельные пользователи Twitter // Utro.ua (http://www.utro.ua/ru/zhizn/nazvany_samye_vliyatelnye_polzovateli_twitter1376398660). – 2013. – 13.08).***

***

С начала года с помощью социальных сетей правоохранители разыскали 15 % без вести пропавших детей

Как сообщает корреспондент «Харьков. Комментарии» по информации пресс-службы МВД Украины, всего с начала года в милицию поступило более 3 720 заявлений об исчезновении детей, 471 ребенок был объявлен в розыск.

По состоянию на середину августа по «горячим следам» разыскали почти 3 200 детей.

Также в МВД отметили, что с работниками управления криминальной милиции по делам детей сотрудники управления по борьбе с киберпреступностью провели учебный семинар по розыску детей с помощью соцсетей.

Как показывает практика, дети, покидая свое место жительства, в большинстве случаев, сообщают через соцсети друг другу о своих намерениях, обмениваются информацией, что в дальнейшем может способствовать установлению их местонахождения, отмечают в МВД.

Кроме того, по их статусам, содержащимся на страницах соцсетей, можно определить психоэмоциональное состояние, направление их движения, желание встретиться с друзьями или знакомыми ***(Соцсети помогли милиции найти 15 % пропавших детей // Комментарии: Харьков***

(http://kharkov.comments.ua/news/2013/08/21/200240.html). – 2013. – 21.08).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Если Вы один из тех людей, которые не могут ни минуты прожить без социальных сетей, то этот первый Twitter-тематический в мире отель в Магалуфе, (Испания), станет идеальным местом для вас, пишут NovostiUA (http://novostiua.net/world/42546-pervyy-twitter-otel-v-mire.html).

Постоянно растущие требования клиентов, необходимость разнообразия и увеличения числа приверженцев социальных медиа по всему миру вдохновили компанию Melia Hotels International, ведущую гостиничную сеть в Испании, создать первый в мире Twitter-отель. Расположенный в Магалуфе этот отель SolWaveHouse позволяет гостям взаимодействовать с сотрудниками и другими туристами через текстовые сообщения длиной до 140 символов. Генеральный директор отеля Г. Эчеваррия говорит, что «отель сделал новый шаг в удовлетворении ожиданий клиентов при помощи новых технологий».

В основе этого социального медиа-тематического отеля лежит Wi-Fi. Как только посетители заходят на свои страницы в Twitter, они могут воспользоваться системой #SocialWave, чтобы общаться с другими туристами в чатах, обмениваться фотографиями и даже флиртовать, отправляя виртуальные поцелуи. Также к услугам гостей имеется два консьержа в Twitter, которые всегда готовы к удовлетворению просьб гостей через Twitter и ведут общение только в этом виртуальном мире ***(Первый Twitter отель в мире // NovostiUA (http://novostiua.net/world/42546-pervyy-twitter-otel-v-mire.html). – 2013. – 6.08.).***

***

Каждый год в сети появляются новые инструменты для анализа и мониторинга социальных сетей – Mashable.com не успевает делать обзоры. В прошлом месяце появился еще один стартап – SumAll, который тут же стал популярным. Мы решили составить список сервисов, которые появились за прошедшее полугодие 2013 г.

SumAll

Бесплатный и простой в использовании сервис для анализа активности компании в соцсетях и других площадках. Например, можно получить данные профиля компании даже в Amazon или eBay. В отличие от других бесплатных инструментов, имеет широкий выбор площадок для анализа: кроме Facebook, Twitter, Instagtram, есть еще WordPress, Google AdWords, Foursquare, Tumblr и др. Легко управляется с планшета, среди клиентов – TED, Starbucks и National Geographic.

Synomos

Инструмент сложный как в дизайне, так и в использовании, однако в

отличие от многих других, способен удовлетворить потребности крупных компаний. Можно зарегистрировать сразу несколько аккаунтов для smm-менеджера, администратора и ассистентов, сколько бы их ни было. Synomos вытаскивает данные из Twitter, LinkedIn, Facebook, YouTube, блогов и форумов.

В первый день запуска ресурс может показать статистику за последний месяц. Система сохраняет данные, пока вы остаетесь ее клиентом, т. е. неограниченное время. Программа также может работать с данными из Google Analytics и создавать из них buzzgraph.

UberVU

Инструмент предоставляет доступ к большому объему информации в очень сыром виде, но в компании уверены, что таким образом клиент сможет получить самые точные оценки кампании в СМИ и социальных медиа. Инструмент, можно сказать, «прослушивает» социальные сети в реальном времени – данные поступают мгновенно, в том числе об упоминаниях бренда. Мониторинг происходит на следующих площадках: блоги, новостные сайты, форумы, Facebook, Twitter, LinkedIn, YouTube Blogger ***(Новые инструменты для анализа соцсетей // Marketing Media Review (http://mmr.ua/news/id/novye-instrumenty-dlja-analiza-socsetej-35725/). – 2013. – 6.08).***

***

Известная социальная сеть подала заявку в «Роспатент» на регистрацию товарного знака vk.com для 19-ти различных видов продукции и услуг. Среди них лицензирование программного обеспечения, предоставление доступа на форумы в Интернете. Но в списке есть и непрофильные товары, в частности, презервативы, парфюмерия, кондитерские изделия, одежда и аксессуары, сообщает AIN.

В издании Hopes&Fears предположили, что одна из крупнейших российских социальных сетей таким образом пытается защитить свое доброе имя от предприимчивых бизнесменов, которые используют его в коммерческих целях. Так, в мае 2012 г. предприниматель И. Рогов патентовал презервативы «ВКонтакте». А А. Коротенко недавно выпустил на рынок мужские духи «ВКонтакте» по 250 рублей за флакон.

В 2011 г. в Роспатент поступила заявка от дистрибутора кондитерских изделий и кофе «Европа Фудс» на регистрацию товарного знака «ВКонтакте» для производства жевательной резинки и конфет. А годом ранее компании «Инвест парк» разрешили производить пиво и соки «ВКонтакте» и даже открывать под этим брендом гостиницы.

Очевидно, в компании П. Дурова постарались охватить все, что еще не было охвачено. Кроме вышеперечисленных товаров, соцсеть хочет получить право на выпуск фирменных бумажников, амулетов, рамок для фото, а также открытие дома отдыха, предоставление услуг бронирования билетов и даже услуг психологов ***(«ВКонтакте» выпустит презервативы, конфеты и***

одежду // MyTime (http://mytime.net.ua/news/2013/08/2013-08-07-65.htm). – 2013. – 7.08).

***

Twitter способен существенно увеличить рейтинг телевизионных передач благодаря тому, что большинство пользователей сети заходит на свои страницы как раз во время просмотра телевидения. Таковы результаты исследования агентства Nielsen, передает IT Expert со ссылкой на агентство «РБК-Украина».

Комментарии, которые телезрители оставляют в социальных медиа, способны существенно увеличить рейтинги программы, которая в это время находится в эфире.

Именно возможность мобилизовать активность зрителей делает сервис микроблогов еще более привлекательным для рекламодателей, отмечают аналитики Nielsen. В частности, в отчете указывается, что наиболее эффективно сообщения пользователей в Twitter увеличивают рейтинг разнообразных шоу в жанре реалити-шоу.

Исследование призвано повысить интерес к Twitter среди рекламодателей и компаний, стремящихся повысить телевизионные рейтинги.

«Очевидным следствием озвученного является то, что вещатели выиграют благодаря партнерству с социальными сетями, увеличив там свое присутствие, – сообщил аналитик Р. Кей из Endpoint Technologies Associates в интервью MarketWatch. – Это также подразумевает, что социальные медиа могут выиграть от более тесной координации с вещательными компаниями, хотя вещатели нуждаются в социальных медиа больше».

Весной Twitter достиг договоренности с некоторыми медийными компаниями о сотрудничестве. Сеть микроблогов собирается отслеживать, что пишут пользователи во время просмотра той или иной телепередачи. Кроме того, подписано соглашение с Nielsen о создании собственной рейтинговой системы.

Новые инструменты для рекламодателей позволяют отслеживать эффективность медиакампаний, а также рассылать дополнительную таргетированную рекламу тем, кто увидел ролик на ТВ или поделился мнением об увиденной рекламе в Twitter. Сервис микроблогов уже заручился поддержкой крупных медиакомпаний, включая Major League Baseball, Time Inc, Vevo и Vice.

Благодаря новому сервису рекламодатель может оценить, как социально активные люди относятся к телевизионным кампаниям. Механизм позволяет отслеживать хэштеги в соцсети, чтобы вычленить аудиторию, которая публикует твиты об одном и том же шоу или программе. Таким образом, формируется выборка аудитории, которой рекламодатель может демонстрировать связанную рекламу.

Twitter также анонсировал запуск программы Twitter Amplify – серии партнерских пакетов контента от крупных медиакорпораций. Они призваны

поставлять большее количество видеоклипов, а также спонсорских ссылок, связывающих рекламу телевизионную и объявления в Twitter.

Накануне сообщалось, что социальные сети Facebook и Twitter активизировались на рынке мобильной рекламы во время сезона летних отпусков, куда пользователи берут с собой планшеты и смартфоны, находясь в отдалении от телевизионных экранов.

Twitter – система, позволяющая пользователям отправлять короткие текстовые заметки (до 140 символов), используя веб-интерфейс, SMS, средства мгновенного обмена сообщениями или сторонние программы-клиенты. Характерной особенностью Twitter является публичная доступность размещенных сообщений – это называется микроблоггингом. Хотя услуга является бесплатной, доступ к ней через SMS может значительно увеличить телефонные счета, так как каждое посланное SMS, так или иначе, оплачивается по тарифам оператора ***(Twitter способен повысить рейтинги телепрограмм // IT Expert (http://itexpert.in.ua/rubrikator/item/28652-twitter-sposoben-povysit-rejtingi-teleprogramm-issledovanie.html). – 2013. – 7.08).***

***

Никто не живет вечно. В особенности пост в новостных лентах социальных сетей, где каждую минуту генерируется огромное количество нового контента. Как долго пост «живет» решила выяснить исследовательская компания Wisemetrics и пришла к неутешительному выводу – всего несколько часов.

Например, в среднем 75 % (плюс-минус 5 %) активных действий со стороны пользователей публикация в Facebook получает в течение п’ять часов, сообщает компания. Затем активность заметно падает.

С показами и охватом все еще печальнее. 75 % (плюс-минус 5 %) показов пост набирает за 2,5 часа. Чтобы охватить 75 % (плюс-минус 5 %) всех пользователей, заявленных в статистике, посту требуется менее двух часов. За 30 мин. пост способен охватить 50 % своей аудитории.

Такая нерадостная статистика заставляет в полной мере оценить полезность новой аналитики Facebook – благодаря отчету «Когда ваши поклонники в сети» можно выбрать правильное время для постинга, и тем самым не только увеличить срок жизни особо важных публикаций, но и увеличить их охват и показы ***(Жизненный цикл поста в Facebook еще короче, чем вы думали // Marketing Media Review (http://mmr.ua/news/id/zhiznennyj-cikl-posta-v-facebook-esche-koroche-chem-vy-dumali-35752/). – 2013. – 8.08).***

***

Лишь 32 % гендиректоров из 500 крупнейших компаний США по версии журнала Fortune имеют аккаунт хотя бы в одной социальной сети, свидетельствует исследование компании Domo и портала CEO.com.

Примерно 68 % руководителей успешных компаний не имеют аккаунтов

ни на одном из популярных сервисов, включая Facebook, Twitter, LinkedIn или Google+. В то же время, около 28 % работают с соцсетью для профессионального общения LinkedIn – примечательно, что популярность сайта среди топ-менеджеров выше, чем среди обычных интернет-пользователей в США.

Из пяти сотен гендиректоров 28 или 5,6 % ведут микроблоги на Twitter, однако лишь 19 активно публиковали сообщения за последние 100 дней. Несмотря на это, Twitter остается одним из немногих сервисов, где число пользователей-гендиректоров топ-500 Fortune постепенно растет. Аккаунты на Google+ имеют лишь пять глав крупнейших компаний США.

«Рост Twitter отражает потребность гендиректоров в высокой скорости сервиса. Бизнес-лидерам нужна информация, которая будет быстрой, краткой и легкоусваиваемой», – говорит основатель CEO.com и DOMO Д. Джеймс.

Порядка 7 % глав компаний имеют аккаунты в крупнейшей в мире соцсети Facebook по сравнению с 7,6 % в прошлом году. Наиболее популярен из гендиректоров на Facebook глава соцсети М. Цукерберг с почти 17 млн подписчиков ***(Почти 70 % глав крупнейших компаний США не пользуются соцсетями // InternetUA (http://internetua.com/pocsti-70--glav-krupneishih-kompanii-ssha-ne-polzuuatsya-socsetyami). – 2013. – 11.08).***

***

Роль соцсетей в 2013–2014 гг. в SEO-практике вырастет: прогноз

Золотые дни SEO-специалистов – когда можно было «налить трафика» из любых источников, меняться постовыми и «вечными» ссылками с любыми ресурсами и даже псевдо-бложеками – похоже, в 2013–2014 гг. останутся в прошлом. На страницах Search Engine Journal появился прогноз 10 ключевых трендов поисковой оптимизации на второе полугодие текущего и на весь следующий год. Если судить по этому материалу, то придется больше внимания уделять именно качеству, а не количеству постов. Да к тому же социальные сети, которые SEOшники не очень жалуют, скажут свое веское слово; они и так уже претендуют на звание отдельной блогоплатформы.

В 2013–2014 гг. соцсети станут генераторами преимущественной части привлекаемого трафика. С появлением около двух лет назад великого и ужасного Google+ в игру поисковой оптимизации включились социальные медиа. Популярностью контента среди пользователей, – а не поисковых роботов, – нельзя манипулировать при помощи ключевиков или удачно «скормленных» ботам скриптов. Оценка контента из чисто механического процесса превратится в процесс «очеловеченный», и влияние ранжирования не только за счет индексации, но и за счет читаемости и «вирусности», будет только расти в дальнейшем.

Для компаний, которые не покладая рук трудятся над завоеванием более высоких позиций своего контента в поисковой выдаче, появится еще одна задача: создание брендированных аккаунтов для своих сайтов в соцсетях.

Растет роль плагинов и других инструментов для публикации контента в соцсетях («лайки-шэры» теперь важны не для продаж, а для индексации контента поисковиками).

Продолжится индексация в первую очередь материалов с подтвержденным авторством при помощи Google Authorship; в «корпорации добра» продолжат активную работу над самообучающимися механиками индексации и ранжирования пользовательского контента из различных источников.

Из других трендов на полтора года вперед:

• растущая роль оптимизации для мобильных устройств, адаптивная верстка и удобство потребления контента на экранах смартфонов;

• рост спроса на осмысленный и качественный контент;

• борьба поисковиков с «мусорными» и сомнительными ресурсами (вплоть до пожизненного исключения контента из выдачи);

• более высокие позиции в выдаче для ресурсов, которые быстрее открываются у пользователей (прим. редакции – пора искать более быстрого хостера, если у вас «тормозит» сайт при большой нагрузке; хотя может вам просто стоит попробовать HTML5).

А еще эпоха гостевых постов завершается: статейный маркетинг, по мнению специалистов, попадет в поле пристального внимания Google. И стоит вам обменяться статьями с обратными ссылками с каким-то сомнительным ресурсом, – вас тут же отправят в бан. В статейном маркетинге возрастет роль ресурсов с качественной аудиторией, высоким уровнем «шэринга» в соцсетях и уникальной ценностью размещаемых материалов (эксклюзивы, партнерские совместные материалы, потенциально «вирусный» контент) ***(Роль соцсетей в 2013–2014 году в SEO-практике вырастет: прогноз // InternetUA (http://internetua.com/rol-socsetei-v-2013---2014-godu-v-SEO-praktike-virastet--prognoz). – 2013. – 11.08).***

***

Портал Pixability.com опубликовал исследование, в котором подведены итоги работы с YouTube 100 ведущих брендов во всем мире.

За время существования видеохостинга обсуждаемые бренды опубликовали 258,000 видеороликов, создали 1,378 каналов, а общее количество просмотров достигло 9,5 млрд. Были затрачены миллиарды долларов.

Согласно исследованию, общее количество просмотров брендового контента с каждым годом увеличивается на 73 %. В среднем, самые успешные компании выпускают от 78 до 500 видеороликов в месяц.

Самыми активными на YouTube являются следующие отрасли бизнеса: СМИ, технологии (как B2C, так B2B), автомобильная индустрия.

По словам организаторов, данное исследование было проведено для того, чтобы помочь маркетологам по всему миру добиться похожих результатов, а может и превзойти «лучшую сотню». Вот на что стоит обратить внимание и

как расставить приоритеты по мнению Pixability:

1. Создавайте много качественного контента.

Количество видеороликов на каналах самых успешных брендов на 50 % больше, чем у других. Первые в списке публикуют огромные объемы контента как по расписанию.

2. Относиться к SEO-оптимизации и оформлению канала серьезно.

Ориентированное на YouTube SEO подчиняется другим правилам.

Чтобы видео на YouTube плодотворно сказывалось на SEO, не забывайте добавлять в название, тэги и описания ролика необходимые ключевые слова.

По результатам работы 100 ведущих брендов можно сделать вывод, что верхний квартиль использует в два раза больше тэгов и плейлистов, по сравнению с нижним. Это показатель того, что успешные маркетологи уделяют намного больше внимания созданию детализированного и комплексного канала, наряду с оптимизацией метаданных – и это приносит результаты.

3. Маркетологи, работающие с лучшими брендами, отлично понимают, что вовлечение аудитории производится с помощью различных точек контакта с клиентами. Они специально создают разные видео, подходящие для каждой из них. Обычно видеоролики отличаются друг от друга качеством или длиной, но суть и сюжет всегда остаются интересными пользователям.

4. Лучшие бренды объединяют стратегии онлайн и оффлайн. YouTube уже не воспринимается как отдельный маркетинговый канал, а является частью маркетинговой инициативы.

Также успешные маркетологи не боятся рискнуть и снять ряд видеороликов специально для ограниченного количества людей, например участников какого-либо события. Например, поздравление с 8 марта для одной из групп.

5. Подойдите к разработке брендинга основательно, с умом. Главные бренды Интернета упоминают свой логотип не только в видео, но и в метаданных: title, tag и description.

6. В ходе исследования выяснилось, что 56 из 100 брендов ведут 10 или более YouTube каналов. 17 из 100 брендов используют меньше 50 из имеющихся каналов, 37 % всех существующих каналов не обновлялись последние 120 дней.

Более 50 % видео этих брендов набрали менее 1000 просмотров.

Количество каналов не является ключом к успеху, т. к. view rank (позиция компании, согласно количеству просмотров видео) брендов с наибольшим количеством каналов меньше, чем у других.

7. Продвигайте бренд в соцсетях. Одним из основных источников трафика на YouTube являются Twitter и Facebook. 25 % лучших брендов расшаривают видео намного активнее 25 % худших ***(Успешные бренды публикуют на YouTube до 500 видеороликов в месяц // Marketing Media Review (http://mmr.ua/news/id/uspeshnye-brendy-publikujut-na-youtube-do-500-***

videorolikov-v-mesjac-35803/). – 2013. – 13.08).

***

Как сообщается в официальном блоге Twitter, сервис микроблогов запускает новый инструмент, предоставляющий маркетологам детальную информацию о том, как твиты влияют на оффлайн-продажи компании. Новинка, разработанная совместно с агентством Datalogix, носит название offline sales impact и призвана отражать влияние вовлечённости пользователей во взаимодействие с твитами бренда (как «продвигающими», так и органическими) на оффлайн-продажи.

Прежде чем запустить инструмент, аналитическая группа Twitter совместно с представителями Datalogix длительное время проводила исследования с привлечением 35 различных брендов. В свою очередь, результаты проделанной работы выявили следующее: вовлечённость пользователей в общение с брендом в сервисе микроблогов положительно влияет на продажи в офлайн-магазинах и офисах компаний; органические твиты способствуют увеличению продаж, однако фоловеры, которым транслируются «продвигающие твиты» покупают больше.

Так, по заявлению А. Ранадива, менеджера по продукту Twitter, в результате исследований выяснилось, что управление вовлечённостью пользователей в общение с брендом в Twitter позволило в целом повысить оффлайн-продажи компании на 12 %. В случаях односторонней коммуникации – когда пользователям просто транслировали «продвигающие твиты» – офлайн-продажи повышались на 2 %. При этом сообщается, что пользователи, которым транслировались органические твиты компаний (5 и более за анализируемый период), в среднем, совершали на 8 % больше покупок, чем клиенты, которым эти твиты не показывались.

И всё же, согласно заявлениям представителей сервиса микроблогов, с точки зрения увеличения продаж «продвигающие твиты» более эффективны, чем органические. Так, пользователи, которым на протяжение всего периода тестирования транслировались «продвигающие твиты», совершили на 29 % больше покупок, чем люди, которым показывались только органические твиты от брендов.

В настоящее время новый сервис статистики доступен продавцам и рекламодателям из США, работающим в сегменте потребительских товаров (CPG) ***(Twitter запустил новый инструмент для измерения влияния твитов на офлайн-продажи // Marketing Media Review (http://mmr.ua/news/id/twitter-zapustil-novyj-instrument-dlja-izmerenija-vlijanija-tvitov-na-oflajn-prodazhi-35782/). – 2013. – 9.08).***

***

Как добиться признания и любви в социальных сетях? Этим вопросом задаются как рядовые пользователи, так и администраторы страниц брендов.

Сервис социальной аналитики KISSMetrics подготовил наглядное пособие о том, что помогает увеличить количество лайков за пост. Перевод инфографики опубликован на Lifehacker, сообщает AIN.UA (http://ain.ua/2013/08/09/135576).

Составители считают, что вовлеченность пользователей помогут повысить пять таких советов:

1. Фотографии обычно получают на 53 % больше лайков, на 104 % – комментариев и на 84 % – количество переходов по линку, чем обычные текстовые посты, содержащие ссылку.

2. У сообщений из 80 и менее символов уровень engagement (количество лайков или комментариев) может быть выше на 66 %.

3. Посты, содержащие в себе вопрос, получают на 100 % больше комментариев.

4. Посты, опубликованные во время пиковой активности, естественно, получают больше внимания (для американской аудитории это – 15:00). Здесь есть и альтернативное мнение – 12:00.

5. Если на странице бренда появится один-два поста за день, уровень вовлеченности повысится на 40 % по сравнению со страницей со средним количеством три и более сообщения в день.

Недельное количество постов также имеет значение. Если сообщения на странице появляются в количестве от одного до четырех в неделю, это повысит уровень вовлеченности на 71 % по сравнению со страницами, где в неделю пять и более постов ***(Как получить больше «лайков» на Facebook // AIN.UA (http://ain.ua/2013/08/09/135576). – 2013. – 9.08).***

***

Facebook запускає нові метрики, які мають стати в нагоді маркетологам, – місячну та денну аудиторії для десктопної та мобільної версії у розрізі країн.

Нова статистика розрахована на рекламодавців, дані щодо США та Великобританії Facebook вже розіслав електронною поштою. Наразі ніде у відкритому доступі такі дані побачити не можна. Денна аудиторія соціальної мережі у США становила 128 млн користувачів для десктопної версії (понад 40 % населення країни), для мобільної – 101 млн. Для Великобританії це 24 та 20 млн користувачів відповідно.

У Facebook сказали, що орієнтуватися на місячну активну аудиторію чи кількість зареєстрованих користувачів – це старий підхід. Наразі розуміти, хто заходить до соціальної мережі лише один раз на місяць, – це лише невеличка частина картини. Бізнес має орієнтуватися на тих, хто повертається до соцмережі щодня, тому що це частина способу їхнього життя. Для рекламодавців, вважають у Facebook, нова статистика допоможе знайти правильних людей у правильний час і на правильному пристрої ***(Костинян М. Facebook рахуватиме місячну та денну активні аудиторії за країнами // UkrainianWatcher (http://watcher.com.ua/2013/08/14/facebook-rahuvatyme-misyachnu-ta-dennu-aktyvni-audytoriyi-za-krayinamy/). – 2013. –***

14.08).

***

Німецький автоконцерн Volkswagen AG та інтернет-корпорація Google розробили мобільний додаток для автомобілістів SmileDrive, пише «Корреспондент» (http://ua.korrespondent.net/business/auto/1592020-volkswagen-i-google-rozrobili-socmerezhu-dlya-avtomobilistiv).

Як стало відомо, по суті, компанії запропонували автовласникам соціальну мережу.

Звернемо увагу, що створений сервіс став доступним через додаток для Android-пристроїв, розміщений у каталозі Google Play Store.

Видання повідомляє, що смартфон або планшет зі встановленою програмою SmileDrive підключається до бортової системи автомобіля по бездротовому каналу Bluetooth і збирає дані про поїздку: місце розташування, час у дорозі і навіть поточну погоду. Маршрут відображається на карті Google Maps. Навіть якщо автомобіль не підтримує підключення мобільного пристрою за допомогою Bluetooth, додаток все одно буде агрегувати відомості про поїздку.

Цією та іншою інформацією (фотографіями, текстовими нотатками) можна ділитися з іншими водіями в режимі реального часу. Усі дані реєструються у фоновому режимі, а звіт формується після прибуття у пункт призначення, у тому числі у відеоформаті.

Також SmileDrive може вказати автовласникові місце розташування його припаркованої машини. У програму доданий ігровий функціонал. Після завершення поїздки користувачеві виставляються бали за різні досягнення, враховуючи пересування у темний час доби, тривалість поїздки на далекі відстані і дотримання правил дорожнього руху.

Додаткові очки присуджуються в тому випадку, якщо в дорозі водієві зустрінеться автомобіль марки Volkswagen, власник якого також встановив SmileDrive.

Незважаючи на те, що це розробка німецького автоконцерну, користуватися додатком і соцмережею можуть не тільки власники моделей цієї марки. А ось обліковий запис Google і доступ в Інтернет для роботи з додатком необхідні.

Цікаво, що у Google вже є власний нещодавно придбаний схожий онлайн-сервіс для водіїв. У червні 2013 р. корпорація за 1,1 млрд дол. купила ізраїльський стартап Waze. На відміну від SmileDrive, ПО цього розробника працює на різних мобільних платформах.

Служба аналізує ситуацію на дорогах у режимі реального часу і, відштовхуючись від цього, вибудовує оптимальний маршрут до точки призначення. Відомості про аварії, радарний контроль швидкості, дорожні роботи і статуси альтернативних маршрутів руху додаток отримує від самих користувачів. Аудиторія Waze перевищує 50 млн осіб.

Крім сказаного вище, звернемо увагу, що автогіганти намагаються йти в

ногу з часом, щоб задовольнити більш високі вимоги користувачів. Так, наприкінці минулого року повідомлялося, що Volvo і Ericsson мають намір представити хмарний автомобіль ***(Volkswagen і Google розробили соцмережу для автомобілістів // Корреспондент.net (http://ua.korrespondent.net/business/auto/1592020-volkswagen-i-google-rozrobili-socmerezhu-dlya-avtomobilistiv). – 2013. – 14.08).***

***

Шесть типов постов в Facebook, которые успешно конвертируют читателей в потенциальных клиентов

Эксперты по онлайн-маркетингу из HubSpot рассказывают и показывают, как посты в Facebook можно превратить в деньги.

Что такое лидогенерация?

Если кратко – это процедура привлечения пользователей, которые готовы у вас что-то купить или заказать, поскольку проявили явный интерес к вашему предложению (продажа, заказ, оплата, подписка и т. д.).

В зависимости от того, как приходят пользователи на посадочную страницу (или целевой пост в соцсети) и как они себя ведут, различают несколько лидов, которые можно привлечь при помощи Facebook.

Прямые лиды: те, кто пришел в ответ на пост с прямой ссылкой на форму заказа и кто готов обменять личные данные на ваше предложение (купон, книжку, файл, скидку, инфографику, любой контент или информационное вознаграждение). Форма для привлечения таких лидов, как правило, размещена на отдельной посадочной странице.

Непрямые лиды: пользователи, которые пришли путем опосредованной конверсии. Вы, например, расшарили пост в блоге с призывом-ссылкой на посадочную страницу, а ссылку эту поместили в конце поста. Пользователи в Facebook прочли и лайкнули пост, затем перешли по ссылке из него на ту страницу, которая может превратить их в ваших потенциальных клиентов.

Есть несколько способов лидогенерации в Facebook, о них мы и поговорим.

1. Использование призыва к действию в обложках страниц (Cover Photos).

Недавно в Facebook убрали ограничение на добавление призывов на обложки. А значит, призывы и лозунги можно смело публиковать.

2. Ссылки в заглавиях и описаниях.

Анализ более чем 8 тыс. постов в Facebook от B2B- и B2C-компаний показал, что фотографии на страницах собирали на 53 % больше лайков, чем обычные текстовые посты. Вот почему призывы к действию и ссылки важно включить в вашу стратегию лидогенерации в этой соцсети. Помимо больших фото и надписей к ним, включите в описание фотоснимков еще и ссылки на требуемые посадочные страницы.

3. Провести чат с подписчиками.

В наших широтах эта техника используется сравнительно редко, но суть тут та же, что и в Twitter и «ВКонтакте»: собрать людей вокруг одной общей

темы и обсудить что-то важное и релевантное вашему бренду. Правда, тут надо не забыть, что чат развернуть в комментах можно, только оформив его надлежащим образом (картинка показывает, как).

Тут лидогенерация упакована в диалог: когда по ходу ответов на вопросы вы отвечаете комментарием с указанием ссылки на посадочную страницу (ссылка должна быть релевантна теме вопроса, само собой). Тем, кто заинтересовался таким инструментом общения с аудиторией в Facebook, советуем почитать этот пост от Hubspot.

4. Создание событий (Facebook Events) для ваших вебинаров.

Незаслуженно забытыми в лидогенерации оказались вебинары, так что пора это исправить. Больше пользователей Facebook можно привлечь к вашему вебинару, если в календаре создать событие для пользователей и пригласить их к участию: инструментарий Facebook Events не просто удобен в работе, его публикации еще и намного чаще отображаются в ленте новостей, чем стандартные посты Facebook.

5. Таргетированная реклама в соцсетях.

Согласно Vizu/Digiday и eMarketer, 64 % американских рекламодателей повысили затраты на рекламу в соцсетях в 2013 г. Причина проста: у Facebook довольно изощренный и эффективный инструментарий, чтобы пробиться к целевой аудитории в нужное время и по нужному вам поводу.

6. Формы для лидогенерации – во вкладках.

Тут придется привлечь дизайнера и программиста. Собственно, форму по сбору контактных данных или первичной регистрации потенциального клиента можно встроить прямо в отдельную вкладку на странице в Facebook. Формы вообще тут хорошо играют роль отдельных посадочных страниц в самой соцсети, так что вашим подписчикам не надо даже куда-то переходить: всё совершается не отходя от кассы ***(6 типов постов в Facebook, которые успешно конвертируют читателей в потенциальных клиентов // Marketing Media Review (http://mmr.ua/news/id/6-tipov-postov-v-facebook-kotorye-uspeshno-konvertirujut-chitatelej-v-potencialnyh-klientov-35814/). – 2013. – 13.08).***

***

Крупнейшая в мире соцсеть Facebook обновляет мобильные приложения для Android и iOS, а также мобильную версию своего сайта в США возможностью забронировать столик на публичных страницах ресторанов, пишет техноблог TechCrunch.

Бронь столиков с 20 тыс. Facebook-страниц американских ресторанов постепенно станет доступна пользователям мобильных продуктов соцсети в США благодаря интеграции с сервисом OpenTable. Бронирование будет осуществляться напрямую с Facebook-страницы, без необходимости посещать отдельный мобильный сайт или приложение. Когда такая же возможность появится у пользователей в других странах, пока не сообщается.

В свою очередь владельцы мобильных устройств от Apple также смогут просмотреть актуальную телепрограмму на Facebook-страницах американских телеканалов, включая название, описание и время трансляции телешоу, благодаря интеграции с Rovi. Когда аналогичный функционал получат мобильные сервисы для платформ помимо iOS, не уточняется.

Версия Facebook 6.4 для iOS уже доступна в Apple App Store. Хотя в России функционал брони отелей и телепрограмм пока не доступен, в приложении появилась возможность искать по хэштегам и кликать по ним для отслеживания тем – в июне эта опция появилась на мобильном сайте Facebook. Кроме того, разработчики обещают, что версия для iPad теперь загружается быстрее и отличается улучшенным дизайном «Хроники».

С помощью нововведений Facebook старается сделать публичные страницы на мобильных устройствах более полезными и, как следствие, более посещаемыми и важными для бизнеса. Предоставление интерактивной информации о местных бизнес-организациях позволит Facebook эффективнее конкурировать с Yelp, Foursquare и Google. Наконец, рост трафика позволит соцсети наращивать выручку от мобильной рекламы, которая по итогам II квартала уже составляла свыше 40 % от общих рекламных доходов Facebook ***(Facebook обновляет мобильные сервисы функцией брони ресторанов в США // InternetUA (http://internetua.com/Facebook-obnovlyaet-mobilnie-servisi-funkciei-broni-restoranov-v-ssha). – 2013. – 14.08).***

***

На первый взгляд SMM – не совсем подходящий инструмент дополнения маркетинг-микса для финансовых учреждений. Но это не так. Ниже – 12 простых советов, что делать и чего не делать, продвигая финасовый бренд в соцсетях.

1. Взвешивайте достижимость маркетинговых целей.

Чтобы понять необходимость присутствия своего бренда в популярных соцсетях, нужно оценить целевую аудиторию. Не стоит «распыляться» на все социальные медиа сразу – выбирайте только те, где преобладают именно ваши потребители. А банковских потребителей в Украине, имеющих профиль в крупнейших социальных сетях, насчитывается: «ВКонтакте» – охват 76,4 % (10 243 856 человек), Facebook – 25,1 % (3 371 973 человек); «Одноклассники» – 59,7 % (8 009 370 человек). (Средневзвешенные показатели приведены из исследования Opinion Software Media компании InMind).

2. Планируйте.

Многие украинские банки приходят в социальные сети с массой идей, энтузиазмом и «горящими глазами». Однако их запала хватает ненадолго. Уже через несколько недель или месяцев аккаунт «глохнет». Это неприемлемо и принесет бренду больше вреда, чем пользы (потребитель видит угасший энтузиазм, давно не обновленные новости и у него создается впечатление о несостоятельности компании). Следует

выработать подробный, понятный и выполнимый план активности на год, так сказать «крупными мазками». Для начала определите маркетинговую стратегию. Далее составляйте контент-план (тактику) еженедельно. Стратегия может претерпеть корректировки, она должна быть гибкой, как сам рынок, реагировать на появляющиеся факторы, однако ни в коем случае не отворачивайтесь от изначальной цели.

3. Собирайте новости внутри структуры.

Далеко не все сотрудники компании понимают важность присутствия своего бренда в социальных сетях. Однако каждый руководитель подразделения должен понимать возможные бонусы и как следствие хотеть пиариться – дайте ему такую возможность. Параллельно решите вопрос формирования контента.

4. Сохраняйте «лицо» бренда в социальных сетях.

Каково ваше позиционирование? Профессионал? Дружественный? Серьезный советчик? Каждый бренд должен вести себя как личность и вырабатывать уникальный стиль общения в соцсетях, который будет узнаваем пользователями, и поддерживать существующее позиционирование.

5. Контент-план.

Это очень важный этап. Развивайте все ваши публикации на каждую тему. Отслеживайте то, что произвело наибольший резонанс, отклик – и продолжайте «раскручивать спираль». У каждого отдельного финучреждения темы могут быть различными, в зависимости от маркетинг-плана. Доля имиджевых постов должна составлять не менее 10 %, однако не забывайте, более 10 % прямых рекламных постов, именно рекламных – отпугнут подписчиков.

6. Не частите.

Оптимальное количество публикаций в день 1–2, иногда можно 3. Одна из наиболее частых причин отписки от бренда или пользователя – навязчивость, слишком много сообщений, которые засоряют новостную ленту.

7. Заимствуйте контент.

Не пишите только о ваших финансовых продуктах. Каждодневных (при этом свежих и интересных!) новостей об этом не накопит даже самый гениальный копирайтер. У вашей целевой аудитории есть и другие интересы – стройте свой контент-план на этом. Публикуйте ссылки на публикации, которые интересны им. Заменяйте иллюстрации и добавляйте собственные комментарии. Но не стоит забывать и про собственные посты – как минимум 10 % публикаций должны быть посвящены бренду.

8. Анализируйте и обращайте внимание.

Считается, что в социальных сетях не имеет значение время размещения поста, мир находится онлайн всегда – это не так. Анализируйте активность своей аудитории. Составляйте time budget, экспериментируйте с днями и частотой публикаций. Одно из исследований утверждает, что самым хорошим временем для отклика аудитории является дневное время в среду

(офисные работники уже «пережили» начало трудовой недели, но еще не находятся в лихорадочном ожидании пятницы). Попробуйте проверить. Делайте также поправку на время года и социальные факторы. Благо, для проведения подобного анализа в Украине хватает исследовательских панелей.

9. Стимулируйте общение.

Пользователи не любят, когда «вещают», но при этом не интересуются их мнением. Поэтому вопросы пользователям, ответы на их комментарии, развитие дискуссий – жизненно необходимы. Будьте понятными: все призывы к действию должны быть четкими, однозначными и находиться в полном соответствии с намеченными вами маркетинговыми целями продвижения в социальных сетях.

10. Отвечайте на вопросы.

Своевременная реакция на вопросы пользователей в социальных сетях, развернутые ответы всегда идут компании в плюс. Это прямой маркетинг!

Как правило, пользователи ждут моментальных ответов на свои вопросы, так что не затягивайте. Максимальный срок ответа на запрос – один день. В идеале – несколько часов.

11. Приглашайте подписчиков.

Приглашайте! В соцсетях подписчики должны приходить сами, а не покупаться на «черном рынке». Количество подписчиков – своеобразный показатель одобрения бренда пользователями. Так заработайте его – публикуйте интересный контент, запустите рекламную кампанию, продвигайте посты, разместите виджет соцсети у себя на сайте. Все, что угодно, кроме «ботов».

12. Развивайте отношения с пользователями.

Социальные сети – прекрасное место для налаживания контактов со своими клиентами, как настоящими, так и будущими. Все, что нужно – слушать их и вовремя реагировать (помогать советом или рекомендацией, отвечать на вопросы и т. д.). Многие пользователи до сих пор не разобрались в тонкостях финансовых операций, а значит, постоянно боятся быть обманутыми, так помогите им сориентироваться – для того вы и затевали маркетинговую кампанию! Заработайте их доверие честно. Пусть потребитель получит желаемое, и только так вы достигнете своих целей ***(Березицкий А. 12 советов, как продвигать финансовую компанию в социальных сетях // Marketing Media Review (http://mmr.ua/news/id/12-sovetov-kak-prodvigat-finansovuju-kompaniju-v-socialnyh-setjah-35839/). – 2013. – 15.08).***

***

Социальная сеть Facebook создает новый платежный продукт, который позволит пользователям покупать товары в сторонних приложениях, подключив к ним аккаунт в соцсети. Об этом сообщает All Things Digital со ссылкой на анонимные источники. Представители Facebook заявили изданию, что тестирование новинки начнется примерно в следующем месяце.

Воспользоваться новым продуктом сможет любой пользователь, указавший реквизиты своей банковской карты в Facebook. В дальнейшем, совершая покупки в приложениях-партнерах соцсети, он сможет не вводить каждый раз финансовые данные, а просто входить в свой аккаунт в Facebook.

All Things Digital отмечает, что новый платежный продукт может стать конкурентом платежной системы PayPal, а также аналогичных сервисов от Google, Amazon и других компаний. Сама соцсеть, благодаря нововведению, сможет лучше узнать предпочтения своих пользователей. Правда, указывает издание, пока неясно, как много пользователей указали в Facebook данные своих банковских карт.

Реальные деньги используются в Facebook для покупки физических подарков для своих друзей и приобретения виртуальных улучшений в играх в соцсети. Сейчас пользователи могут оплачивать услуги с помощью счета в PayPal либо напрямую со своей карты.

Facebook – крупнейшая соцсеть в мире, которой каждый месяц пользуется около миллиарда человек. В свою очередь, у PayPal 132 млн активных пользователей из 193 стран. Ежедневно через платежную систему проходит по 7,7 млн транзакций ***(Facebook решил составить конкуренцию PayPal // Marketing Media Review (http://mmr.ua/news/id/facebook-reshil-sostavit-konkurenciju-paypal-35853/). – 2013. – 16.08).***

***

Сервис микроблогов Twitter тестирует функцию, которая будет рассказывать пользователям о популярных телешоу. Об этом сообщает TechCrunch.

Доступ к нововведению получил пользователь @ASG. Он рассказал, что в мобильном клиенте Twitter для iOS у него виден блок Trending, в котором рассказывается о популярном на данный момент шоу. В браузере эта информация не показывается.

Блок, занимающий примерно половину экрана, появляется в верхней части основной ленты Twitter. На нем показан логотип шоу, указаны время и канал, по которому оно идет, и приводится количество твитов, посвященных передаче. Кликнув по этому блоку, пользователь перейдет на отдельную страницу с дополнительной информацией: списком аккаунтов, связанных с шоу, и твитами, в которых оно обсуждается.

В Twitter отказались комментировать нововведение.

В последнее время Twitter активно занимается технологиями, затрагивающими телевидение. Такой подход связан с тем, что пользователи часто обсуждают шоу и сериалы, которые они смотрят по телевизору, в своих микроблогах.

Например, в мае компания представила сервис, который в режиме реального времени отслеживает, о каких передачах пишут пользователи. Это нужно, чтобы показать им в Twitter ту же рекламу, которую они только что посмотрели по телевизору.

Еще раньше, в декабре 2012 г., Twitter заключил соглашение с компанией Nielsen, занимающейся измерением телерейтингов. Результатом сотрудничества стала Nielsen Twitter TV Rating – система измерений, основанная на данных из сервиса микроблогов ***(Twitter расскажет пользователям о популярных телешоу // InternetUA (http://internetua.com/Twitter-rasskajet-polzovatelyam-o-populyarnih-teleshou). – 2013. – 16.08).***

***

Топ-10 самых обсуждаемых глобальных брендов в Facebook

Более 1 млн пользователей вовлечены с брендом Coca-Cola на ее странице в Facebook, возведя компанию в топ самых обсуждаемых брендов в социальной сети.

За Coca-Cola следуют Avon, Walmart и Disney, хотя больше ни один из брендов не достиг миллионной отметки.

Компания Statista исследует самые вовлеченные бренды на Facebook, основываясь на количестве пользователей, обсуждающих бренд в сети ***(Топ-10 самых обсуждаемых глобальных брендов в Facebook // Marketing Media Review (http://mmr.ua/news/id/top-10-samyh-obsuzhdaemyh-globalnyh-brendov-v-facebook-35897/). – 2013. – 21.08).***

***

Вот как восемь популярных брендов используют вкладки на страницах Facebook для бизнеса, знания бренда и более глубокого уровня общения с поклонниками.

Кофейная сеть Starbucks делает скидки через е-карты. Вкладка на странице Starbucks в Facebook позволяет поклонникам отправлять друзьям подарочные карточки на кофе. С помощью вкладки пользователи могут оставить виртуальную подарочную карточку на стене друга посредством нескольких кликов. Это создает узнаваемость бренда кофейного гиганта и помогает продавать, так как человек, получив подарочную карточку на 5 дол., обычно покупает кофе или выпечку на большую сумму.

Телепрограмма ABC News взаимодействует с поклонниками с помощью опросов. Фаны ABC News в Facebook могут использовать сетевые вкладки, чтобы голосовать. Например, почти 4 тыс. человек проголосовали в опросе, приуроченном ко Дню матери. Цель простая – увеличить вовлеченность поклонников бренда в Facebook. ABC News надеется, что они не только проголосуют, но и перепостят опрос у себя на странице. Можно также посмотреть предыдущие опросы (а их результаты часто используются в новостях), что даст зрителям дополнительный стимул голосовать.

Продуктовая сеть Target встраивает в Facebook Twitter и получает чат в режиме реального времени. Target регулярно проводит сессии Twitter-чатов со знаменитостями. Так как многие поклонники бренда не пользуются Twitter, гигант розничной торговли проводит и сохраняет эти Twitter-беседы

на своей странице в Facebook.

Авиакомпания Delta использует вкладки как еще один канал обслуживания клиентов. Delta Airlines уделяет много внимания работе с ними.

Обслуживание пассажиров для этого авиаперевозчика – самое главное. Он относится к этому серьезно и в онлайне. Вкладка Delta в Facebook – часть общей картинки. С помощью простой формы на вкладке клиенты могут подать жалобу или описать свою проблему.

Toyota предоставляет возможность увидеть и пообщаться с представителями бренда. Эта компания использует на своей странице в Facebook разные вкладки, но одна из них особенная. Она демонстрирует круглый стол с «Нью-Йорк автошоу», в котором принимают участие ее представители, рассказывающие о новой модели Avalon. Прямая трансляция прибавляет Facebook серьезности и дает поклонникам возможность вживую пообщаться с представителями компании и другими владельцами автомобилей Toyota.

Косметическая Tom's of Maine обращает внимание на переживания клиентов. Tom's of Maine – компания, которая, как и ее клиенты, очень заботится об окружающей среде и устойчивом развитии. Но когда огромная корпорация Colgate-Palmolive ее купила, некоторые из клиентов слегка заволновались. Компания отреагировала на их переживания на своей странице в Facebook – разместила вкладки с длинным списком FAQ. На этой странице можно найти ответы на все вопросы и сомнения, включая те, которые касаются ингредиентов, входящих в состав продуктов, а также гарантий.

Производитель футболок Threadless дает клиентам возможность влиять на дизайн продукта. Это не лучшая вкладка на Facebook в плане покупательского переживания, но в данном случае стратегия производителя вполне адекватна: завлечь самых ярых фанов на свою страницу и позволить им голосовать за будущий дизайн футболок, готовящихся к выпуску.

Косметическая Clarisonic узнает своих самых ярых сторонников. Данная компания выгодно использует новый популярный тренд на Facebook «Поклонник месяца». Это хороший способ вовлечь фанов и поставить их в центр внимания. Победитель получает средства Clarisonic и ссылку на свою страницу во вкладке, на которой проводится также блиц-опрос каждого победителя ***(Как восемь популярных брендов используют вкладки в Facebook // Marketing Media Review (http://mmr.ua/news/id/kak-vosem-populjarnyh-brendov-ispolzujut-vkladki-v-facebook-35904/). – 2013. – 21.08).***

***

Поиски оптимального дня для вовлечения фанатов на Facebook продолжаются, и хотя исследование от компании Socialbakers показывает некоторые интересные данные, компания признает, что не существует

идеального дня для размещения постов.

Проанализировав 2 858 620 постов на 23 000 страницах брендов Socialbakers обнаружили, что понедельник один из лучших дней для вовлечения в социальных сетях, тем не менее, большинство постов размещаются к концу недели.

Анализ также показал, что выходные дни не достигают большого успеха в рамках «Уровень вовлечения».

Ниже приводится анализ процента постов, созданных в каждый день недели, по отношению с вероятностью (%) рейтинга вовлечения на примере одного из 4000 постов с высоким уровнем вовлечения:

Понедельник – 14,8 % / 7,1 %
Вторник – 16,6 % / 0,2 %
Среда – 16,7 % / 2,4 %
Четверг – 16,8 % / –1,8 %
Пятница – 17,1 % / 2,6 %
Суббота – 9,9 % / – 12,1 %
Воскресенье – 8,2 % / –5,3 %

Socialbakers допускает, что нет идеального дня для размещения поста, так как много факторов оказывают влияние на уровень вовлечения с контентом. Эти факторы включают демографию фанатов, природу продукта или услуги, даже пору года ***(Исследование: понедельник – один из лучших дней для вовлечения в социальных сетях // Marketing Media Review (http://mmr.ua/news/id/issledovanie-ponedelnik-odin-iz-luchshih-dnej-dlja-vovlechenija-v-socialnyh-setjah-35908/). – 2013. – 21.08).***

***

Специальная версия фотоаппарата Canon PowerShot N позволяет делиться фотографиями и видеозаписями с друзьями в Facebook с помощью одной кнопки.

12,1-мегапиксельная компактная фотокамера Canon PowerShot Nc восьмикратным зумом оснащена специальной кнопкой, которая позволяет отправлять фотографии и видеозаписи из ее памяти в соцсеть Facebook. Кнопка расположена на боковой панели фотоаппарата, оснащенного 2,8-дюймовым LCD-экраном и 28-миллиметровым широкоугольным объективом. Для отправки фотографий камера подключается к WiFi. Кроме того, ее можно присоединять к смартфону, используя последний как точку доступа в Интернет.

Первоначальный вариант PowerShot N был оснащен кнопкой, которая позволяла просто отправлять фотографии в Интернет, однако в Canon заметили, что ее используют в основном для того, чтобы выкладывать снимки в Facebook, и решили переделать кнопку под более узкоспециализированные нужды. Предыдущая «неFacebookизированная» версия Pwershot N пока также доступна в магазинах.

Продажи Canon Powershot N Facebook начнутся в сентябре в онлайн-

магазинах Canon Direct по цене 299 дол. ***(Анонсирована фотокамера с кнопкой быстрого доступа к Facebook // InternetUA (http://internetua.com/anonsirovana-fotokamera-s-knopkoi-bistrogo-dostupa-k-Facebook). – 2013. – 22.08).***

***

Во II квартале количество кликов по рекламе в Facebook увеличилось на 16,4 %, а доходы рекламодателей – больше чем на 28 %. Такие данные были получены маркетинговой платформой Kenshoo Social.

В отчете Kenshoo Social рекламные тренды в Facebook во II квартале текущего года сравниваются с трендами в I. В результате, выяснилось, что благодаря более оптимизированной и таргетированной рекламе количество кликов по ней увеличилось на 16,4 %, а рейтинг кликабельности поднялся на 18,5 %, в результате чего цена за клик сократилась на 15,9 %.

Данные были получены в ходе анализа 75 млрд рекламных объявлений в Facebook по репрезентативной выборке рекламодателей и агентств, пользующихся услугами Kenshoo Social.

Переходы, определяемые сторонними продажами, лайками, комментариями, шерингом, установкой приложений, участиям в играх и прочей деятельностью пользователей Facebook, согласно исследованию, увеличились на 56,9 %.

Тем временем доход рекламодателей от размещения рекламы в социальной сети в период между I и II кварталами возрос на 28 %. «Рекламодатели выяснили, что использование рекламы в Facebook может привести к успеху в достижении их маркетинговых целей и, что более важно, большему количеству переходов и высоким доходам», – заявил старший директор по маркетингу продукта Kenshoo Social Т. Герольд.

Он также добавил, что Facebook «постоянно оптимизирует свои рекламные возможности и выпускает все новые инструменты рекламного таргетинга, разработанные специально для получения прямых откликов». Это включает в себя схемы Custom и Lookalike Audiences, начавшие работу в марте, Partner Categories, запущенную в апреле, и Facebook Exchange (FBX), выпущенную в прошлом году.

«В то же время рекламодатели начали точнее определять свои целевые аудитории и более точно отрабатывать свои тактики на пользователях, которые могут счесть рекламу привлекательной. Их работа стала более утонченной», – сказал Т. Герольд ***(Facebook увеличивает доходы рекламодателей // Marketing Media Review (http://mmr.ua/news/id/facebook-uvelichivaet-dohody-reklamodatelej-35932/). – 2013. – 22.08).***

***

Facebook анонсировал ряд обновлений, направленных на увеличение визуальной привлекательности рекламных объявлений, размещаемых в социальной сети. Новость об этом появилась 23 августа на официальной

странице Facebook For Business.

Одним из ключевых нововведений станет программа сотрудничества с фотобанком Shutterstock. Она позволит рекламодателям получить бесплатный доступ ко всем стоковым изображениям, хранящимся в фотобанке. Ранее при покупке рекламного размещения в социальной сети рекламодатели должны были предоставлять свои собственные изображения.

Shutterstock предоставляет доступ к более чем 25 млн изображений в высоком качестве. В ближайшее время все они станут доступны рекламодателям Facebook.

Также соцсесть заявила о предоставлении новой возможности загружать несколько изображений одновременно для проведения A/B-тестирования. Эта функция позволит создавать два варианта одной и той же рекламы, которые будут показываться на странице поочередно. Таким образом, рекламодатель сможет определить какой из них вариантов лучше воспринимается аудиторией.

На сегодняшний день вся рекламная информация в социальной сети размещается в виде баннеров, которые располагаются рядом с лентой новостей, а также непосредственно в самой ленте (в виде продвигаемых постов).

По прогнозам экспертов, в 2013 г. Facebook может только на продажах мобильной рекламы заработать более 2 млрд дол. ***(Facebook поможет рекламодателям сделать рекламу привлекательнее // InternetUA (http://internetua.com/Facebook-pomojet-reklamodatelyam-sdelat-reklamu-privlekatelnee). – 2013. – 23.08).***

***

Twitter подаст документы на размещение на бирже в конце 2013 г. Компания уже ведет переговоры с банками об организации IPO.

Twitter проводит предварительные переговоры с банками, чтобы выбрать андеррайтеров IPO. Об этом сообщает The New York Post. Среди возможных претендентов на роль организаторов публичного размещения интернет-компании – JPMorgan Chase, Goldman Sachs, Morgan Stanley, Citigroup, Bank of America и Credit Suisse.

В процессе переговоров генеральный директор Д. Костоло и финансовый директор Twitter М. Гупта заявили банкирам, что хотят избежать чрезмерного ажиотажа и публичного внимания в течение первичного публичного размещения, как это было в случае с Facebook.

Это не первое упоминание в СМИ о скором выходе сервиса микроблогов на IPO. В конце прошлого месяца USA Today обнаружила на LinkedIn открытую Twitter вакансию финансового менеджера, среди обязанностей которого фигурировала подготовка документов для Комиссии по ценным бумагам перед IPO. Как писали All Things Digital, IPO Twitter может произойти в конце этого года или в начале 2014 г. ***(Twitter выйдет на IPO в конце года // InternetUA (http://internetua.com/Twitter-viidet-na-IPO-v-konce-***

goda). – 2013. – 23.08).

***

Социальная сеть Facebook приняла решение убрать «настоящие» подарки из сервиса Gifts и вместо них сконцентрироваться на цифровых «товарах» и подарочных картах, сообщает AllThingsDigital со ссылкой на Л. Линдена, главу сервиса. «На самом деле мы приняли это решение на основании отзывов пользователей. Физические вещи, конечно, интересны, но наша цель – предлагать услуги, которые интересуют большинство пользователей», – заявил он в интервью ресурсу.

По словам Л. Линдена, «осязаемые» подарки дарят не более 20 % тех, кто пользуется Facebook Gifts, при этом наличие настоящих, «физических» вещей требует серьезных затрат на логистику и работу с партнерами, которые их предоставляют. Цифровые подарки и виртуальные подарочные карты намного проще и удобнее как для компании так и, судя по всему, для пользователей социальной сети. При этом глава Gifts не стал раскрывать затраты Facebook на поддержание «физической» части сервиса.

Интересно, что хотя этот шаг Facebook делает его прямым конкурентом некоторых своих партнеров, рвать с ними отношения не планируется. Речь идет прежде всего о сервисе Wrap, который доступен как приложение для пользователей социальной сети. «Мы по-прежнему рады видеть Wrap на нашей платформе», – заявил Л. Линден. Физические подарки из Gifts должны исчезнуть уже на этой неделе – отдельные пользователи могли заметить их пропажу еще в конце прошлой недели.

В Рунете идея сервисов подарков не очень популярна. Даже у Facebook на русской версии сервиса Gifts стоит «заглушка», которая по-прежнему рассказывает про «настоящие подарки» («Настоящие чувства. Настоящие подарки» – гласит слоган). Возможно, что-то изменить получится у Ф. Мучника, который недавно анонсировал запуск сервиса Wishkey. Вероятно, ему и его команде могут пригодиться опыт и выводы Facebook относительно работы с подарками в Интернете ***(Facebook отказывается от «физических» подарков // InternetUA (http://internetua.com/Facebook-otkazivaetsya-ot--fizicseskih--podarkov). – 2013. – 26.08).***

***

По данным ресурса TechCrunch, Instagram приобрела компанию, создавшую приложение Luma. Сумма сделки не называется, а цель, в общем-то, вполне ясна – существенно улучшить возможности популярной мобильной службы в области редактирования и обработки видеороликов. Команда Luma вышла на рынок всего 18 месяцев назад, и теперь работу в составе Instagram рассматривает для себя в качестве нового этапа развития.

Вдобавок к базовым средствам редактирования видео вроде компенсации дрожаний, настройки яркости, контрастности и насыщенности, Luma также может предложить технологию Infinite Filter, которая позволяет накладывать

фильтры во время съёмки, а потом столь же просто их убирать или накладывать другие.

Текущим пользователям службы Luma следует иметь в виду, что компания сворачивает свою деятельности 31 декабря, так что нужные видеоролики лучше скачать, чтобы не их утратить. Улучшенные видеовозможности не помешают Instagram в противостоянии с Vimeo – в ближайшее время накал борьбы, похоже, будет только нарастать ***(Instagram приобрела Luma для улучшения средств редактирования видео // InternetUA (http://internetua.com/Instagram-priobrela-Luma-dlya-ulucssheniya-sredstv-redaktirovaniya-video). – 2013. – 26.08).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Всё больше пожилых людей по всему миру заводят себе учётные записи в социальных сетях и активно ими пользуются.

Самые разнообразные социальные проекты – сети и микроблоги – привлекают всё больше людей пожилого возраста, от 65 лет и старше. В общей сложности 72 % взрослого населения планеты пользуются социальными сетями. Такую информацию приводят аналитики компании Pew Research Center.

Уточним, что в 2006 г. всего 1 % людей данной возрастной категории пользовался социальными сервисами. Теперь же их количество увеличилось до 43 %.

Впрочем, как следует из отчёта Pew Research Center, более молодые люди тоже стали гораздо активнее пользоваться социальными интернет-проектами. Например, в категории от 50 до 64 лет активных участников сетей и микроблогов набралось 60 %. Среди людей в возрасте от 30 до 49 лет интересующихся социальными сетями стало 78 %, по состоянию на июль 2013 г.

Особое внимание аналитики уделили микроблогам Twitter. Этим проектом пользуется 18 % от общего взрослого населения планеты. В 2010 г. этот показатель был равен 8 %. Люди старшего поколения в категории от 50 до 64 лет тоже оставляют записи и комментарии – таковых насчитывается 13 %.

Тех, кому уже больше 65 лет, Twitter интересует не столь сильно – всего 5 % людей в данной возрастной категории используют этот сервис. За три года этот показатель возрос ровно на 1 % ***(Социальные сети стремительно «взрослеют» // InternetUA (http://internetua.com/socialnie-seti-stremitelno--vzrosleuat). – 2013. – 10.08).***

***

Размещение фотографий на Facebook может привести к потере друзей. К таким выводам пришли исследователи из Бирмингемского университета, изучив 500 пользователей соцсети. Ученые обнаружили, что те пользователи, кто регулярно публикует свои фотографии, рискуют оттолкнуть многих людей, заглядывающих на их страницу. «Наше исследование показывает, что те, кто часто отправляет свои фотографии на Facebook, рискуют разрушить реальные отношения», – рассказывает доктор Д. Хаутон.

Личные фотографии в соцсети могут испортить отношения с друзьями, родственниками и даже коллегами. Ведь все это разные группы, которые по-разному воспринимают пользователя.

Родственников и настоящих друзей может огорчить, что человек делится своими фотографиями с какими-то непонятными «друзьями» из Facebook, о которых по-настоящему близкие люди не имеют представления. Коллегам может не понравиться информация о некоторых приватных сферах, о которых они бы предпочли не знать. Было также замечено охлаждение отношений внутри пар, которые публикуют много своих фотографий.

«Будьте осторожны, делясь своими фотографиями, думайте, как они будут восприниматься теми, кто их может увидеть. Делиться своими впечатлениями – это отличный способ улучшить отношения, но он так же может привести к противоположным результатам», – предупреждают исследователи ***(Размещение фотографий в Facebook может привести к потере друзей // Подробности.UA (http://podrobnosti.ua/internet/2013/08/12/923224.html). – 2013. – 12.08).***

***

Согласно исследованию британского Общества по предотвращению жестокого обращения с детьми, каждый пятый ребенок в течение последнего года испытывал унижения в социальных сетях. Об этом сообщает IT Expert со ссылкой на BBC Украина.

В частности, речь идет об издевательствах, непристойных предложениях сексуального характера, кибер-преследованиях и требованиях выглядеть и одеваться определенным образом.

В докладе NSPCC также отмечается, что многим пользователям Facebook, Twitter и YouTube меньше 13 лет – возраст, определенный как минимальный для тех, кто может участвовать в этих социальных сетях.

Полный отчет, в котором были опрошены более тысячи британских подростков в возрасте от 11 до 16 лет, будет обнародован в ноябре.

Но предварительные результаты исследования свидетельствуют о том, что наиболее распространенными формами унижения в Интернете являются издевательство и троллинг, предусматривающий оскорбительные и обычно анонимные высказывания в адрес «преследуемых», чтобы вызвать их реакцию.

В NSPCC говорят, что решили провести исследования из-за роста

озабоченности тем, какие невзгоды могут ожидать подростков и молодых людей в Интернете.

6 августа 14-летняя британская школьница Х. Смит покончила с собой из-за того, что ее травили в Интернете. Ее отец заявил, что Х. Смит регулярно получала оскорбительные сообщения в социальной сети ask.fm. «Невозможно представить, что кто-то настолько молодой может думать, что когда над тобой издеваются в социальных сетях, другого выхода, как покончить жизнь самоубийством, просто нет», – говорит представительница NSPCC К. Лилли. Она также утверждает, что исследователи, которые сосредоточились на таком явлении, как «троллинг» в социальных сетях, обнаружили особо опасные тенденции, когда речь идет об 11–12-летних подростках. «Мы должны приложить усилия, чтобы подростки знали, к кому можно обратиться, и не чувствовали себя изолированными в случае, когда возникает такая проблема», – заявила представительница благотворительной организации.

Британский премьер Д. Кэмерон призвал к бойкоту сайтов, которые не могут справиться с издевательствами в сети.

После смерти Х. Смит основанная в Латвии ask.fm заказала «полный и независимый юридический аудит» своего сайта на предмет мер безопасности.

В июне количество посетителей сайта превышало 13 млн ежедневно. Члены сети могут обмениваться информацией, фото и видео через сам сайт или через приложения к нему.

Одна из самых противоречивых черт сайта – возможность задавать вопросы другим участникам сети анонимно ***(Каждый пятый ребенок подвергается издевательствам в онлайн // IT Expert (http://itexpert.in.ua/rubrikator/item/28796–kazhdyj–pyatyj–rebenok–podvergaetsya–izdevatelstvam–v–onlajn.html). – 2013. – 13.08).***

***

Время, которое человек проводит в социальной сети Facebook (и, возможно, в других аналогичных онлайн-сервисах) отрицательно коррелирует с его настроением.

Проведенные американскими учеными наблюдения показали, что у тех, кто проводит в соцсети много времени, портится настроение: подробности приведены в статье исследователей для журнала PLoS One.

Ученые набрали 82 добровольца в штате Мичиган. Участникам заплатили по 20 дол. и разыграли среди них один iPad2: в обмен от подписавшихся на эксперимент людей требовалось пройти психологические тесты до и после двухнедельного периода, а на протяжении двух недель аккуратно отвечать на приходящие по SMS вопросы о своем настроении и о том, сколько времени было проведено в социальной сети.

Обработав информацию как о настроении участников в ходе опыта, так и о затратах времени на Facebook, психологи обнаружили отрицательную

корреляцию. Иными словами, настроение у тех, кто много времени проводил в онлайне, обычно оказывалось хуже, чем у тех, кто тратил на Facebook сравнительно мало часов своей жизни. Причем этот эффект был заметен как на небольших временных отрезках (в течение дня), так и при сопоставлении результатов тестирования до и после эксперимента. Последнее говорит о том, что снижение психологического комфорта носит долговременный характер.

Исследователи подчеркивают, что они отдельно проанализировали влияние на эмоциональный фон числа друзей в Facebook, наличия симптомов депрессии у самого пользователя, выраженности чувства одиночества, уровня самооценки, пола и даже цели, с которой человек заводил аккаунт в социальной сети. Все эти факторы оказались неспособны объяснить найденную закономерность. Иными словами, дело вовсе не в том, что изначально подверженные депрессией люди стремятся больше времени провести в Facebook.

Возможную связь плохого настроения со стремлением выбирать не реальное общение, а какую-то деятельность в одиночестве ученые рассмотрели отдельно. Против этой гипотезы психологи приводят как ряд научных аргументов (данные предыдущих исследований), так и один интуитивно понятный довод: люди, которые в одиночестве читают книги или занимаются спортом, как правило получают от этого удовольствие, а вовсе не расстраиваются.

Ранее японские ученые доказали, что если человек проводит слишком много времени на работе, а начальство при этом предъявляет к нему слишком высокие требования, то это тоже приводит к депрессии ***(Исследование: Facebook портит настроение // Utro.ua (http://www.utro.ua/ru/zhizn/issledovanie_facebook_portit_nastroenie1376562896). – 2013. – 15.08).***

Маніпулятивні технології

В социальных сетях разразилась информационная война между русскими и украинцами.

Внимательные телезрители, которым доступны российские каналы в кабеле или по спутнику, разглядели в рекламном ролике чистящего средства Bref циничное и крайне оскорбительное для украинцев изображение украинского флага, который натурально смывается в унитаз потоками воды. Действительно, стикер, который прикрепляется к стенке сантехнического устройства, на вид – вылитый национальный флаг Украины.

Шум, который поднялся уже в социальных сетях, похож на объявление информационной войны русским… Заголовки в лентах новостей выглядят так – «Российская реклама призывает смывать Украину в унитаз».

Между тем, достаточно пары кликов, чтобы узнать, что Bref производится немецким концерном Henkel и что форма и цвет стикеров разработаны дизайнерами этого химического гиганта. Производитель

выпустил серию из трех Duo Stick: Blue Ocean (синяя полоса вверху и голубая полоса внизу), Fresh Flower (синяя полоса вверху и бордовая внизу) и Lemon-Lime (синяя полоса вверху и желтая внизу).

Самые горячие уже призвали бойкотировать продукцию фирмы Henkel, но главный тренд, конечно, другой – умелое и настойчивое разжигание ненависти к России…

… Действительно реклама выглядит дурным тоном и, возможно, не умышленным, но издевательством. А буквально за неделю до начала этого скандала все бурно обсуждали другой – унижение самого что ни на есть настоящего украинского флага музыкантами американской группы, которые на него помочились, куда уж дальше? ***(В социальных сетях разразилась информационная война между русскими и украинцами // Свобода слова в Україні (http://svobodaslova.in.ua/news/read/20947). – 2013. – 13.08).***

***

Немецкая компания Henkel после жалоб Украины изъяла с восточноевропейского рынка освежитель для унитазов в виде украинского флага, сообщила в блоге Foreign Policy журналистка Л. Томкиу.

«По-видимому, продукт Bref Duo Stick с синими и желтыми полосами чересчур похож на украинский флаг», – пояснила автор, уточняя, что в Украину освежитель в продажу не поступал.

Компания приняла решение после негодующих комментариев на своей странице в Facebook («в том числе картинки с флагом Германии в унитазе») ***(Украина пожаловалась на немецкого производителя // Левый берег (http://world.lb.ua/news/2013/08/15/220156_henkel_izyala_prodazhi_osvezhitel.html). – 2013. – 15.08).***

***

В соціальній мережі Facebook шириться хвиля протесту проти товарів, вироблених у Росії.

Активісти і прості користувачі закликають українців бойкотувати російські товари, зокрема, російські шоколадки: «Росія оголосила Україні тотальну економічну війну! Всі українські товари заборонені для експорту до Росії. Чи це правда, а чи просто залякування, однак м’ясні, сирні, шоколадні та інші торговельні війни Кремля з Україною просто ДІСТАЛИ! Тому пропонуємо всім небайдужим долучися до бойкоту російських товарів в Україні. Їх можна знайти за країною-виробником на упаковці, а також за першими трьома цифрами штрих-кодів – це 460–469. Пишіть відомі Вам російські товари в Україні в коментарях, щоб можна було зробити список», – пишуть активісти на Facebook-сторінці Віктор Медведчук – антиУкраїнський вибір.

Причиною стали інциденти з продукцією української компанії Roshen, котру росіяни заборонили через нібито невідповідність якості, і заява прес-служби Федерації роботодавців України про те, що Росія фактично

заблокувала всі українські товари на митниці… ***(Активісти просять не купувати російські шоколадки // Свідомо (http://www.svidomo.org/defend_article/18324). – 2013. – 15.08).***

***

Украинцы не сдерживают свои эмоции и открыто делятся о себе информацией в соцсетях, разбрасываясь данными, которые в будущем могут быть использованы против них. Социальные сети превратились в океан полезных сведений для практичных и циничных профессионалов. Сетевой жизнью граждан интересуются журналисты, спецслужбы, воры и работодатели. Парадокс в том, что большинство пользователей настолько откровенны в онлайне, что делают сбор информации о себе довольно легким делом.

В развитых странах огромный массив частной информации из соцсетей стал объектом серьезного бизнес-анализа. Украинцы в этом смысле еще более беспечны, чем европейцы или американцы.

Наполнением онлайн-страниц пользователей в Украине все чаще интересуются не только воры, которые высматривают будущих жертв по фотографиям роскошных интерьеров, но и руководители, желающие оценить лояльность подчиненных.

Онлайн-проверками, по словам главы исследовательского центра HeadHunter У. Ходорковской, регулярно занимаются HR-отделы крупных фирм. У. Ходорковская отмечает, что человека, который постит фотографии котиков или собак в социальные сети, могут не взять на высокий пост. Также эксперты советуют не обсуждать начальство и коллег в Интернете.

Украинские компании теперь устанавливают корпоративные правила поведения в онлайне. Например, надо публиковать только конструктивные комментарии, не делать оскорбительных замечаний, уважать права собственности.

Сетевая социализация стала настоящим подарком для бизнеса. Как утверждает эксперт К. Кириченко, соцсети – это почти идеальный инструмент, чтобы без особых усилий отработать целевую аудиторию.

Владельцы страничек в социальных сетях уже не скрывают, что их данные это ценный ресурс. Особенно после того, как в Facebook появилась опция – Graph Search. Это поисковик внутри сети, который позволяет анализировать и подбирать пользователей по интересам.

Эксперты советуют украинским пользователям «фильтровать» информацию, которую они выкладывают в Интернете ***(Украинцы активно пользуются соцсетями, забывая о слежке работодателей и спецслужб // InternetUA (http://internetua.com/ukrainci-aktivno-polzuuatsya-socsetyami--zabivaya-o-slejke-rabotodatelei-i-specslujb). – 2013. – 18.08).***

***

Исследователи из Калифорнийского университета в Беркли на

протяжении 10 месяцев занимались изучением «черного рынка» аккаунтов в социальной сети Twitter. Результаты исследования были представлены на 22-м симпозиуме по компьютерной безопасности USENIX в Вашингтоне.

Группа под руководством В. Паксона из Международного института компьютерных исследований (International Computer Science Institute, ICSI) отслеживала действия 27 торговцев аккаунтов, ответственных за несколько миллионов фальшивых профилей, которые впоследствии используются для распространения спама, фишинга и вредоносного ПО. 95 % из них исчезли из онлайн-доступа после того, как исследователи сообщили о них администрации Twitter. По подсчетам ученых, они были ответственны за 10–20 % всех нелегитимных аккаунтов, созданных за весь период наблюдений. Мошенники, контролировавшие данные «торговые точки», за это время заработали от 127 до 159 тыс. дол.

Доход злоумышленников, работающих на этом рынке спама и сопутствующих программ, за период исследований колебался в широких пределах от 12 до 92 млн дол. «Специализация на “черном рынке” сети Twitter является нормой, – рассказывают исследователи. – Продавцам аккаунтов, например, не приходится заниматься решениями CAPTCHA, уклонением от “черных списков” или проблемой приобретения уникальных электронных адресов».

Монетизация спама и, как итог, его стоимость зависит от серого рынка и легитимных партнерских программ, а также от синдикатов рекламных серверов или рекламных сервисов коротких ссылок (например, adf.ly). По данным исследователей, средняя стоимость аккаунта в сети Twitter составляет всего 0,04 дол. Стоимость аккаунта в Facebook колеблется в пределах от 0,45 дол. до 1,5 дол., если аккаунт верифицируется по номеру телефона, и от 0,1 дол. за аккаунт без верификации. Стоимость аккаунтов в Google составляет около 0,03–0,05 дол. за штуку. В самых доступных сетях цены на аккаунты падают до минимума: на Hotmail – 0,004–0,03 дол. за аккаунт и на Yahoo 0,006–0,015 дол. Отдельно покупатели аккаунтов доплачивают за верификацию: от 0,1 до 0,15 дол. для оптовых заказов (от 100 тыс. верификаций) и 0,25 дол. за верификацию небольших по объему заказов.

Подводя итоги своей работы, исследователи рекомендуют поднять себестоимость мошеннических операций внутри сети. Одним из возможных способов сделать это является введение подтверждения по электронной почте, что, по расчетам ученых, повысит стоимость аккаунтов в Twitter на 56 %. Необходимость введения CAPTCHA заставляет 92 % торговцев отказаться от регистрации фальшивых аккаунтов.

Исследование было ограничено сетью Twitter, потому что ни одна из других социальных сетей, куда обратились ученые (Facebook, Google и Yahoo), не дали согласия на проведение аналогичных исследований. Исследователи также отмечают, что, помимо фальшивых аккаунтов для распространения спама, им поступали предложения по приобретению спам-

хостинга, программ для взлома CAPTCHA, программ вида PPI (Pay-Per-Install) и готовых комплектов эксплойтов ***(Как бороться со спамом в соцсетях? // InternetUA (http://internetua.com/kak-borotsya-so-spamom-v-socsetyah). – 2013. – 16.08).***

***

Журналисты под прикрытием посетили «клик-ферму» в Бангладеше, где работники сидят в темных комнатах с решетками на окнах и зарабатывают по 1 дол. за 1000 Facebook-лайков. Об этом пишет UkrainianWatcher.

Один из выпусков расследовательской программы Dispatches на британском Channel 4 посвятили фейковым сторонникам в социальных сетях. Команда программы поехала в Бангладеш в поисках «клик-ферм», где «малооплачиваемые работники манипулируют социальными медиа в пользу крупных западных брендов».

Работники такой «клик-фермы» в Дакке, Бангладеш, работают в три смены и зарабатывают примерно 120 дол. в год. При том что они зарабатывают по 1 дол. за 1000 лайков, их босс берет по 15 дол. за 1000 лайков ***(Работники клик-ферм работают в нечеловеческих условиях и получают по $ 1 за 1000 Facebook-лайков // Vlasti.net (http://vlasti.net/news/171637). – 7.08. – 2013).***

***

Портал WikiLeaks опубликовал новую порцию разоблачительных документов. 400 гигабайт свежей информации доступны для скачивания любому интернет-пользователю. Однако секретные файлы защищены ключом, который WikiLeaks обещает «раздать» в сети в случае причинения вреда кому-либо из ключевых фигур организации.

На страницах WikiLeaks в Facebook и Twitter 18 августа были опубликованы ссылки на скачивание документов объёмом более 400 гигабайт. Но, даже загрузив файлы в свой компьютер, пользователь не сможет открыть их, не имея пароля, который WikiLeaks сохранил для себя в качестве гарантии безопасности своих сотрудников, в первую очередь, Д. Ассанжа и Э. Сноудена.

Организация помогала бывшему агенту ЦРУ вести переговоры о предоставлении ему политического убежища в России. Э. Сноуден обвиняется властями США в раскрытии конфиденциальной информации и краже государственных секретов. Будучи сотрудником ЦРУ, он передал WikiLeaks секретные документы, подтверждающие, что американское правительство шпионит за своими гражданами.

Опасения WikiLeaks были вызваны, в частности, призывами избавиться от Д. Ассанжа. На днях репортёр журнала Time М. Грюнвальд «взорвал» Twitter заявлением, что жаждет написать «статью в поддержку атаки беспилотника, которая нейтрализует Д. Ассанжа».

Администрация журнала Time отреагировала на скандал весьма

сдержанно: «М. Грюнвальд опубликовал оскорбительную запись в своём личном блоге, который не имеет отношения к позиции журнала». «Он сожалеет, что написал это заявление, и уже его удалил», – добавил пресс-секретарь журнала, в то время как некоторые интернет-пользователи призвали читателей отказаться от его покупки.

Г. Гринвальд, журналист The Guardian, опубликовавший разоблачения Э. Сноудена, в свою очередь написал, что «такие заявления – яркое свидетельство о глубоком разложении крупных СМИ».

Команда портала WikiLeaks уже направила в редакцию официальное письмо с просьбой уволить «кровожадного» репортёра. «Time должен продемонстрировать обществу, что когда журналисты призывают к уничтожению других журналистов, это неприемлемо», – сообщает WikiLeaks в своем Twitter ***(WikiLeaks разместил в Интернете 400-гигабайтный архив закрытых данных // InternetUA (http://internetua.com/WikiLeaks-razmestil-v-internete-400-gigabaitnii-arhiv-zakritih-dannih). – 2013. – 19.08).***

***

Эксперты по вопросам поисковой оптимизации обнаружили прямую зависимость места страницы в поисковой выдаче от количества отметок «+1» в социальной сети Google+. К такому неожиданному выводу пришли аналитики, исследуя свойства, которые чаще всего встречаются у самых «успешных» в поисковой выдаче web-страниц.

Как выяснилось, количество отметок «+1» – второй по важности фактор, который коррелирует с позицией страницы в поиске.

Хотите, чтобы Ваша страница была первой в поисковой выдаче? +1!

Результаты исследований были направлены представителям компании Google, которые уже успели уточнить: такая корреляция не означает того, что количество «+1» напрямую учитывается при ранжировании страницы.

Но эксперты утверждают, что, даже если количество «плюсиков» не учитывается напрямую, сообщения в сети Google+ специально оформляются таким образом, чтобы более явно влиять на ранжирование в Google, чем, например, отметки Like в Facebook ***(Плюсование записи в Google+ влияет на место страницы в поисковике // InternetUA (http://internetua.com/pluasovanie--zapisi-v-Google--vliyaet-na-mesto-stranici-v-poiskovike). – 22.08. – 2013).***

***

Специалисты компании Symantec предупреждают, что приложение для работы с Instagram с настольных компьютеров, реклама которого появляется в последнее время в Facebook и Twitter, является мошенническим. Клиентские программы для фотосервиса Instagram выпускаются только для мобильных устройств.

Популярность сервиса Instagram привлекла внимание спамеров и других

мошенников, поясняют в Symantec. Оба рекламируемых в сетях приложения для персональных компьютеров не работают с сервисом и представляют собой лишь средство привлечения пользователей к заполнению различных маркетинговых анкет, благодаря чему авторы зарабатывают деньги на партнерских программах. К счастью, в приложениях не обнаружено функций для похищения данных.

В рекламе утверждается, что приложение эмулирует на компьютере функциональность клиента Instagram для мобильных устройств. После загрузки и запуска программа показывает окно для ввода пароля, но вместо входа на сервис сообщает об ошибке и предлагает загрузить еще один файл, якобы необходимый для работы. Перед загрузкой пользователя просят поделиться информацией о программе в социальных сетях (более 4 тыс. человек уже дали ссылки на нее в Twitter и Facebook) и, наконец, перенаправляют на страницу с маркетинговым опросом ***(Клиент Instagram для ПК – мошенничество // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/08/22/instagram-for-pc-fraud.html). – 2013. – 22.08).***

Зарубіжні спецслужби і технології «соціального контролю»

Сервис микроблогов Twitter обновил правила для своих пользователей, дополнив информацию о недопустимости оскорблений и агрессивного поведения в соцсети. Отчет о нововведениях опубликовали в британском блоге компании Д. Харви – старший директор Twitter по безопасности – и Т. Ван – руководитель сервиса в Великобритании.

«Мы хотим, чтобы пользователи Twitter чувствовали себя в безопасности, – говорится в сообщении, – и чтобы правила Twitter давали четкий сигнал каждому, кто думает, что такое поведение допустимо или когда-либо будет допустимо». В настоящее время пользовательские правила включают подробное описание разных видов оскорблений и спама.

Помимо обновления правил, Д. Харви и Т. Ван подтвердили скорое упрощение приема жалоб, которое Т. Ван анонсировал еще в июле. Речь идет о возможности пожаловаться на содержание твита непосредственно из меню сообщения. В настоящее время эта функция уже есть в клиенте Twitter для iOS и мобильном приложении, а с сентября она должна появиться также в клиенте для Android и на сайте Twitter.com.

Нововведения Twitter связаны с недавней серией оскорблений и угроз, которым подверглись некоторые пользователи сервиса. В частности, широкую огласку получили случаи с феминистками К. Криадо-Перес и депутатом парламента от Лейборитской партии С. Кризи: обеим женщинам в микроблогах угрожали изнасилованием, и полиция уже провела в связи с этим два ареста. Как пишет The Daily Telegraph, сейчас Скотланд-Ярд расследует жалобы еще восьми пользователей Twitter, в том числе трех журналисток, которых угрожали взорвать ***(Twitter не позволит оскорблять***

своих пользователей // Подробности.UA (podrobnosti.ua/internet/2013/08/05/921751.html). – 2013. – 5.08).

***

Уряд В'єтнаму прийняв постанову, згідно з якою інтернет-користувачам заборонено розміщувати у блогах і соціальних мережах будь-яку інформацію, крім персональної, пише «Корреспондент» (http://ua.korrespondent.net/business/mmedia_and_adv/1588883-uryad-v-etnamu-zaboroniv-koristuvacham-socmerezh-publikuvati-novini-zmi).

За інформацією в'єтнамських ЗМІ, згідно з новим правилом в Інтернеті не можна ділитися інформацією з новинних видань, сайтів урядів. Особистою сторінкою вважаються власний блог або сторінка у соціальній мережі. При цьому інформацію також не можна компілювати і резюмувати.

Постанова дає змогу запобігти поширенню неправдивої інформації в інтернеті, сказав заступник міністра з інформації та комунікацій Л. Нам Чанг. За його словами, власникам персональних сторінок і сторінок у соцмережах забороняється використовувати інформацію медіа-агентств як свою власну.

Водночас, керівник одного з в'єтнамських ділових журналів Н. Ван Фу вважає, що, виходячи зі змісту прийнятої постанови, заборона стосується тільки цитування користувачем соцмережі тексту новини на своїй сторінці, але не належить до можливості викласти посилання на новинний ресурс.

Нова постанова набере чинності з 1 вересня, повідомляють ЗМІ.

У вересні минулого року південно-в'єтнамський суд засудив трьох блогерів до тюремного ув'язнення за розміщення політичних статей на забороненому в'єтнамському сайті і в їх особистих блогах, визнавши це підривом комуністичних і національних підвалин ***(Уряд В'єтнаму заборонив користувачам соцмереж публікувати новини ЗМІ // Корреспондент.net (http://ua.korrespondent.net/business/mmedia_and_adv/1588883-uryad-v-etnamu-zaboroniv-koristuvacham-socmerezh-publikuvati-novini-zmi). – 5.08. – 2013).***

***

Интернет-пользователям в Таиланде стоит внимательно следить, под каким постом они ставят лайк в социальной сети Facebook, предупреждает The Washington Post. Тем, кто одобряет сообщения о государственном перевороте, грозит тюрьма.

Такое решение власти страны приняли после того, как по сети появились несколько сообщений о том, что скоро произойдет революция. Авторы постов предупреждали тайцев, что скоро наступит дефицит продуктов и сейчас самое время запастись всем необходимым. Против авторов сообщений уже возбудили уголовное дело.

Кроме того, власти призвали граждан быть осторожнее и в других соцсетях. Если слухи о грядущей революции продолжат распространяться, это негативно скажется на стране.

Провести несколько лет за решеткой рискуют и те, кто ставит лайки под антимонархическими постами. Это расценивается как оскорбление короля, который является в Таиланде священной особой. Провинившимся придется провести в тюрьме не менее 15 лет. Причем гражданство тут не играет никакой роли: шансы отправиться за решетку у тайцев и у тех, кто просто приехал в страну – одинаковые.

В начале года Конституционный суд приговорил журналиста С. Пруксакасемсука к 10 годам лишения свободы за оскорбление короля П. Адульядета. Примечательно, что скандальные статьи писал не журналист, а бывший сотрудник пресс-службы правительства, который сбежал в Камбоджу. Тем не менее, суд решил, что виноват именно С. Пруксакасемсука, так как он был редактором журнала «Голос Таксина», где были размещены материалы.

Причем в самих статьях имя монарха даже не упоминается. В первой заметке речь шла о семье, планирующей ради сохранения власти и уничтожения демократии убийства миллионов людей, а вторая рассказывает о духе, который преследует Таиланд и замышляет зверства и массовые убийства. Суд решил, что в обоих случаях речь идет о короле Пхумипоне ***(В Таиланде за «лайк» под «революционным сообщением» в соцсети грозит тюрьма // Судебно-юридическая газета (http://sud.ua/news/2013/08/06/52803-v-tailande-za-lajk-pod-revolyutsionnim-soobshcheniem-v-sotsseti-grozit-tyurma). – 2013. – 6.08).***

***

Группа инженеров-программистов из Военной академии США в Вест-Поинте разработали инновационное программное обеспечение для аналитической разведки в социальных сетях. Об этом сообщает xakep.ru.

Естественно, военных интересуют не гражданские социальные сети вроде Facebook, а реальные социальные сети неформальных организаций, таких как партизанские отряды повстанцев в Ираке и Афганистане. Программа Organization, Relationship, ContactAnalyzer (ORCA) помогает составить социальную сеть и выявить неформальных лидеров.

Подобный софт давно используется армией США, а теперь его собираются приспособить против организованной преступности – уличных банд и криминальных группировок, которые действуют на территории Америки. Как выяснилось, принципы социальной иерархии таких полуанархических формирований очень похожи на структуру повстанческих отрядов, с которыми боролась армия. Здесь тоже нет званий, но члены банд и группировок объединены в мелкие группы со своими неформальными лидерами.

Кроме выявления неформальных лидеров, программа позволяет определить связь между членами банды, которые не признают друг друга, а также получить общее наглядное представление о группировках внутри банды. Информацию для работы системы извлекают из полицейских отчетов.

При аресте в отчете часто указывают принадлежность арестованного к той или иной группировке. Социальные связи проявляются, в том числе, по совместным арестам ***(В США применят «военное» ПО для аналитической разведки в социальных сетях // IT Expert (http://itexpert.in.ua/rubrikator/item/28829-v-ssha-primenyat-voennoe-po-dlya-analiticheskoj-razvedki-v-sotsialnykh-setyakh.html). – 2013. – 14.08).***

***

Более 30 тыс. сайтов Рунета заблокированы с сентября 2012 г. неправомерно, сообщил портал Digit.ru.

По оценке авторов нового сайта «Блоку – нет!», направленного на борьбу с произвольной блокировкой ресурсов, легальные сайты в основном заблокированы по нормам Закона «О защите детей от вредной информации», вступившем в силу 1 сентября 2012 г., а также по «антипиратскому» закону, который вступил в силу 1 августа 2013 г.

Как сообщил Digit.ru руководитель проекта «РосКомСвобода» А. Козлюк, создателем сайта «Блоку – нет!» стал активист движения против «антипиратского» закона, автор скрипт-заглушки с протестом, известный под ником Shara. Сайт создан как свободная энциклопедия, в которой может размещать свои статьи по теме борьбы с блокировкой интернет-ресурсов любой желающий.

«Блокировка производится по IP-адресу, это значит, что доступ закрывается ко всем ресурсам, размещённым на одном IP-адресе с заблокированным сайтом. На одном таком адресе могут находиться тысячи ресурсов», – объясняют авторы сайта «Блоку – нет!» блокировку легальных ресурсов.

По сообщению «Блоку – нет!», от блокировки ресурсов страдает не только Россия, но и другие страны, трафик в которые проходит через российских провайдеров. В первую очередь это Беларусь и Украина.

В настоящее время вики-проект фактически включает только главную страницу и несколько статей. Среди них публикация про Tor – распределенную анонимную сеть.

11 июля Госдума приняла закон о создании в России единого реестра доменов и сайтов с противоправным контентом. Так называемый «черный список» сайтов включает в себя ресурсы, размещие опасный для детей контент – детское порно, инструкции по суицидам и по наркотикам.

Закон, вступивший в силу 1 августа, закрепляет правовые основания и определяет порядок ограничения доступа к информационным ресурсам, через которые распространяются кинофильмы с нарушением исключительных прав. Он дает возможность блокировки ресурса, обвиненного правообладателем в размещении нелегального контента, на 15 дней на основании решения суда об обеспечительных мерах еще до подачи формального судебного иска правообладателем. Однако уже в первый день действия закона сопровождался онлайн-забастовкой интернет-

компаний и техническими проблемами.

Новый закон призван бороться только с теми, кто незаконно размещает в Интернете фильмы и сериалы. На тех, кто их скачивает, действие закона не распространяется.

«Разрабатывая законопроекты по борьбе с пиратством в Интернете, мы осознанно возложили ответственность за пиратский контент не на пользователей, а на тех, кто пиратский контент в сети размещает, осознанно воруя чужую интеллектуальную собственность», – рассказал С. Железняк ***(Активисты насчитали более 30 тысяч неправомерно заблокированных сайтов // Четверта Влада (http://4vlada.net/smi/aktivisty-naschitali-bolee-30-tysyach-nepravomerno-zablokirovannykh-saitov). – 2013. – 14.08).***

***

Агентство национальной безопасности США за последние пять лет многократно нарушало свои полномочия в сфере сбора информации.

Об этом написала газета The Washington Post 16 августа со ссылкой на результаты внутренней проверки АНБ, предоставленные изданию Э. Сноуденом.

Согласно документам о внутренней проверке, датированным маем 2012 г., АНБ, начиная с 2008 г., тысячи раз нарушало свои юридические полномочия в области слежки за коммуникациями. Так, только в период с мая 2011 г. по май 2012 г. было зафиксировано 2776 нарушений. Большинство этих нарушений касалось незаконного наблюдения за гражданами США и иностранными спецслужбами, причем эти нарушения совершались как сознательно, так и в результате случайных ошибок.

В качестве примера случайного нарушения полномочий приводится случай, когда в 2008 г. АНБ случайно перехватило большое количество телефонных переговоров из Вашингтона. Это произошло в результате ошибки программы, перепутавшей местный код 202 с кодом для международных звонков в Египет: 20.

Самое серьезное сознательное нарушение закона касалось несанкционированного использования данных более 3 тыс. граждан США и обладателей грин-карт.

Многие данные, содержащиеся в документах, предназначались только для внутреннего пользования АНБ и не предполагали раскрытия их Конгрессу США или специальным комиссиям по программам слежки. Так, в одном из документов сотрудников АНБ просят не приводить подробные данные и использовать как можно более общие формулировки в отчетах для Министерства юстиции и офиса директора национальной разведки США.

В ответ на запрос, отправленный в АНБ газетой The Washington Post, представитель агентства признал, что в работе организации время от времени случаются ошибки, и подчеркнул, что сотрудники стараются как можно раньше их обнаруживать. Представитель АНБ добавил, что число нарушений кажется высоким только в абсолютном значении: если же рассматривать

относительные значения, то все выглядит по-другому.

Ранее, 12 августа, АНБ опубликовало документ, в котором было указано, что агентство анализирует только 0,00004 % от всего объема данных, передающихся в интернете. Так, согласно документу, АНБ «касается» только 1,6 % из 1826 петабайт данных, передаваемых в интернете каждый день, причем только 0,025 процента от этих данных отбирается для анализа.

Несколькими днями ранее газета The Guardian со ссылкой на предоставленные Сноуденом документы сообщила, что с октября 2011 г. АНБ могло без санкций суда следить за перепиской граждан США. Ранее в американских спецслужбах опровергали такую возможность: концепция программы слежки PRISM предполагала сбор данных, касающихся только иностранцев, находящихся за пределами США.

В начале июня 2013 г. Э. Сноуден, работавший с ЦРУ и АНБ, передал СМИ секретные материалы о работе американских спецслужб. Так, он рассказал о программе слежки PRISM, в рамках которой спецслужбы отслеживали частную электронную переписку и телефонные переговоры американцев и иностранных граждан. Э. Сноуден также рассказал, что спецслужбы имеют неограниченный доступ к серверам крупнейших интернет-компаний мира.

В АНБ заявили, что слежка ведется только за иностранцами, проживающими за пределами США. Кроме того, спецслужбы опровергли информацию о доступе к серверам интернет-компаний, подчеркнув, что данные предоставляются только по запросу ***(АНБ уличили в незаконной слежке за американцами // Левый берег (http://world.lb.ua/news/2013/08/16/220182_anb_ulichili_nezakonnoy_slezhke.html). – 2013. – 16.08).***

***

Компания Google запатентовала новую технологию, способную вызвать очередную волну ярости у поборников защиты прав на неприкосновенность частной жизни. На фоне неутихающих споров вокруг «умных очков», разработчики зарегистрировали процесс, позволяющий отслеживать взгляд человека и его эмоциональную реакцию на различные внешние раздражители, сообщает Infowars.com.

Технология предусматривает использование некоего «устройства», которое крепится на голову пользователя, например высокотехнологичных очков. С помощью установленных в них небольших видеокамер, можно будет следить за положением глаз человека и определять объект, на который направлен его взгляд.

Устройство также фиксирует состояние зрачков пользователя и таким образом распознает изменение его реакции при виде разных предметов. Вся эта информация передается на удаленный сервер. Предполагается, что полученные данные Google будет продавать рекламодателям, желающим оценить реакцию пользователей на продвигаемые ими продукты.

Сами пользователи также смогут просматривать «журнал» своих эмоций наподобие того, как это обычно делается со списком просмотренных сайтов в интернет-браузерах. В Google также обещают, что, прежде чем продать данные рекламодателям, вся личная информация, касающаяся пользователя, а не продукции, будет удаляться.

Впрочем, пока идея Google выглядит весьма спорно. Критики компании отмечают, что стремление компании создавать продукты и технологии, связанные со «слежкой» за пользователями, напоминает одержимость. «Шокирует то, что люди, которые будут покупать Google-очки, могут в конечном счете получить то, что их глаза будут контролироваться Google», – заявил глава Big Brother Watch Н. Пиклес.

Infowars.com отмечает, что его опасения вполне обоснованны, учитывая, что ранее на этой неделе в Google признали использование компьютерных программ для чтения писем, отправленных через почтовый сервис Gmail. В ответ на иск возмущенных пользователей в компании заявили, что имеют на это право ***(Google знает, на что ты смотришь: компания патентует технологию по контролю за взглядом // InternetUA (http://internetua.com/Google-znaet--na-csto-ti-smotrish--kompaniya-patentuet-tehnologiua-po-kontrolua-za-vzglyadom). – 2013. – 18.08).***

***

Раскрытая Э. Сноуденом и поразившая правительства информация о том, что американские спецслужбы ведут обширную слежку за гражданами в сети, может в недалеком будущем оказаться нормой, которую просто не будет смысла засекречивать. Уже в следующем десятилетии число так называемых виртуальных личностей превысит реальное население Земли, что создаст «проблему» для властей многих стран. Решив, что иметь такое «подполье» в виде тысяч анонимных, бесконтрольных и непроверенных виртуальных граждан – слишком рискованно, они, скорее всего, захотят узнать, кто в действительности скрывается за каждым интернет-аккаунтом. Вполне возможно, что правительства потребуют верификации на государственном уровне, чтобы таким образом усилить контроль над виртуальным пространством.

Такую перспективу видят председатель совета директоров Google Э. Шмидт и глава Google Ideas Д. Коэн, чья книга «Новый цифровой мир» вышла на русском языке. Отрывок из нее печатает Forbes.

Будущее, переполненное виртуальными личностями – носителями огромных массивов информации, таит ряд серьезных опасностей. И главная из них – опасность утраты контроля над персональной информацией, считают авторы. У большинства из нас и сейчас есть сетевые «двойники» – те, кем мы сами представляемся в соцсетях, блогах и прочих аккаунтах. Но по-настоящему конфиденциальная или личная информация остается скрытой от посторонних глаз.

В будущем же на реальную личность все большее влияние станут

оказывать виртуальная деятельность и контакты в Интернете. «Детально документированное прошлое начнет определять наши перспективы, и мы утратим контроль над тем, как нас воспринимают другие», – предупреждают эксперты отрасли.

Одновременно возрастет вероятность несанкционированного доступа к персональным данным, их кражи или манипулирования ими. В силу этого авторы предвидят «пышный расцвет отрасли, связанной с защитой персональных данных и репутации». Такой бизнес существует и сегодня: есть специальные компании, которые с помощью различных методов могут быстро удалить из сети нежелательный для их клиентов контент или минимизировать ущерб от его появления.

Более того, по мысли руководителей Google, «онлайн-личности возобладают столь высокой ценностью, что их – реальные или придуманные – можно будет купить на черном рынке». Они станут продаваться в комплекте со всей необходимой информацией: записями в лог-файлах интернет-провайдеров, фиктивными «френдами» и данными о покупках – то есть всем тем, благодаря чему будут выглядеть правдоподобно. В их покупке могут быть заинтересованы многие – от преступников до диссидентов.

Соответственно, появится и новый вид страхования: можно будет застраховать свою онлайн-личность от кражи и взлома, ложных обвинений, злоупотреблений и несанкционированного присвоения ***(«Цифровое будущее»: в мире появится «подполье» виртуальных граждан и черные рынки онлайн-личностей // InternetUA (http://internetua.com/cifrovoe-budusxee---v-mire-poyavitsya--podpole--virtualnih-grajdan-i-csernie-rinki-onlain-licsnostei). – 2013. – 18.08).***

***

Отраслевые эксперты и представители законодательной власти диаметрально противоположно относятся к запрету на анонимность в Рунете, следует из их оценок, высказанных в беседе с Digit.ru.

В России, как сообщили «Известия», на законодательном уровне рассматривается вопрос о блокировке доступа Рунета к сети Tor, позволяющей установить анонимное соединение в Интернете, защищенное от «прослушивания», и другим анонимным серверам, включая публичные proxy-серверы.

Члены нижней палаты Федерального собрания РФ подтвердили Digit.ru существование этой законодательной инициативы и высказались в ее поддержку. «Этот законопроект, вероятно, поступит на рассмотрение в Госдуму в осеннюю сессию», – прокомментировал Digit.ru депутат Госдумы от ЛДПР В. Деньгин. Депутат одобрил инициативу, заявив, что выступает за верификацию пользователей. «Отмена анонимности – метод борьбы с мошенниками, терроризмом и экстремизмом. Давно пора понять, что за всеми следят. Общество находится под колпаком, но законопослушным гражданам бояться совершенно нечего», – сказал В. Деньгин.

Депутат Госудмы Р. Шлегель высказался за введение запрета на анонимность в Интернете, отметив, что в любом случае она будет частичной, так как останется возможность выбора псевдонима на различных ресурсах. Рядовые пользователи при этом нововведения, скорее всего, не заметят.

Представители интернет-общественности, напротив, ничего хорошего от отмены анонимности в рунете не ждут.

Председатель Пиратской партии России П. Рассудов осудил инициативу, заявив, что запрет на анонимность в Интернете означает подмену понятий и нарушает право пользователей на неприкосновенность частной жизни. «Вместо того чтобы ловить преступников, нам предлагают блокировать сайты, закрывать сети. Это путь к тому, чтобы заблокировать сотовую связь из-за того, что ее используют террористы. Однако анонимность – это как нож, которым может работать и хирург, и убийца. Но это же не повод запрещать ножи», – прокомментировал Digit.ru П. Рассудов. Анонимность в Интернете, по мнению П. Рассудова, необходима многим людям например, психологам, журналистам, самим правоохранительным органам. В то же время эксперты единогласно отметили, что в настоящее время число пользователей Tor и подобных инструментов невелико.

Примерно такой же позиции придерживается руководитель движения «РосКомСвобода» А. Козлюк. «Если провести аналогию с реальной жизнью, то это то же самое, как если бы ФСБ в обязательном порядке приказала бы гражданам ходить по улице с приклеенной на груди табличкой с паспортными данными и обозначила обязательные места перемещения, которые проходят строго только под видеокамерами», – сообщил А. Козлюк Digit.ru.

«Но, во-первых, с каждым годом число использующих данные инструменты заметно растет – люди стали задумываться как над вопросом прозрачности своих данных в сети, так и над своими правами и свободами. Во-вторых, если будет создан первый прецедент запрета какого-либо определенного инструмента или протокола в глобальной сети, то это будет фундаментом для построения очередного многоэтажного здания законодательных запретов в интернет-сфере», – заявил А. Козлюк.

Жесткое законодательное регулирование Интернета в настоящее время существует в Китае, где установлены шлюзы на входящий и исходящий трафик – так называемый золотой щит. Он блокирует вход и выход информации, а также контролирует движение информации внутри страны.

Депутат В. Деньгин считает, что запрет на анонимность не означает введения в России китайского варианта – в России подобной перспективы нет, поскольку, в отличие от России, в Китае граждане относятся к подобному методу более лояльно и больше ценят собственную безопасность. «В Китае, например, есть альтернатива соцсети Facebook, а у нас люди широко ею пользуются», – прокомментировал В. Деньгин.

П. Рассудов имеет противоположную точку зрения. «Запрет на анонимность в Интернете – это путь в Китай, Иран и Северную Корею», –

считает лидер Пиратской партии ***(Запрет на анонимность в рунете – путь в Китай или безопасность? // InternetUA (http://internetua.com/zapret-na-anonimnost-v-runete---put-v-kitai-ili-bezopasnost). – 2013. – 17.08).***

***

За сообщения, опубликованные в Twitter, могут посадить. По словам юристов из Великобритании, фразы в соцсетях могут быть использованы в качестве улик, что неоднократно применялось в судебной практике.

Британские адвокаты предупреждают блогеров, что сообщения в соцсетях могут быть использованы против них в суде. По словам юриста М. Макдональда, твиты и другие комментарии, сделанные онлайн, все чаще рассматриваются уголовным судом и полицией в качестве улик.

Его высказывание прозвучало в связи с громким делом: американскому подростку поменяли статью «убийство по неосторожности» на «убийство», после того как нашли в Twitter его весьма недвусмысленные высказывания о быстрой езде, сообщает Russia Today. В микроблоге у 18-летнего парня, сбившего насмерть велосипедистку, были найдены слова «Живи на высоких скоростях – умри молодым!» и «Давай, смерть, прокатись со мной!». Эти неосторожные фразы добавили ему срок. «Высшая степень наивности считать, что высказанное вами в соцсетях никогда не будет использовано против вас», – заявил М. Макдональд.

Администрация микроблога Twitter предупреждает, что там следует оставлять только ту информацию, которой пользователь готов открыто поделиться с окружающими. «То, о чем вы говорите в Twitter, мгновенно разлетается по всему миру!» – напоминают разработчики.

По словам адвоката, иногда соцсети даже становятся способом сбора улик. «Суд и полиция часто используют блоги ради получения доказательств. К примеру, предполагаемую жертву изнасилования просят написать письмо ее обидчику с вопросом, зачем он это совершил. Ответ используется в качестве свидетельства», – рассказал юрист ***(За запись в Twitter может грозить тюрма // Utro.ua (http://www.utro.ua/ru/zhizn/za_zapis_v_twitter_mozhet_grozit_tyurma1376943486). – 2013. – 20.08).***

***

Кандидат у мери Москви від ЛДПР М. Дегтярьов вніс до Держдуми законопроект, що передбачає для журналістів кримінальну відповідальність за використання інформації зі сторінок користувачів соцмереж без їхньої згоди, повідомляє Lenta.ru.

Текст законопроекту розміщений на сайті нижньої палати парламенту. Згідно з текстом документа, максимальний термін позбавлення волі за подібні дії становитиме п’ять років. Як альтернативне покарання законопроект передбачає штраф на суму від 200 тис. до 500 тис. руб. При

цьому дія закону буде поширюватися не тільки на ЗМІ, а й на всіх, хто без дозволу доводить особисту інформацію користувачів соцмереж до широкої громадськості.

При цьому заборонено буде цитувати тільки інформацію з акаунтів, власники яких підтвердили свою особистість. У рамках боротьби з підробленими сторінками та анонімами М. Дегтярьов у тому ж законопроекті пропонує зобов'язати всі соціальні мережі, цільовою аудиторією яких є росіяни, змушувати нових користувачів проходити процедуру верифікації. В іншому випадку їм загрожує офіційне попередження.

У пояснювальній записці уточнюється, що в перспективі право розміщувати, редагувати і видаляти інформацію в соцмережах зможуть тільки користувачі, які пройшли цю процедуру. Сам спосіб верифікації М. Дегтярьов залишає на розсуд власників соціальних мереж.

На думку депутата, підтвердження автентичності запису можна проводити за допомогою автоматичної відсилання на телефон користувача текстового повідомлення з кодом, який той повинен ввести для завершення реєстрації на сайті або через електронну пошту. Однак насправді такі заходи дають змогу тільки переконатися, що зареєструватися намагається жива людина, а не робот. Законно встановити таким чином особу користувача неможливо. Законопроект дає змогу соцмережам вимагати у користувачів паспортні дані, але це, згідно з текстом документа, є їхнім правом, а не обов'язком.

До соціальних мереж, націлених на російську аудиторію, депутат пропонує включити і ряд зарубіжних сервісів, у тому числі Facebook, Google+ і LinkedIn. У пояснювальній записці М. Дегтярьов пояснює це тим, що їхні власники активно просувають свій продукт на російському ринку і працюють з російськими рекламодавцями. Крім того, у всіх цих сервісів є російськомовні версії.

Головною метою законопроекту депутат назвав захист користувачів від вторгнення в їхнє особисте життя, а також від анонімних образ. Як пояснив М. Дегтярьов, до розробки документа його підштовхнула критика в соцмережах, що з'являється, на його думку, з боку користувачів, зареєстрованих там під вигаданими іменами ***(У Росії журналістів хочуть саджати на 5 років за інформацію, взяту без згоди з соцмереж // Інститут масової інформації (http://www.imi.org.ua/news/41478-u-rosiji-jurnalistiv-hochut-sadjati-na-5-rokiv-za-informatsiyu-vzyatu-bez-zgodi-z-sotsmerej.html). – 2013. – 20.08).***

***

Британские спецслужбы создали на Ближнем Востоке секретную базу, которая перехватывает электронную переписку, интернет-трафик и информацию о телефонных звонках региона. Об этом 23 августа пишет британская газета The Independent, которая ссылается на документы бывшего сотрудника спецслужб США Э. Сноудена.

Власти получали информацию благодаря подключению к

оптоволоконным кабелям. Собранные данные об интернет-пользователях Ближнего Востока направляются в Центр правительственной связи Великобритании, который затем делится информацией с Агентством национальной безопасности (АНБ) США.

Власти Великобритании, пишет газета, утверждают, что эта база является ключевым элементом в борьбе с терроризмом и что собранная информация позволяет своевременно узнавать о готовящихся атаках.

The Independent отказалась рассказывать более подробно об этой базе, в том числе о ее точном местонахождении. Издание напомнило, что детальная публикация информации от Э. Сноудена привела к конфликту между британскими властями и газетой The Guardian. Также авторы The Independent напомнили, что их коллеги согласились не публиковать информацию, которая может повредить национальным интересам Великобритании.

Конфликт, о котором пишет The Independent, произошел в середине августа 2013 г. Британские правоохранительные органы потребовали от The Guardian удалить все переданные Э. Сноуденом документы. Также полиция начала преследование партнера журналиста газеты Г. Гринвальда, который тесно сотрудничал с бывшим сотрудником АНБ ***(Сноуден рассекретил британскую базу интернет-слежки на Ближнем Востоке // InternetUA (http://internetua.com/snouden-rassekretil-britanskuua-bazu-internet-slejki-na-blijnem-vostoke). – 2013. – 23.08).***

***

Офис директора национальной разведки США Д. Клаппера завел блог в Tumblr, посвященный слежке за интернет-пользователями. Об этом сообщает BuzzFeed.

Вечером 21 августа в блоге IC ON THE RECORD («Отчеты разведки») появилось заявление Д. Клаппера. В нем говорится, что дневник создан в соответствии с требованием президента США Б. Обамы раскрыть обществу информацию о законных методах внешней разведки, которые используют американские спецслужбы.

В блоге был опубликован ряд рассекреченных документов, в том числе три – отражающих позиции суда по контролю за внешней разведкой (FISA) и датированных октябрем и ноябрем 2011 г., а также сентябрем 2012 г.

Примечательно, что первые две записи в блоге IC ON THE RECORD были сделаны еще в январе 2009 и июне 2012 г. Впоследствии дневник регулярно обновлялся. В частности, в нем было опубликовано заявление Б. Обамы от 9 августа, где он и призывает спецслужбы рассказать обществу о своих методах во внешней разведке.

Объявление о «перерождении» блога Д. Клаппер сделал во время телефонной конференции с журналистами. Однако, как отмечает BuzzFeed, директор национальной разведки отказался отвечать на вопросы о сообщениях СМИ, утверждающих, что спецслужбы контролируют 75 % интернет-трафика в США ***(Глава американской разведки выложил***

рассекреченные документы в Tumblr // InternetUA (http://internetua.com/glava-amerikanskoi-razvedki-vilojil-rassekrecsennie-dokumenti-v-Tumblr). – 2013. – 22.08).

***

Слежка за пользователями сети: Украина набирает обороты

В последнее время власть активно занимается решением вопроса о легализации слежки за пользователями сети и доступа к их персональной информации. Осуществляется это, как известно, под разными предлогами, начиная от защиты интеллектуальной собственности и заканчивая предотвращением террористических угроз.

Слежка за пользователями – мировой тренд

Последние мировые новости говорят о печальной тенденции, связанной с интересом всех правительств к тому, чем занимаются их подданные в Интернете. Американская газета The Guardian сообщила в начале месяца о том, что госорганы США обладают возможностью следить за сообщениями электронной почты, проверять социальные сети и чаты в 150 странах мира. И все это без соответствующих на это судовых санкций. Объем собираемой информации огромен. Данные о паролях пользователей могут храниться на серверах агентства три дня. Содержание интернет-переписки – месяц. После этого правительство США заявило, что следит только за пользователями других стран, что, вероятно, нужно расценивать как оправдание. «У нас нет шпионских программ внутри страны. То, что у нас есть, это механизмы, позволяющее отслеживать телефонный номер или адрес электронной почты, которые могут быть связаны с террористической атакой. Следует скептически относиться к возможности вторжения в частную жизнь (в связи с реализацией данных программ). Ни одно из разоблачений (о деятельности спецслужб) не означает, что мы злоупотребляем властью», – заявил Б. Обама в передаче The Tonight Show на канале NBC.

Россия также стремится следовать этой тенденции. После вступления в силу раскритикованного общественностью антипиратского закона, правительство решило перейти к открытому контролю над международным трафиком. Согласно опубликованной на правительственном сайте «концепции развития мультисервисных сетей связи общего пользования Российской Федерации», все российские операторы связи будут поделены на обычных и федеральных. За последними закрепят право на осуществление самостоятельного пропуска зарубежного трафика – к ним уже будут подключаться остальные. Эксперты полагают, что впоследствии на территории страны останется только один главный оператор. Больше всего шансов стать им у корпорации «Ростелеком».

Украинская законодательная практика

За последний год интернет-сообществу пришлось отбиваться не от одной законодательной инициативы парламентариев. То «регионал» В. Олейник предложит Верховной Раде обязать провайдеров финансировать слежку за

пользователями, то МВД возьмется за продвижение этой перспективной инициативы. Ранее этот законопроект, предлагающий внести изменения в ст. 39 Закона Украины «О телекоммуникациях», силовики пытались пронести в сессионный зал тайно. Только благодаря СМИ и критике со стороны общественности его принятия удалось избежать.

После этого власти решили пойти иным путем. Путем защиты «информационного пространства» от маньяков, пиратов и сепаратистов. Законопроект № 2208а «О защите информационного пространства», авторства того же В. Олейника, неожиданно «всплыл» в Раде в начале июня. В этом законопроекте шла речь о предоставлении силовым структурам права требовать от провайдеров удалять «неугодные» ресурсы в течение пяти суток. Помимо этого, в соответствии с законопроектом, представителям отдела по борьбе с кибер-преступностью СБУ было бы предоставлено еще и право на получение данных о пользователе и его деятельности в сети.

Еще один путь легализации информационного «паноптикума» – защита авторских прав. Из последнего – законопроект, инициированный Госслужбой интеллектуальной собственности, как заявляют чиновники из Минобразования, сможет изменить ситуацию и «отбелить» Украину в глазах мировой общественности. По факту, это еще одна возможность легальной борьбы с неугодным контентом и возможность требовать раскрытия конфиденциальной информации о пользователе – потенциальном распространителе контрафакта.

Но это всего лишь некоторые из инициатив, которым пока не суждено стать реальностью. На практике силовики и без них имеют все возможности для закрытия ресурса или получения конфиденциальной информации о пользователе.

Недавно писали о том, что WebMoney без особых раздумий и сожалении передает спецслужбам информацию о денежных переводах пользователей системы без соответствующего на то решения суда.

Представители WebMoney раскритиковали эту информацию, ссылаясь на особые внутрисистемные правила. «Напоминаем, что, в соответствии с правилами системы, в случае выявления противоправных действий со стороны пользователя (продажа порнографии, других запрещенных товаров, организация финансовых пирамид и т. д.) система может принять решение об отказе в обслуживании и оставляет за собой право предоставить необходимые сведения правоохранительным органам в строгом соответствии с действующим законодательством Украины», – сообщили в пресс-службе компании.

Пользователи соцсетей остались недовольны таким ответом.

Комментарий юриста

Д. Гадомский, партнер практики IT и медиаправа АО «Юскутум».

Контроль над деятельностью интернет-пользователей все чаще становится темой обсуждения общественности. Ведь изначально Интернет воспринимался как поле абсолютной свободы от каких-либо внешних

факторов, обладающих принудительной силой.

Украинским законодательством предусмотрены случаи, когда такой контроль может осуществляться путем проведения негласных следственных действий. В нашем случае, это снятие информации с телесетей и электронных информационных систем.

Однако следует сразу начать с нескольких оговорок.

Во-первых, согласно нормам УПК, такие действия могут осуществляется лишь в рамках открытого уголовного производства (что с недавних пор перестало быть проблемой), да и то, только относительно тяжких (наказание в виде лишения свободы на срок до 10 лет) и особо тяжких (наказание в виде лишения свободы на срок более 10 лет или пожизненного заключения) преступлений.

Решение про осуществление таких действий должно быть изложено в постановлении следственного судьи. Во-вторых, интернет-пользователям следует учитывать тот факт, что доступ уполномоченных органов к информации из электронных информационных систем или их частей, доступ к которым не ограничивается ее собственником, владельцем или держателем или не связан с преодолением системы логической защиты, не требует разрешения следственного судьи. На практике такое пренебрежение законными средствами защиты может привести к злоупотреблениям со стороны соответственных органов.

Правоохранительные органы всегда использовали возможность направить запрос, не разъясняя при этом, что отвечать на него не обязательно. Например, если для направления запроса нет достаточных оснований, но информацию получить очень хочется. Тем лицам, которые склонны исполнять любое, даже самое абсурдное требование, изложенное на бланке правоохранительного органа, хотелось бы напомнить о том, что раскрывающая сторона несет ответственность за разглашение информации о третьих лицах.

Невозможно не уделить внимание также вопросу считывания файлов Cookies. На сегодняшний день в украинском законодательстве отсутствует специальный нормативный акт, который посвящен регулированию данного вопроса. Однако это вовсе не значит, что украинские чиновники не имеют представления о таких файлах.

Начнем с того, что Европейской ассоциацией исследователей гражданского мнения и маркетинга (ESOMAR) был разработан проект Корпоративного кодекса поведения для предприятий, который регулирует вопросы, связанные с защитой персональных данных при осуществлении маркетинговой деятельности в сети Интернет. Наиболее важной частью проекта Корпоративного кодекса являются практические рекомендации ESOMAR касательно Cookies (проведение аудита Cookies, их роль в политике приватности).

Анализ ЗУ «О защите персональных данных» (ст. 11, 12) дает возможность говорить о том, что ответ на вопрос «Необходимо ли получить

предварительное согласие на установку и считывание Cookies с технического оборудования пользователя?» является утвердительным. Сбор персональных данных, который, как правило, имеет место при чтении Cookies, является составляющей процесса их обработки, на что, согласно Закону, получатель должен получит согласие субъекта персональных данных ***(Купченко А. Слежка за пользователями сети: Украина набирает обороты InternetUA (http://internetua.com/slejka-za-polzovatelyami-seti--ukraina-nabiraet-oboroti). – 2013. – 22.08).***

***

Из онлайн-магазина Google Play исчезло приложение Boyfriend Tracker, которое позиционировало себя как «частный детективі в кармане вашего партнера» и позволяло шпионить за перемещениями и перепиской пользователя.

Судя по всему, изъятие приложения произошло в ответ на жалобы на нарушения тайны частной жизни и потенциальные возможности его применения для вымогательств и преследований. Между тем всего за два месяца приложение успели скачать уже десятки тысяч ревнивых жителей Бразилии.

«Это совершенно новый вид шпионажа, – говорит М. Алмейда, 47-летняя женщина из Рио-де-Жанейро, сравнивая эту программу со слежкой Агентства национальной безопасности США. – Ты следишь за кем-то, кого близко знаешь, не за каким-то незнакомцем».

Приложение способно отправлять отслеживающему пользователю данные о местонахождении его партнера и копировать ему текстовые сообщения, отправляемые и принимаемые на телефон, находящийся «под наблюдением», передает «Голос Америки».

Кроме того, в нем предусмотрена команда, позволяющая инициировать беззвучный звонок телефона «жертвы» на телефон пользователя, так что последний может подслушать, о чем говорит его партнер.

Как отмечает The Daily Mail, подобные приложения предлагаются пользователям смартфонов и в других странах, включая европейские государства и США. Но Boyfriend Tracker стало первым приложением, получившим распространение в Бразилии – стране, которая до сих пор выражает возмущение программами электронной слежки Вашингтона.

М. Грийо, 24-летний программист из Сан-Паулу, причастный к созданию Boyfriend Tracker, заявил, что с момента выхода этой программы около двух месяцев назад ее приобрели около 50 тыс. человек, причем большинство скачиваний пришлось на последние две недели, когда на приложение обратили внимание СМИ.

Напомним, в июле благодаря разоблачениям Э. Сноудена, выяснилось, что столице Бразилии ранее находилась совместная база данных американского Агентства национальной безопасности и ЦРУ, в которой собирались разведданные о резидентах. Как и за американцами, США следили за

гражданами Бразилии – их телефонными разговорами, активностью в соцсетях, сообщил Э. Сноуден. Правда, неизвестно, работает ли разведка в Бразилии до сих пор – пока точно известно лишь, что база в Бразилиа функционировала до 2002 г. и была одной из 16 разведывательных точек, расположенных на всех континентах ***(Google удалила приложение, позволяющее отслеживать перемещения и переписку пользователя // InternetUA (http://internetua.com/Google-udalila-prilojenie--pozvolyauasxee-otslejivat-peremesxeniya-i-perepisku-polzovatelya). – 2013. – 24.08).***

***

По сведениям журналиста немецкого издания Die Zeit, власти Германии считают, что компьютеры под управлением Windows 8 позволяют шпионить за их владельцами благодаря встроенному бэкдору.

Федеральное управление по информационной безопасности Германии (BSI) выступило с предостережением, что компьютеры под управлением операционной системы Windows 8, вероятно, представляют более высокий уровень угрозы для пользователей, компаний, государственных ведомств и операторов объектов инфраструктуры государства, сообщает Reuters.

В частности, в заявлении говорится, что комбинация Windows 8 и микроконтроллера TPM (Trusted Platform Module) 2.0, которым оснащаются компьютеры под управлением Windows 8, ведет к «потере контроля над аппаратным и программным обеспечением системы». Это, утверждают в управлении, позволяет, в свою очередь, скрыто удаленно получать доступ к системе третьим лицам.

В связи с этим в управлении рекомендуют внимательно изучить предлагаемое решение и с осторожностью использовать ПК на базе Windows 8 в компаниях и организациях, хакерские атаки на которые могут привести к серьезным последствиям.

Официальная позиция BSI была разъяснена на сайте управления после нагнетания атмосферы немецким изданием Die Zeit. Во вторник, 20 августа, оно опубликовало статью, в которой говорилось, что BSI нашла в модуле TPM бэкдор (лазейку), предназначенный для осуществления слежки со стороны Агентством национальной безопасности США (NSA).

Автор статьи П. Бойд, со ссылкой на внутренний документ BSI, который якобы оказался в его распоряжении, сообщил, что BSI подозревает американские спецслужбы в шпионаже с помощью технологии TPM. То есть компьютеры с американскими технологиями, распространяемые по всему миру, однажды могут начать выполнять команды, которые на них будут присылать NSA или другие спецслужбы.

П. Бойд написал статью под впечатлением от серии новостей, связанных с раскрытием деятельности NSA. Однако BSI поспешила выступить с официальным заявлением, в котором пояснило, что лишь рекомендует с повышенной осторожностью относиться к указанным технологиям, и что никаких предположений в шпионаже со стороны США управление не имеет.

Модуль TPM был разработан некоммерческой организацией Trusted Computing Group, в состав которой входят американские компании AMD, Cisco, HP, IBM, Intel, Microsoft и др. Он включает в себя средства ограничения шифрования, удаленного контроля за системой и удаленной защиты данных. В частности, с помощью TPM удаленный пользователь может запретить владельцу ПК изменять или копировать приобретенный им цифровой контент.

Ранее американские компании опровергли свою связь со спецслужбами США, заявив, что они всего лишь обрабатывают поступающие к ним запросы на предоставление данных о пользователях, если эти запросы являются легитимными. Участие в каких-либо программах, связанных со шпионажем, они отрицают.

Пока установка модуля TPM в компьютеры является добровольной, однако в ПК с предустановленной Windows 8.1 его наличие будет обязательным ***(В ПК с Windows 8 найдена «дыра» для шпионажа // InternetUA (http://internetua.com/vlasti-germanii-obespokoeni-vozmojnim-bekdorom-v-realizacii-TPM-v-Windows-8). – 2013. – 24.08).***

***

Издание The Guardian опубликовало очередную порцию документов, переданных Э. Сноуденом. Согласно документам, АНБ выплачивали миллионы долларов крупнейшим интернет-компаниям для покрытия их издержек, связанных с программой слежки PRISM. Выплаты были осуществлены согласно решению суда (FISA), который признал, что действия АНБ были неконституционными в связи с тем, что программа слежки не могла разграничить иностранный трафик от внутреннего.

Сам суд состоялся в октябре 2011 г., но его решение была рассекречено только 21 августа. В решении суда прямо не говорится о программе PRISM, однако документы, переданные Э. Сноуденом, описывают проблемы и решения, связанные с этим судебным процессом.

Таким образом, интернет-компании должны были подписать соглашения и получить лицензию на осуществление слежки за гражданами. Согласно письму с грифом «совершенно секретно», датированному декабрем 2012 г., на новые требования в лицензировании пришлось потратить миллионы долларов. Эти средства были покрыты за счет Special Source Operations – партнерства АНБ и интернет-компаний.

В более раннем письме говорится, что все провайдеры PRISM прошли сертификацию в течение нескольких дней после решения суда за исключением Google и Yahoo, которые должны были закончить свой переход 6 октября 2011 г. Компании получили лицензии на осуществление слежки на год – до 2 октября 2012 г.

До публикации этих документов многочисленные СМИ, в том числе The Guardian, неоднократно обращались к вышеупомянутым компаниям с вопросами касательно передачи личных данных пользователей спецслужбам.

Представители компаний всегда утверждали, что все данные передаются исключительно по решению суда и отрицали свою причастность к программе слежки ***(Google, Yahoo, Microsoft и Facebook получали миллионы долларов от АНБ в рамках PRISM // InternetUA (http://internetua.com/Google--Yahoo--Microsoft-i-Facebook-polucsali-millioni-dollarov-ot-anb-v-ramkah-PRISM). – 2013. – 26.08).***

***

Инженерный совет Интернета намерен применять механизм безопасной связи, позволяющий шифровать все данные, которыми обмениваются веб-сайты и браузеры.

Крупнейшие интернет-разработчики будут бороться против программ слежки, используемых США и Великобританией. В частности, Инженерный совет Интернета (Internet Engineering Task Force, IETF) – орган, разрабатывающий интернет-стандарты, намерен шифровать все данные, которыми обмениваются веб-сайты и браузеры. Об этом сообщает Financial Times.

На практике IETF намерен применять механизм безопасной связи, который используют банки и магазины электронной торговли для защиты своих клиентов. В настоящее время план находится на стадии разработки, представители IETF хотят обезопасить пользователей интернета от слежки со стороны правительства и государственных компаний. Сейчас только небольшая часть сайтов, как правило, располагающих финансовой информацией клиентов, используют технологию шифрования данных при обмене информацией с веб-обозревателями.

Инженер программного обеспечения М. Белш, который участвовал в разработке Google Chrome, заявил, что после раскрытия секретной информации Э. Сноуденом общественность стала по другому «воспринимать мир». Шифрование информации в Интернете сейчас является очень важным вопросом.

М. Ноттингем, разработчик, председатель рабочей группы IETF по HTTP, заявил на конференции, прошедшей в Берлине в этом месяце, что члены IETF почти единогласно приняли решение о необходимости разработки системы шифрования в Интернете.

М. Ноттингем считает, что план IETF следует обсудить с интернет-сообществом, прежде чем принимать решение о его реализации. В настоящее время обсуждается вопрос обязательного использования TLS (Transport Layer Security), криптографического протокола, обеспечивающего защищенную передачу данных между узлами в Интернете. Его внедрение запланировано на 2014 г.

Эксперты в свою очередь поддают сомнению мнение о том, что TLS не позволит следить за интернет-пользователями. Это связано с тем, что умелые хакеры найдут способ взломать шифрование или будут использовать другие уязвимости, присутствующие в системах ***(Интернет-сообщество***

разработает технологию для борьбы со слежкой в Глобальной сети // InternetUA (http://internetua.com/internet-soobsxestvo-razrabotaet-tehnologiua-dlya-borbi-so-slejkoi-v-globalnoi-seti). – 2013. – 26.08).

Проблема захисту даних. DOS та вірусні атаки

Украинские хакеры обрушили сайт группы Bloodhound Gang, басист которой надругался над флагами России и Украины…

Веб-страница недоступна, пишет браузер во время посещения сайта http://bloodhoundgang.com.

Стоит добавить, что в Госдуме уже отреагировали на историю с осквернением российского флага ***(Хакеры отомстили осквернителям украинского флага из Bloodhound Gang // InternetUA (http://internetua.com/hakeri–otomstili–oskvernitelyam–ukrainskogo–flaga–iz–Bloodhound–Gang). – 2013. – 5.08).***

***

Аутентификация в один клик, реализованная в системе Google Android и позволяющая автоматически авторизоваться веб-проектах Google, может стать причиной воровства персональных данных пользователей.

Эксперты полагают, что мошенники могут использовать данную технологию для кражи логинов, паролей и другой полезной для них информации. Данное мнение было озвучено на конференции Defcon, на которой традиционно обсуждаются вопросы информационной безопасности. Как сообщает портал PC World, многие из участников мероприятия – самые настоящие хакеры.

Функция автоматической аутентификации, названная weblogin, работает путем создания уникального маркера на мобильных устройствах, позволяющего моментально подключаться ко всем сервисам Google. По словам экспертов, приложения, ворующие персональные данные с помощью weblogin, уже существуют, в том числе и то, что было написано специально для Defcon. Оно маскируется под удобное средство взаимодействия с проектом Google Finance, и в настоящее время его может скачать каждый желающий из каталога Google Play.

Данная программа действительно дает доступ к Google Finance, но в скрытом режиме копирует все данные пользователя, используемые для подключения к проекту. Приложение никуда их не пересылает, а просто демонстрирует, что это тоже возможно.

Компания Google пока никак не отреагировала на нахождение еще одной уязвимости в ее многочисленных разработках, но, так как об этом стало известно на весь мир, не исключено, что в скором будущем данная неприятность будет устранена, а брешь в системе заделана.

С учетом того, как оперативно интернет-гигант латает подобные «дыры»,

можно предположить, что на это у него уйдет всего лишь несколько дней. Напомним, что недавно Google выпустила ОС Android 4.3 с новыми настройками безопасности. Все вышесказанное в полной мере относится и к ней ***(Аутентификация в Android может угрожать безопасности данных // InternetUA (http://internetua.com/autentifikaciya–v–Android–mojet–ugrojat–bezopasnosti–dannih). – 2013. – 6.08).***

***

Неосновные аккаунты РИА «Новости» – Международного мультимедийного пресс-центра и RIA Novosti Deutsch – 7 августа были взломаны, агентство проводит внутреннее расследование по факту взлома, пишет «Обозреватель» (http://tech.obozrevatel.com/news/83721-v-ria-novosti-govoryat-chto-hakeryi-vzlomali-ih-twitter-i-pohoronili-gorbacheva.htm).

Хакеры разместили в аккаунтах ложную информацию о смерти президента СССР М. Горбачева, которые немедленно были удалены – оба фальшивых твита провисели не более пяти минут, сообщает агентство.

Помимо внутреннего расследования, РИА «Новости» готовит заявление в ФСБ и прокуратуру с просьбой расследовать факт взлома аккаунтов государственного СМИ. Кроме того, агентство обратится в компанию Twitter для получения IP-адресов взломщиков.

РИА «Новости» не первый раз становится объектом атак злоумышленников. Так например, в мае 2013 г. агентство подверглось крупнейшей DDoS-атаке, которая повторилась в июле ***(В РИА Новости говорят, что хакеры взломали их Twitter и «похоронили» Горбачева // Обозреватель (http://tech.obozrevatel.com/news/83721-v-ria-novosti-govoryat-chto-hakeryi-vzlomali-ih-twitter-i-pohoronili-gorbacheva.htm). – 2013. – 8.08).***

***

Сервис микроблогов Twitter запустил варианты двухступенчатой верификации аккаунта с мобильных устройств на iOS или Android, которые не подразумевают SMS-сообщений, и потому не требуют наличия мобильного номера, сообщает РИА «Новости».

В мае этого года Twitter ввел двойную проверку через код верификации. В этом случае пользователь добавляет номер телефона при попытке зайти в аккаунт получает на него SMS с шестизначным кодом и вводит этот код вслед за основными регистрационными данными.

Обновленные приложения Twitter для iOS и Android позволяют верифицировать данные без вовлечения SMS. Пользователь получает подтверждающий запрос либо в виде push-сообщения, либо в виде оповещения приложения. Это позволит при необходимости верифицировать сразу несколько аккаунтов, которыми управляет пользователь.

В результате возможность двухступенчатой верификации аккаунта Twitter расширит географию – ранее она была ограничена

поддержкой со стороны мобильных операторов. При вводе своих регистрационных данных пользователь получит push-сообщение с просьбой одобрить попытку. Он сможет увидеть, где и с какого браузера совершена попытка зайти в его аккаунт. Наконец, он сможет сохранить специальный код, который восстановит его доступ к аккаунту даже в случае потери мобильного.

Помимо Twitter, двухфакторные системы верификации используют для своих сервисов компании Google, Facebook, Yahoo!, PayPal, Dropbox и др. Ранее в этом году Twitter перенес ряд крупных фишинговых атак, включая взлом официального аккаунта Associated Press ***(Twitter запускает двухфакторную проверку аккаунта без SMS // IT Expert (http://itexpert.in.ua/rubrikator/item/28656-twitter-zapuskaet-dvukhfaktornuyu-proverku-akkaunta-bez-sms.html). – 2013. – 7.08).***

***

Росія лідирує по розробках вірусних схем і програм для мобільної операційної системи Android. Так вважають фахівці компанії Lockout Mobile Security, яка займається розробкою антивірусного софту, передає РБК з посиланням на «Росія 24».

На конференції Black Hat, що проходить у США і присвячена комп'ютерній безпеці, представники Lockout виступили з доповіддю, у якій повідомлялося, що саме в Росії базуються організатори багатьох вірусних атак, які обрушувалися останнім часом на власників гаджетів, обладнаних операційною системою Android.

У Lockout кажуть, що виявлена ними операція отримала назву Dragon Lady за аналогією з американськими розвідувальними літаками часів 1970-х років. «Наш аналіз показав, що торгівля мобільними вадами в Росії – це прибутковий та організований бізнес, – зазначили в Lockout. – Тут з'являються численні команди-стартапи, що спеціалізуються на подібній діяльності».

Р. Сміт, представник Lockout, заявив, що, згідно з їхніми дослідженнями, половина вірусів, створених у першій половині цього року, корінням йде в Росію і країни СНД.

За даними компанії, саме на російській території знаходяться основні «мозкові центри», які займаються створенням особливо витончених мобільних вад. Крім того, подібні тіньові співтовариства часто проводять кампанії з найму працівників для поширення або модифікації кодів, а також для організації Twitter- або e-mail-атак.

Отриманий від вірусних атак прибуток ділиться між стільниковими операторами, організаторами кампаній і посередниками. За оцінками Lockout, велика частина операторів мобільних шкідливих кампаній у Росії заробляють від 700 до 12 тис. дол. на місяць.

Згідно з підрахунками Lockout, наразі у Росії діють понад 1 тис. груп з написання шкідливостей, а їх щомісячний дохід у сумі складає більше 1 млн

дол. на рік.

Як повідомлялося раніше, кількість шкідливого ПЗ для Android зросла у 2012 р. на 163 %. Загалом було зареєстровано більше 65 тис. різних форм зловмисних програм – перепакування, шкідливі URL-адреси та SMS-фішинг тощо. Атаки «шкідників» були в основному спрямовані на гаджети, оснащені операційною системою Android, яка стала улюбленою платформою для мобільних хакерів.

У квітні цього року повідомлялося, що в Україні, Росії, Білорусі та Казахстані був зафіксований новий вірус, який розташовувався у вільному доступі в Google Play і поширювався через мобільні телефони на базі Android. Ці шкідливі програми були замасковані під 34 рекламні, новинні та ігрові додатки.

Якщо користувач скачував BadNews до себе на смартфон, то на пристрої з'являвся вірус AlphaSMS, який відправляв кібершахраям особисті дані користувачів. Згідно зі статистикою Google Play, інфіковані додатки були завантажені від 2 до 9 млн разів.

Раніше аналітична компанія Gartner підрахувала, що ринок мобільних додатків у 2013 р. досягне 25 млрд дол., а приріст становитиме 62 % відносно минулого року ***(Росія лідирує по розробках вірусних схем і програм для мобільної операційної системи Android // АРАТТА. Український національний портал (http://www.aratta–ukraine.com/news_ua.php?id=21321). – 2013. – 5.08).***

***

Обнаружены опасные уязвимости в многомерных кубах, используемых для бизнес-аналитики. Бреши позволяют киберпреступникам компрометировать данные, повышать привилегии пользователя и удаленно выполнять различные коды.

Как сообщили эксперты из Санкт-Петербургской исследовательской компании Digital Security, им удалось обнаружить уязвимости в OLAP-серверах, которые не принимают во внимание разработчики. Речь идет об уязвимостях в языке запросов MDX, которые провоцируют аналог SQL-инъекций для многомерныхструктур.

Так, бреши в MDX позволяют киберпреступникам получать несанкционированный доступ к данным, повышать привилегии пользователя, удаленно выполнять исполнительные коды, перенаправлять запросы, а также внедрять собственные процедуры на уязвимом языке запросов.

Эксперты отмечают, что актуальность проблемы вызвана повсеместным использованием OLAP-серверов для проведения бизнес-аналитики. При этом, исследователи утверждают, что параметры для MDX-запросов на данные OLAP-сервера не фильтруются, а это позволяет хакерам внедрить свои данные в уже существующий запрос, и получить практически неограниченный доступ.

Согласно оценке экспертов, более 80 % OLAP-серверов различных

компаний содержит уязвимость, открывающую доступ к корпоративным ресурсам. «В случае успешной реализации атаки на систему Business Intelligence хакер достигнет сразу двух целей: получит доступ к ресурсам предприятия и скомпрометирует все критичные для компании данные, – резюмируют в Digital Security ***(Обнаружены опасные уязвимости в многомерных кубах, используемых для бизнес-аналитики // InternetUA (http://internetua.com/obnarujeni–opasnie–uyazvimosti–v–mnogomernih–kubah—ispolzuemih–dlya–biznes–analitiki). – 2013. – 7.08).***

***

Британский IT-специалист Э. Кембер обвинил компанию Google в небрежном обращении с пользовательскими паролями. Он указал на то, что получивший случайный доступ к компьютеру злоумышленник может за считанные секунды выяснить пароли, хранящиеся браузером Google Chrome.

Корпорация уже выступила с ответным заявлением, в котором эта проблема признается не столь уж серьезной на фоне других угроз, связанных с попаданием устройства в чужие руки.

Метод, при помощи которого можно подсмотреть чужой пароль, крайне прост. Достаточно подойти к оставленному без присмотра чужому ноутбуку и набрать в адресной строке браузера chrome://settings/passwords (причем адрес будет подсказан системой автозаполнения адресной строки). Далее в появившемся окне можно будет просмотреть перечень тех сайтов, для которых пользователь сохранил пароли и увидеть сами пароли: правда, для открытия их придется еще нажать на кнопку «Показать» рядом с закрытыми точками
символами.

Столь легкий способ получения доступа к паролям возмутил Э. Кембера и он опубликовал соответствующий пост в своем блоге. Как пишет The Verge, отвечающий за безопасность браузера Chrome Д. Шу разработчик уже прокомментировал описанную британским программистом особенность. По словам Д. Шу, это нельзя считать критической уязвимостью потому, что получивший физический доступ к устройству человек и без этого обладает массой возможностей для кражи конфиденциальной информации.

Обозреватель The Verge М. Брайан при этом отмечает, что в других браузерах подобная информация все-таки становится доступна далеко не сразу. Так, в Firefox для этого надо сначала зайти в настройки браузера (Edit – Preferences), потом выбрать вкладку Security, нажать на кнопку Saved Passwords и только потом выбрать пункт Show passwords, который вдобавок попросит подтверждения в отдельном всплывающем окне с кнопками «да/нет». Причем если перед этим задать так называемый Master password (эта опция по умолчанию выключена), то программа запросит еще и его перед тем, как открыть секретную информацию. Аналогичный механизм предусмотрен в Internet Explorer ***(Браузер Chrome обвинили в небрежном хранении паролей // Подробности.UA***

(http://podrobnosti.ua/internet/2013/08/08/922460.html). – 2013. – 8.08).

***

На конференции Black Hat-2013 была представлена новая методика взлома BREACH, которая позволяет извлекать символы логинов, числа идентификаторов сессий пользователей и другую конфиденциальную информацию из зашифрованного web-трафика SSL/TLS. Секретные данные, которые обеспечивают безопасность онлайн-банкинга и магазинов электронной торговли, можно извлечь из канала HTTPS всего лишь за 30 сек.

BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) нацеливается на алгоритм сжатия данных Deflate, который используется для экономии трафика в рамках web-коммуникации. Эксплоит является усовершенствованной версией эксплоита CRIME, который также использует сжатие зашифрованных web-запросов против пользователей.

По заявлениям экспертов, А. Прадо, Н. Харриса и Й. Глюка, все версии TLS/SSL подвержены риску от BREACH независимо от используемого ими алгоритма шифрования.

Для осуществления атаки злоумышленник должен постоянно перехватывать трафик между пользователем и web-сервером для того, чтобы перенаправить жертву на поддельный сайт. Этот портал содержит сценарий, который заставляет браузер жертвы посещать целевой сайт тысячи раз – постоянно добавляя в него новые комбинации данных. Когда те байты, которые контролирует мошенник совпадают с байтами из потока, функция сжатия данных в браузере работает некорректно, а размер передаваемой информации уменьшается и злоумышленник может похитить интересующие его данные.

«Мы не расшифровываем весь поток данных, а только то, что нас интересует. Это целенаправленная атака. Нам нужно найти ту часть (ответ сайта), в которой хранится токен или пароль и последовать туда для того, чтобы получить секретную информацию», – отметил Й. Глюк.

По заявлениям исследователей, токены и другая конфиденциальная информация, отправляемая через SSL, может быть перехвачена, даже если зашифрованный контент и заказы, отправляемые в магазины электронной торговли, не входят в рамки атаки. А. Прадо, Н. Харрис и Й. Глюк выпустили специальные инструменты для того, чтобы проверять сайты на уязвимость к BREACH, а также представили методы защиты от подобных эксплоитов ***(Конфиденциальную информацию из SSL/TLS-трафика можно похитить за 30 секунд // InternetUA (http://internetua.com/konfidencialnuua–informaciua-iz-SSL-TLS-trafika-mojno-pohitit-za-30-sekund). – 2013. – 8.08).***

***

Эксперты предупреждают о появлении банковского трояна для Linux. Банковский троян, получивший название «Рука вора» (Hand of Thief), в настоящий момент доступен для приобретения (вместе с последующими

обновлениями) на подпольных хакерских форумах по цене от 2 тыс. дол., сообщает исследователь из RSA Л. Кессем в своем блоге.

По его словам, текущий функционал программы включает размещение бэкдора на скомпрометированной Linux-системе и механизм захвата данных из полей заполнения форм. При этом сами вирусописатели заверяют, что в ближайшее время в вирусе появится новый набор инструментов для web-инъекций, что сделает его полноценным банковским трояном. Авторы вируса также подчеркивают, что после выпуска этого обновления цена Hand of Thief возрастет до 3 тыс. дол.

Л. Кессем также сообщает, что в настоящий момент троян не способен самостоятельно распространяться через платформу Windows. Вместе с тем продавцы утверждают, что Hand of Thief успешно прошел испытания на 15 различных дистрибутивах Linux, в том числе Ubuntu, Fedora и Debian ***(Эксперты предупреждают о появлении банковского трояна для Linux (ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2013/08/09/thieves–reaching–for–linux–hand–of–thief–trojan–targets–linux.html). – 2013. – 9.08).***

***

Киберпреступники постоянно развивают применение вредоносного ПО, известного как Reveton, главной целью которого является вымогательство.

Последним новшеством стало то, что теперь Reveton не требует от пользователя выплаты определенной суммы денег для разблокировки компьютера. Более того, вирус вовсе не блокирует устройство.

Вредоносное ПО загружается на ПК жертвы и устанавливает поддельную версию антивирусной программы Live Security Professional. Затем пользователю сообщают, что компьютер заражен огромным количеством опасных вирусов, для удаления которых необходимо осуществить подписку ***(Новый вариант Reveton выдает себя за антивирусное ПО, но не вымогает денег // InternetUA (http://internetua.com/novii–variant–Reveton–vidaet–sebya–za–antivirusnoe–po—no–ne–vimogaet–deneg). – 2013. – 10.08).***

***

Эксперты международной антивирусной компании Eset обнаружили банковский троян, нацеленный на пользователей Бразилии. Особенностью данной угрозы стало использование в процессе кибератаки уязвимости правительственного почтового сервера, сообщили CNews в компании.

Для похищения конфиденциальной информации угроза устанавливала специальное расширение для браузера Google Chrome. Это расширение позволяло злоумышленникам перехватывать аутентификационные данные, необходимые для входа в систему онлайн-банкинга. Стоит отметить, что в Бразилии киберпреступники довольно часто используют банковское вредоносное ПО, получая при этом значительную прибыль.

Антивирусные решения Eset детектируют этот вредоносный код как

MSIL/Spy.Banker.AU. Угроза распространялась через специальную спам-кампанию. Главным звеном в такой схеме является дроппер, который отвечает за установку необходимых динамических DLL-библиотек и JavaScript-объектов на скомпрометированном компьютере.

После установки в Google Chrome специального расширения оно начинало мониторить все посещаемые пользователем сайты, стремясь отследить веб-ресурсы бразильских финансовых учреждений. Как только пользователь входил в учетную запись на одном из таких ресурсов, его аутентификационные данные моментально отправлялись на сервер злоумышленников. Для отправки был выбран необычный способ – киберпреступники использовали уязвимость в конфигурации одного из серверов, принадлежащих бразильскому правительству.

Уязвимость в настройках сервера позволила хакерам использовать учетную запись gov.br электронной почты для перенаправления с него писем на два разных аккаунта e-mail, принадлежавших одному из наиболее часто используемых почтовых сервисов.

Через аккаунт gov.br данный плагин отправлял злоумышленникам два письма – первое сигнализировало о новом заражении, а второе сообщало об авторизации пользователя в системе онлайн-банкинга. Вредоносные скрипты содержали целый список различных банковских доменов, и, в случае посещения пользователем одного из них, необходимые для аутентификации данные сохранялись и отправлялись на электронный адрес злоумышленников, рассказали в Eset.

Благодаря совместной работе экспертов Eset и правоохранительных органов Бразилии участвовавшие в кибератаке аккаунты электронной почты были блокированы, а уязвимость сервера, которая использовалась злоумышленниками для получения аккаунта gov.br, была закрыта ***(Банковский троян в процессе атаки использовал сервер правительства // InternetUA (http://internetua.com/bankovskii–troyan–v–processe–ataki–ispolzoval–server–pravitelstva). – 2013. – 10.08).***

***

Хакеры Anonymous утверждают, что ночью 10 августа им удалось кратковременно взломать сайт shlema.me, на котором размещен блог ИТ–журналиста А. Дегелера, сообщили корреспонденту proIT хакеры.

Хакерская атака была совершена в поддержку украинского хакера Dementor'a. Так, в начале августа глава Закарпатской ячейки ИПУ А. Шебелла, более известный как хакер Dementor, обнаружил критическую уязвимость SQL-Injection в международной платежной системе Paypal. Через неделю журналист А. Дегелер в своем блоге раскритиковал и поставил под сомнение новость о найденной уязвимости в PayPal.

В связи с этим хактивисты Anonymous решили «отомстить за клевету» и взломали сайт А. Дегелера. Приблизительно через два часа хостер перезалил backup и сайт был восстановлен.

«Мы не допустим подобной клеветы в будущем в адрес Интернет партии Украины, либо Dementor'a. Все подобные ресурсы будут уничтожены, а персональные и конфиденциальные данные их авторов будут распространены публично», – сообщили хактивисты ***(Анонимные хакеры мстят за Dementor'a // proIT (http://proit.com.ua/news/internet/2013/08/12/115508.html). – 2013. – 12.08).***

***

Facebook созналась в сборе информации о незарегистрированных пользователях.

Даже если человека не регистрировался в социальной сети Facebook, это еще не означает, что в системе нет его профиля. Компания недавно признала наличие бага в системе, из-за которого собирались данные на людей, никогда не регистрировавшихся на сайте. На них заводились так называемые «скрытые профили» (shadow profiles), пишет xakep.ru.

Судя по описанию, баг связан с тем, что мобильное приложение Facebook при установке запрашивает разрешение на сбор информации о людях в контакт-листе, их именах, адресах электронной почты и телефонах. Информация передается даже в том случае, если мобильное приложение Facebook было предустановленно на телефон перед продажей, как это часто делают западные операторы сотовой связи.

То есть, человек покупает мобильный телефон, а в нем уже работает в фоновом режиме приложение, которое отправляет на серверы Facebook информацию о нем и его знакомых. Даже если у него нет аккаунта в социальной сети, на него и его знакомых заранее составляют «скрытые профили», которые хранятся в системе долгое время.

Программисты Facebook объясняют, что причина бага сугубо техническая. Они запрашивают список контактов пользователя для того, чтобы выслать его друзьям приглашения тоже вступить в социальную сеть, это стандартная практика. При этом Facebook не хочет высылать приглашения тем пользователям, которые уже зарегистрированы на сайте. Поэтому осуществляется автоматическая сверка имен и адресов электронной почты в контакт-листе со списком зарегистрированных пользователей Facebook. В результате составляется список тех пользователей, у которых нет аккаунта. Эта информация хранится в системе, вместе с обычными пользователями, но в виде «скрытых профилей» (теперь ее обещают удалить).

Информацию о «теневых профилях» просочилась наружу благодаря инструменту Download Your Information (DYI) для скачивания с сайта всех своих персональных данных. Там пользователь видел кроме своих друзей, еще и некоторые «теневые профили». Этот баг справедливо посчитали утечкой персональной информации, и обнаруживший его хакер получит соответствующее вознаграждение по программе оплаты за баги.

Компания гарантирует, что персональную информацию о незарегистрированных пользователях не передавала рекламодателям.

Каждого такого пользователя видел только один или два человека, воспользовавшихся услугой Download Your Information (DYI).

Представители Facebook говорят, что собрали 6 млн профилей на пользователей с именами, фамилиями и контактной информацией. На остальных есть только e-mail или телефон, без привязки к профилю Facebook или без указания имени. Столь скромная оценка количества пострадавших вызывает сомнения у некоторых специалистов, ведь в социальной сети зарегистрировано 1,1 млрд человек, многие из которых предоставляли доступ к своей адресной книге. С такими масштабами Facebook может получить информацию обо всех пользователях интернета в мире ***(Facebook созналась в сборе информации о незарегистрированных пользователях IT Expert // http://itexpert.in.ua/rubrikator/item/28791–facebook–soznalas–v–sbore–informatsii–o–nezaregistrirovannykh–polzovatelyakh.html). – 2013. – 13.08).***

***

Корпорация Symantec сообщает о множестве атак на аккаунты пользователей в социальной сети Twitter.

Злоумышленники взламывали аккаунты ничего не подозревающих пользователей и публиковали от их имени сообщения, содержащие ссылки на вредоносные программы. При этом многие подобные сообщения были опубликованы на русском языке.

Серия взломов Twitter-аккаунтов началась в начале июля и коснулась пользователей во всем мире. Множество аккаунтов уже несколько недель находятся под контролем злоумышленников, и, хотя с использованием некоторых из них уже опубликовано по несколько сотен твитов, многие владельцы аккаунтов пока этого не заметили.

После того, как пользователь нажимает на ссылку в сообщении, в браузере открывается сайт с вредоносной программой. Вместе с загрузкой страницы стандартный браузер автоматически начинает загружать вредоносное приложение.

И хотя приложение скачивается автоматически, его установка все равно инициируется пользователем.

Эксперты Symantec также заметили, что в этих вредоносных твитах пользователям, помимо всего прочего, предлагается скачать бесплатную версию игры Asphalt 7. Будучи установленной, так называемая бесплатная версия может начать рассылку в фоновом режиме смс-сообщений на платные номера, и потраченная пользователем в итоге сумма будет значительно превосходить стоимость настоящей игры.

Другие подобные твиты содержат изображения, которые привлекают интерес пользователей и побуждают кликать по ссылкам, что также приводит к загрузке вредоносного ПО на их устройства ***(Русскоязычный спам в Twitter // ITnews (http://itnews.com.ua/news/69237-russkoyazychnyj-spam-v-twitter). – 2013. – 13.08).***

***

IT-гігант Google підтвердив присутність діри в Android, за допомогою якої можна викрадати цифрові гаманці Bitcoin. Інженер з питань безпеки Android А. Клюбін виклав на ресурсах Google дані про причини вразливості системи

Про це повідомляє CyberSecurity.

«Ми виявили, що додатки, які використовують Java Cryptography Architecture (JCA) для генерації ключів, підписів або генерації випадкових чисел, не завжди одержують криптографічні стійкі значення на Android-пристроях, що відбувається через неправильну реалізацію технології PRNG. У додатках, які прямо використовують OpenSSL PRNG без ініціалізації механізму Android, теж можуть виникати проблеми», – наголосив програміст.

Серйозні недоліки вияв ряд Bitcoin-розробників. Проблема з безпекою виникала в частині генерації випадкових чисел. Оскільки «діра» містилася в самій платформі, то недоліки виявилися в усіх Bitcoin-додатках, написаних для цієї ОС.

За даними антивірусного виробника Symantec, у результаті аналогічних недоліків у Android SecureRandom-компоненту можуть бути уразливими й близько 360 тис. інших додатків. Програмісти вказують, що низка bitcoin-додатків користується цією функцією не лише для захисту гаманців, але й для генерації чисел-ідентифікаторів шипиків, що дозволяє підробляти платіжні операції в Bitcoin.

Нагадаємо, у липні вперше віртуальна валюта Bitcoin була оголошена поза законом.

Bitcoin – це децентралізована валюта для оплати товарів і послуг в Інтернеті, яку можна обміняти на реальні гроші. Нині за один Bitcoin на токійській площадці Mt. Gox дають 102 дол. Точних даних щодо кількості користувачів Bitcoin не існує, однак курс валюти з 2011 р. зріс більше, ніж в 100 разів, зробивши багатьох її власників мільйонерами. За даними станом на червень 2013 р., в обігу перебуває 11,3 млн «біткойнів», що за відповідним курсом становить 1,15 млрд дол. ***(Google розповіла про «дірку» в Android, через яку викрадають цифрові гаманці // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/08/15/424619). – 2013. – 15.08).***

***

II квартал показал широкое разнообразие информационных угроз: среди них были и средства кибершпионажа, и таргетированные атаки, и ботнеты, и новые серьезные мобильные угрозы. При этом злоумышленники еще плотнее взялись за кражу личных данных и денежных средств, в том числе виртуальных. Такие данные получили специалисты «Лаборатории Касперского». Ожидаемо увеличился темп роста вредоносных программ для мобильных платформ: число добавленных в антивирусные базы модификаций зловредов для мобильных устройств на 30 % превышает этот показатель за первый квартал.

В начале июня «Лаборатория Касперского» раскрыла новую сеть

кибершпионажа NetTraveler, в рамках которой целевым атакам подверглись более 350 компьютерных систем в 40 странах мира. В число жертв вошли государственные организации, посольства, компании из нефтедобывающей и газовой отраслей, исследовательские центры, военные структуры и общественные активисты. Еще одним примером кибершпионажа стали атаки на компании сферы онлайн-игр, организованные хакерской группой Winnti. Начиная с 2009 г. от действий Winnti пострадали более 30 компаний по всему миру, причем помимо кражи интеллектуальной собственности злоумышленников интересовали цифровые сертификаты, подписанные компаниями-разработчиками легитимного ПО, а также исходный код онлайн-игр.

В марте и апреле в связи с кражей средств с банковских счетов были арестованы разработчики троянца Carberp, создающего ботнеты по всему миру и совершающего мошеннические действия в сфере онлайн-банкинга. Сейчас популярность Carberp идет на убыль, но тот факт, что в июне в общий доступ был выложен его исходный код, может спровоцировать появление похожих программ.

Однако хакеров теперь интересуют не только банковские счета. Заоблачный рост курса электронной валюты Bitcoin и анонимность ее использования обеспечили ей популярность у злоумышленников. В апреле эксперты «Лаборатории Касперского» обнаружили серию атак, в ходе которых киберпреступники с помощью Skype распространяли вредоносное ПО для добычи биткойнов, а спустя месяц была зарегистрирована бразильская фишинговая кампания, направленная на кражу этих виртуальных монет.

К концу II квартала число образцов мобильных зловредов в коллекции «Лаборатории Касперского» превысило 100 тыс. Практически все новые вредоносные программы были нацелены на Android – в частности, среди них обнаружен самый сложный на данный момент мобильный троянец Obad, обладающий широкой функциональностью, включая отправку SMS на платные номера, установку других вредоносных программ и пересылку их по Bluetooth.

По сравнению с I кварталом изменения в рейтинге стран по количеству вредоносных хостингов незначительные. США (24,4 %,) и Россия (20,7 %) сохранили лидирующие позиции. При этом первая десятка стран, жители которых наиболее часто сталкиваются с вредоносными программами в Интернете, за исключением Вьетнама, состоит из стран СНГ. Россия (52,9 %) в этом списке занимает второе место после Армении (53,9 %) ***(Во втором квартале число мобильных зловредов еще больше возросло // InternetUA (http://internetua.com/vo-vtorom-kvartale-csislo-mobilnih-zlovredov-esxe-bolshe-vozroslo). – 2013. – 17.08).***

***

По итогам II квартала 2013 г. доля спама в почтовом трафике увеличилась

по сравнению с началом года на 4,2 % и составила 70,7 %. При этом вредоносные вложения содержались в 2,3 % всех электронных сообщений, что на 1 % меньше показателя предыдущего квартала. Таковы результаты анализа почтового трафика за период с мая по июнь 2013 г., проведенного специалистами «Лаборатории Касперского».

Как рассказали в компании, тенденцией II квартала стала рассылка писем с вредоносными вложениями корпоративным пользователям. Причем все из них были замаскированы под автоматические уведомления: сообщения о недоставке/получении письма, о пришедшем факсе или скане. В данном случае расчет злоумышленников был на то, что офисный сотрудник, погруженный в работу, вряд ли обратит внимание на детали и откроет вложенный файл с вредоносной программой.

Неожиданностью стала рассылка открыток с вредоносными вложениями – в последнее время они практически не встречались. Однако в этом квартале эксперты «Лаборатории Касперского» зафиксировали вредоносные рассылки подобного рода, эксплуатирующие бренд известного производителя открыток Hallmark.

Лидеры среди стран-источников спама остались прежними, хотя доли рассылаемой ими мусорной почты немного уменьшились: это Китай (–1,2 %), США (–0,9 %) и Южная Корея (–3 %). При этом в Украине, Казахстане и Беларуси резко увеличилась доля исходящего спама, из-за чего во втором квартале они попали на шестую, седьмую и восьмую строчки соответственно, обогнав Россию, расположившуюся на девятой позиции.

Что касается регионов, места в рейтинге остались неизменными с прошлого квартала, однако доли отдельных регионов все же изменились. На 4,5 % увеличилась доля Азии – лидера в рассылке спама. На 2,6 % увеличилась доля Восточной Европы – во многом за счет резкого увеличения доли Украины и Беларуси в рассылке спама.

В спаме по-прежнему преобладают очень короткие письма, размер которых не превышает 1 кб. Количество таких сообщений во II квартале увеличилось по сравнению с I на 4,8 % и составило 73,8 % от всех спам-рассылок.

Наиболее популярной вредоносной программой в почте оказался, как и в предыдущем квартале, Trojan-Spy.HTML.Fraud.gen. Эта программа, выполненная в виде html-странички, имитирует регистрационную форму сервиса онлайн-банкинга. Она используется фишерами для хищения финансовой информации пользователей.

На втором месте находится почтовый червь Email-Worm.Win32.Bagle.gt, который, в отличие от других червей, может не только рассылать свои копии по контактам адресной книги пользователя, но и принимать удаленные команды на установку других вредоносных программ.

На третьем месте – одна из модификаций шпионской программы ZeuS/Zbot – Trojan–Spy.Win32.Zbot.lbda. Целью программ ZeuS/Zbot является кража различной конфиденциальной информации с компьютеров

пользователей, включая данные кредитных карт.

«В последнее время спамеры распространяют письма с вредоносными вложениями, замаскированные под сообщения сервера о недоставке. Нередко встречаются и подделки под уведомления от известных ресурсов со ссылками на вредоносные сайты. Обилие шпионских программ во вложениях писем говорит о печальной тенденции – все упорнее злоумышленники охотятся за личными данными пользователей – логинами и паролями от аккаунтов, в том числе в системах онлайн-банкинга и платежных системах.

Мы рекомендуем пользователям быть очень аккуратными даже с теми письмами, которые кажутся легитимными», – прокомментировала результаты анализа почтового трафика Д. Гудкова, руководитель отдела контентных аналитиков «Лаборатории Касперского» ***(Названы самые популярные вирусы, которые рассылались по почте // Подробности.UA (http://podrobnosti.ua/internet/2013/08/07/922207.html). – 2013. – 7.08).***

***

Многие пользователи считают, что, загружая приложения из App Store, они не подвергают себя никакой опасности. Исследователям из Georgia Tech удалось доказать обратное, отправив в App Store приложение с вредоносным кодом.

По информации Массачусетского технологического института, Apple запускает приложения на несколько секунд, делая проверку лишь ключевых функций. Благодаря этому любой злоумышленник может разместить в App Store вредоносное приложение.

Решение под названием Jekyll было замаскировано под агрегатор новостей, но после установки на любое из устройств исследователи получили доступ к телефонной книге, смогли удалено отправлять электронную почту и текстовые сообщения, снимать фотографии и перенаправлять Safari на вредоносные сайты.

«После установки приложение отправило сообщение на ранее указанный номер, что сделало возможным управление зараженным устройством. Мы хотим обратить внимание Apple на то, что процесс рассмотрения приложений далек от идеала и требует учета множества различных факторов», – заявил один из исследователей Л. Лу.

Представитель Apple заявил, что компания приняла к рассмотрению все замечания исследователей ***(Вредоносные приложения могут попасть в App Store // InternetUA (http://internetua.com/vredonosnie-prilojeniya-mogut-popast-v-App-Store). – 2013. – 19.08).***

***

«Облачная» платформа Google Cloud Storage начала по умолчанию шифровать все загруженные на нее данные. Об этом сообщается в официальном блоге платформы.

Все файлы, которые будут записываться или перезаписываться на

серверы, будут автоматически шифроваться по алгоритму AES-128. Данные, которые уже хранятся на облачной платформе, будут зашифрованы в течение ближайших месяцев.

Google подчеркивает, что нововведение не потребует от клиентов никаких действий и не скажется на производительности платформы. Данные будут автоматически расшифровываться, когда доступ к ним попытаются получить авторизованные пользователи.

Корпорация отмечает, что клиенты при желании смогут и сами настроить шифрование данных. Как сообщает CNET, в Google уточнили, что не собираются передавать властям ключи шифрования.

Нововведение в Google Cloud Storage появилось на фоне скандала со слежкой за интернет-пользователями со стороны американской разведки. Агентство национальной безопасности США (АНБ) имело полномочия тайно запрашивать нужные ей данные об активности людей в сети у интернет-компаний. В сотрудничестве с АНБ уличили ряд интернет-гигантов, включая Google, Facebook и Yahoo!.

«Облачная» платформа Google позволяет хранить данные на серверной инфраструктуре корпорации. Продукт был запущен в 2010 г. Его используют, в частности, сайт магазина Best Buy и разработчики игр Ubisoft и Rovio ***(«Облачная» платформа Google начала шифровать все данные // InternetUA (http://internetua.com/oblacsnaya--platforma-Google-nacsala-shifrovat-vse-dannie). – 2013. – 17.08).***

***

Международная компания по разработке антивирусного ПО Eset заявила о том, что в интернете активно распространяется новый вирус Win32/Bicololo, который действует преимущественно в социальных сетях. Вредоносная программа используется для кражи персональной информации. Троян проявляет себя как ссылку на графические файлы с расширением .jpg и при активации загружает вредоносное программное обеспечение, модифицируя системный файл hosts и переправляя пользователя на фальшивую страницу вместо загрузки страницы социальной сети.

В один день Bicololo стал проявлять себя одновременно в четырех различных странах – Аргентине, Бразилии, Колумбии и Чили. Примечательно, что в его коде были обнаружены комментарии на русском языке.

Хотя в измененный файл hosts и прописывается много мобильных версий сайтов, действует этот вирус только на семейство настольных операционных систем Windows.

Для размещения вредоносного ПО используются легальные ресурсы, расположенные в доменных зонах .ar, .br, .cl и .co. Эти ресурсы были заражены хакерами и в дельнейшем использовались без ведома их владельцев. Скорее всего, злоумышленники нашли эти сайты с помощью специальных инструментов для поиска уязвимых веб-приложений.

При развертывании своей схемы взломщики использовали два сервера. На одном из них хранились фальшивые подделки «ВКонтакте», «Одноклассники» и Mail.ru, а другой применяется для связи с вредоносной программой. IP-адреса серверов указывают на то, что они расположены в Латинской Америке ***(Троян семейства Bicololo поражает пользователей соцсетей // InternetUA (http://internetua.com/troyan-semeistva-Bicololo-porajaet-polzovatelei-socsetei). – 2013. – 17.08).***

***

Користувачів хмарного сервісу для зберігання даних від компанії Apple iCloud, а також власників iPhone 5 попередили про часті випадки шахрайства, що має на меті викрадення особистої інформації. Зловмисниками використовуються фішингові сайти, що маскуються під офіційні ресурси, відзначають експерти VimpelCom.

Як повідомляється, шахраї спонукають вчинити на них перехід з допомогою електронних листів, SMS і посилань у соцмережах. Вони використовують особливість браузерів в iOS, які приховують адресний рядок після відкриття сторінки. Після цього, під приводом захисту у користувача вимагають реквізити Apple ID (обліковий запис, використовувана для виконання будь-яких дій пов'язаних із Apple, включаючи завантаження додатків), пароль та інші дані, що дозволяє отримати доступ до інформації на пристроях, а також до систем мобільного банку. Таким чином шахраї отримують доступ до особистої інформації користувача та купівель, що зберігається в iCloud, які власник аккаунта здійснив у фірмовому магазині iTunes Store, в окремих випадках – до даних банківської карти.

Експерти додають, що схожа схема може використовуватися і для пристроїв під управлінням ОС Android.

Нагадаємо, у лютому нинішнього року в ОС смартфона iPhone знайдена чергова помилка, яка дає можливість отримати доступ до файлів девайса, навіть якщо він захищений паролем.

Раніше повідомлялося, що iPhone 5, який раніше лідирував у споживчих рейтингах, утратив звання найулюбленішого телефону серед користувачів.

Нагадаємо, що в Німеччині смартфон на Android зуміли зламати завдяки холодильнику ***(Зловмисники знайшли спосіб викрадати особисті дані користувачів iPhone 5 // Корреспондент.net (http://ua.korrespondent.net/business/web/1593220-zlovmisniki-znajshli-sposib-vikradati-osobisti-dani-koristuvachiv-iphone-5). – 2013. – 16.08).***

***

Кибер-атака неизвестных хакеров на компьютерную базу данных министерства энергетики США стала причиной утечки персональной информации 14 тыс. нынешних и бывших сотрудников этого ведомства.

По сообщению ведомства, злоумышленники, в частности, могли получить номера социального страхования граждан, которые часто используются в

различных мошеннических схемах.

Однако, опять же по сообщению ведомства, хакеры, чье проникновение в информационную систему Министерства энергетики произошло в конце июля, не смогли получить доступ к какой-либо секретной информации, в том числе касающейся ядерного комплекса и ядерного оружия США.

Служба безопасности и компьютерные специалисты минэнерго вместе с экспертами из других федеральных ведомств расследуют обстоятельства инцидента. Людям, персональные данные которых могли оказаться в руках злоумышленников, в случае необходимости обещана помощь со стороны правительства ***(Хакеры атаковали базу данных минэнерго США // InternetUA (http://internetua.com/hakeri-atakovali-bazu-dannih-minenergo-ssha). – 2013. – 17.08).***

***

Модифицированный вирус, ранее использовавшийся для кражи данных кредитных карт, генерирует лайки в Instagram.

В настоящее время социальные медиа находятся на пике своей популярности и имеют огромное значение для создания репутации. В связи с этим, хакеры используют свои навыки для продажи таких знаков одобрения в соцсетях, как лайки и подписчики.

Злоумышленники модифицировали ранее использовавшееся для кражи данных кредитных карт вредоносное ПО Zeus для генерации фальшивых лайков в Instagram. Об этом сообщило агентство Reuters со ссылкой на исследователей RSA. Поддельные знаки одобрения продаются на хакерских интернет-форумах «пачками» по 1 тыс. лайков в каждой. 1 тыс. подписчиков на Instagram обойдется честолюбивому пользователю в 15 дол., а тысяча лайков – в 30 дол. Отметим, что 1 тыс. номеров кредитных карт стоит в несколько раз дешевле – всего 6 дол.

Казалось бы, что от номеров кредитных карт должно быть больше пользы, чем от знаков одобрения в соцсетях, однако маркетологи считают, что компании с большой охотой будут использовать фальшивые лайки, чтобы «раскрутить» новый продукт и прибавить ему популярности. «Люди обращают внимание на то, что модно. Эффект повального увлечения», – заявил старший аналитик компании WordStream В. Пэн.

Модифицированный Zeus контролирует зараженные компьютеры с центрального сервера, заставляя из генерировать лайки для конкретного пользователя. Инфицированные системы также могут получать команды участвовать в других операциях или загружать другое вредоносное ПО.

С тех пор как вирус начал свою деятельность пять лет назад, кибер-преступники использовали его для заражения сотен миллионов компьютеров. То, что Zeus модифицирован для Instagram, свидетельствует о возрастающей значимости социальных медиа ***(Хакеры модифицировали Zeus для Instagram // InternetUA (http://internetua.com/hakeri-modificirovali-Zeus-dlya-Instagram). – 2013. – 20.08).***

***

Видоизмененный вариант Ramnit, изначально представляющего собой банковское вредоносное ПО, был обнаружен экспертами безопасности из Trusteer при анализе атаки на пользователей игрового клиента Steam от Valve. Вирус осуществляет инъекции вредоносного кода в веб-браузер платформы, в результате чего злоумышленникам удается скомпрометировать учетные данные геймеров.

Напомним, что впервые червь Ramnit был обнаружен еще в 2010 г. Тогда его основным методом распространения являлось заражение исполняемых файлов HTML и Microsoft Office на локальном компьютере.

В настоящий момент возможности вируса были расширены и дополнены такими функциями, как хищение куки-файлов и учетных данных FTP (хранящихся локально), а также перехват процессов браузера для осуществления MitB (man-in-the-browser) атаки, в рамках которой Ramnit изменяет web-формы и внедряет вредоносный код в web-страницы.

Кроме того, по словам аналитика Trusteer Э. Маора, обнаруженный вариант червя способен обойти интегрированную в Steam криптозащиту (она используется при авторизации), а также оставаться незамеченным для системы обнаружения атак, работающую на серверах Valve ***(Хакеры используют вирус Ramnit в ходе атак на пользователей Steam // InternetUA (http://internetua.com/hakeri-ispolzuuat-virus-Ramnit-v-hode-atak-na-polzovatelei-Steam). – 2013. – 21.08).***

***

Мобильные вирусы стремительно развиваются, и в первом полугодии 2013 г. их количество увеличилось на 180 %. По данным экспертов немецкой антивирусной компании G Data, за первые шесть месяцев текущего года было обнаружено свыше 519 тыс. новых вредоносных программ для ОС Android, тогда как во втором полугодии 2012 г. этот показатель составил примерно 185 тыс. Ежедневно продукты G Data детектировали 2868 новых зловредов, нацеленных на пользователей этой платформы. Примечательно, что в первом полугодии прошлого года было обнаружено чуть больше 29,5 тыс. новых угроз.

На сегодняшний день Android является абсолютным лидером среди мобильных платформ по количеству нацеленных на нее вредоносных программ. Это объясняется не только распространенностью гаджетов, работающих на этой ОС, но и доступностью появившихся в последнее время специальных инструментов (malware kit), с помощью которых создание зловредов становится под силу даже не самым опытным пользователям. Более того, вирусописатели все чаще стали маскировать вредоносный код в приложениях, что затрудняет анализ такого ПО. В результате зараженное приложение долго остается активно на устройстве и может использоваться злоумышленниками в корыстных целях.

Большинство (46 %) новых мобильных угроз для Android составляют

троянские программы, нацеленные среди прочего на кражу банковской информации или отправку платных СМС-сообщений на премиум-номера. Одним из ярких образцов подобного рода зловредов стал троянец FakeSite.A, известный также как Perkele. Он отличается тем, что вирусописатели могут использовать его с любым другим вредоносным кодом, который действует как обычный банковский троянец. Таким образом, киберпреступники используют кросс-платформенное вредоносное ПО, например, для перехвата СМС-сообщений, содержащих коды авторизации, которые банки отправляют клиентам своих онлайн-сервисов.

«Сегодня, чтобы стать вирусописателем, к сожалению, не требуется обладать особыми техническими навыками. Доступность в Интернете специальных инструментов только способствует распространению опасных технологий, которые помогают кибер-преступникам зарабатывать незаконным путем, что видно на примере троянца Perkele. Анализируя сложившуюся тенденцию, можно с уверенностью сказать, что ситуация будет и дальше развиваться, и во втором полугодии количество новых вредоносных программ для Android может увеличиться втрое», – отмечает Э. Вильямс, антивирусный эксперт G Data ***(Количество мобильных угроз для Android за полгода увеличилось на 180 % // InternetUA (http://internetua.com/kolicsestvo-mobilnih-ugroz-dlya-Android-za-polgoda-uvelicsilos-na-180). – 2013. – 21.08).***

***

Сеть микроблоггинга Twitter отвергает обвинения хакера, утверждающего, что он смог скачать пользовательские данные, в том числе пароли, из базы данных Twitter. В самой компании говорят, что никаких нарушений систем безопасности замечено не было.

Хакер, известный под именем Mauritania Attacker, представляющий одноименную западно-африканскую страну, сегодня заявил, что ему удалось получить доступ к полной базе данных Twitter. Индийский ИТ-сайт Techworm, связавшийся с хакером, пишет, что ему, якобы удалось скачать данные множества пользователей на локальный компьютер.

Однако сам сайт предполагает, что не Twitter, как таковой, стал жертвой хакинга, а стороннее приложение, работавшее с сетью микроблогов. В результате ошибок в приложении под угрозу были поставлены примерно 15 тыс. пользовательских аккаунтов. «Мы исследовали ситуацию и можем подтвердить, что никакие Twitter-аккаунты не были скомпрометированы», – заявили в Twitter.

Так или иначе, но на файлообменном хостинге Zippyshare хакером были размещены OAUTH-ключи, которые в теории можно использовать для входа в пользовательские аккаунты многих пользователей Twitter. Такие ключи используются для верификации подключающихся к Twitter приложений. Сами по себе они не обладают достаточными для входа в аккаунт полномочиями, однако их можно применять, как промежуточное звено в атаке ***(Twitter отрицает информацию о взломе аккаунтов // InternetUA***

(http://internetua.com/Twitter-otricaet-informaciua-o-vzlome-akkauntov). – 2013. – 22.08).

***

В соцсети Facebook может сохраняться часть персональных данных пользователя даже после удаления его аккаунта, если пользователь ранее пересылал их своим друзьям. Об этом заявил в четверг журналистам член Совета Федерации Р. Гаттаров после встречи с директором Facebook по коммуникациям с органами государственной власти Т. Кристенсеном.

«В таком случае пользователь, удаливший свой аккаунт, не имеет возможности повлиять на ранее отправленные персональные данные», – сказал Р. Гаттаров.

По словам Р. Гаттарова, Т. Кристенсен заверил, что Facebook не предоставляет неконтролируемого доступа к своим серверам с данными пользователей американским спецслужбам.

Кроме того, Р. Гаттаров сказал, что Т. Кристенсен признал возможность передачи компанией Facebook некоторых персональных данных пользователей компаниям-разработчикам сервисов для их развития.

Относительно предоставления персональных данных разработчикам Р. Гаттаров заявил, что такой механизм, в принципе, допустим, однако целесообразно соответствующим образом доработать действующее российское законодательство для придания полной легитимности этой практике. Что касается участия Facebook в международной конференции по защите персональных данных, то, по информации Р. Гаттарова, компания пока не приняла решения об участии в ней.

Следующие встречи по вопросу соблюдения конфиденциальности данных пользователей будут проведены с представителями компаний Twitter и южнокорейской компанией LG, заявил сегодня Р. Гаттаров.

«К LG есть много вопросов, в отличие от Samsung», – сказал Р. Гаттаров ***(Данные пользователей Facebook остаются у третьих лиц // InternetUA (http://internetua.com/dannie-polzovatelei-Facebook-ostauatsya-u-tretih-lic). – 2013. – 22.08).***

***

Пока жертвы пытаются отразить атаку, злоумышленники похищают миллионы из систем онлайн-банкинга.

Как отметили исследователи компании Gartner, в последнее время кибер-преступники начали использовать DDoS-атаки на компьютерные системы банков, в качестве отвлекающих маневров, за борьбой с которыми жертвы не замечают хищение огромных денежных средств из сервиса онлайн-банкинга.

По словам представителей исследовательской компании, им удалось обнаружить, по крайней мере, три случая, когда под видом DDoS-атаки на американские банки, злоумышленники под их прикрытием проникали в системы незамеченными, поскольку специалисты занимались отражением

атак.

Примечательно, что в Gartner не говорят, какие именно американские банки пострадали от атак, однако за последние несколько месяцев целая группа финучреждений США, в том числе JP Morgan, Wells Fargo, Bank of America, Chase, Citigroup, HSBC, сообщала о проводимых в их отношении DDoS-атаках.

«Это были не политически мотивированные группы. Организаторы ставили перед собой цель вывести сайты банков из строя всего на несколько часов, то есть сама DDoS-атака не была их конечной целью, – отмечает А. Литан, вице-президент Gartner в интервью SCmagazine. – Когда DDoS-атака в самом разгаре, группа мошенников переключается на атаку платежных систем и систем онлайн-банкинга, пытаясь получить расширенные привилегии в системе» ***(Хакеры используют DDoS-атаки в качестве отвлекающих маневров // InternetUA (http://internetua.com/hakeri-ispolzuuat-DDoS-ataki-v-kacsestve-otvlekauasxih-manevrov). – 2013. – 23.08).***

***

Как сообщают исследователи безопасности из Symantec, в их распоряжении оказался образец вредоносной программы вымогателя, использующей довольно непривычные приемы мошенничества. Вместо угрожающих сообщений о штрафах и уголовном преследовании, ориентированный на китайских граждан вирус просто меняет учетные данные текущего пользователя Windows и перезагружает систему.

После этого жертвы злоумышленников, как правило, не могут вернуть себе доступ и для того, чтобы разобраться в ситуации связываются с создателем вируса через популярный в Китае IM-сервис – свой ID вирусописатели заботливо разместили на экране авторизации.

Далее злоумышленники требуют выплатить им 20 китайских юаней, что равняется примерно 3 дол., в обмен на которые пользователю предоставляется новый пароль.

«Вирус написан на простом языке программирования и большей частью распространяется через популярный китайский сервис мгновенных сообщений», – поясняют эксперты Symantec. По их словам, проанализированный образец всегда генерирует один и тот же пароль – tan123456789.

Вместе с тем исследователи отмечают, что для нейтрализации действий вируса пользователю достаточно авторизоваться в любой другой учетной записи с правами администратора и сбросить пароль для заблокированной учетной записи ***(Вирус вымогатель изменяет учетные данные пользователей Windows // InternetUA (http://internetua.com/virus-vimogatel-izmenyaet-ucsetnie-dannie-polzovatelei-Windows). – 2013. – 23.08).***

***

Несколько тысяч сайтов, зарегистрированных в национальном

китайском домене .cn, подверглись масштабной DDoS-атаке в воскресенье, 25 августа. Об этом сообщает The Wall Street Journal.

Атака, которую правительство страны называет крупнейшей в истории страны, началась в воскресенье в два часа ночи по пекинскому времени. В четыре часа утра за первой волной атаки последовала вторая, еще более мощная. В результате значительная часть всего китайского Интернета оказалась недоступна для пользователей.

По данным информационного центра China Internet Network, ликвидировать последствия DDoS-атаки и полностью восстановить доступ к интернет-ресурсам удалось лишь к утру 26 августа.

М. Принс, генеральный директор компании CloudFlare, специализирующейся на защите интернет-ресурсов от DDOS-атак, сообщил, что атака на китайский домен вызвала падение общего интернет-траффика в стране на 32 %.

В КНР установлена одна из самых сложных систем фильтрации Интернета, что, однако, не делает китайский сегмент сети неуязвимым от подобных атак. Сам Китай регулярно фигурирует в многочисленных отчетах как одна из главных стран – источников DDOS-атак. На долю Китая приходится от 38 до 55 % всех совершаемых DDOS-атак в мире ***(Китай подвергся самой мощной DDOS-атаке в своей истории // InternetUA (http://internetua.com/kitai-podvergsya-samoi-mosxnoi-DDOS-atake-v-svoei-istorii). – 2013. – 26.08).***

***

Как следует из недавнего отчета исследователей Cisco, группа хакеров, называющих себя Сирийской электронной армией (Syrian Electronic Army), вероятнее всего прибегает к услугам третьих лиц для осуществления атак на сайты различных СМИ. Более того, для тех порталов, чей контент генерируется сторонними компаниями, риск компрометации заметно увеличивается.

Отметим, что Сирийская электронная армия неоднократно брала на себя ответственность за атаки на множество различных медиа-ресурсов. Только за текущий год участники группировки заявляли о нападении на Twitter, Thomson Reuters, The Associated Press и The Guardian.

22 августа представители The Washington Post признали, что их web-сайт стал жертвой атаки, а инициировавшие нападение злоумышленники выступают в поддержку режима текущего президента Сирии Б. Асада. Аналогичная ситуация на прошлой неделе сложилась вокруг онлайн-каналов CNN.

Исследователь Cisco Д. Шульц в своем блоге пояснил, что определить метод нападения стало возможным после анализа аналогичных инцидентов, связанных с файлообменниками Outbrain и ShareThis.

«Согласно поиску whois доменное имя sharethis.com зарегистрировано через GoDaddy на компанию Akamai. Однако начиная с 21 августа их DNS-

серверы были привязаны к серверам Сирийской электронной армии», – пояснил Д. Шульц ***(Хакеры из Сирийской электронной армии используют услуги третьих лиц для атак на СМИ // InternetUA (http://internetua.com/hakeri-iz-siriiskoi-elektronnoi-armii-ispolzuuat-uslugi-tretih-lic-dlya-atak-na-smi). – 2013. – 26.08).***

***

Гаджеты, как и их ПО, уязвимы, и главная задача разработчиков усовершенствовать обе стороны так, чтобы у злоумышленников было как можно меньше шансов попасть в ваш телефон или компьютер. Таков главный итог конференциия по информационной безопасности Black Hat USA-2013. Однако эксперты согласны не со всеми угрозами. Вот что рассказал IT Expert И. Здобнов, главный вирусный аналитик компании «Доктор Веб», комментируя наиболее резонансныеугрозы.

Перехват трафика пользователя – сегодня реальность в умелых руках. Как это легко сделать, используя усилители сигнала мобильной сети от компании Femtocell, продемонстрировали на Black Hat USA-2013. И здесь аналитик согласен – проблема реальна.

«Такие устройства на самом деле применяются для построения локальных 3G-сетей. И речь тут идёт об уязвимом оборудование компании Verizon. В принципе, нет ничего удивительного в том, что можно перехватить трафик от этих устройств к провайдеру», – объяснил И. Здобнов.

Еще одна вполне реальная угроза – внедрение в приложение для Android вредоносного кода, оставляя нетронутым сертификат разработчика.

«Уязвимость, действительно, реальная и мы уже успели обнаружить вредоносную программу, которая её использует. Android.Nimefas.1.origin способен отправлять СМС-сообщения, передавать злоумышленникам конфиденциальную информацию пользователей, а также позволяет удаленно выполнять ряд команд на инфицированном мобильном устройстве. На данный момент троянец распространяется в большом количестве игр и приложений, доступных для загрузки в одном из китайских онлайн-каталогов приложений для Android. Тем не менее, не исключено, что в ближайшее время число эксплуатирующих уязвимость Master Key вредоносных программ увеличится, и, соответственно, расширится география распространения угрозы», – говорит главный вирусный аналитик «Доктор Веб».

Тогда как главная сенсация конференции – взлом iPhone при помощи модифицированного специальным образом зарядного устройства, по словам эксперта, давно уже не новость.

«Устройство представляет собой маленький компьютер на базе Linux. Для того, чтобы получить доступ к iPhone используется специальный механизм профилей разработанный Apple для разработчиков софта. Причем для получения доступа требуется получения специального сертификата с сайта Apple и тут проблема в том, что на сайте отсутствует capcha, поэтому этот

процесс удалось автоматизировать. Выглядит это, конечно, эффектно, но на деле это и так все знали», – объяснил И. Здобнов.

Опроверг аналитик и данные об исследовании, что в мире фишинговых атак наблюдается новая опасная тенденция – вместо создания вредоносных писем от якобы надежного источника, злоумышленники все чаще прибегают к попыткам имитации стиля письма тех или иных людей, опираясь на их сообщения в социальных сетях.

«На самом деле такого исследования не было. Было проведено исследование возможностей использования методов NLP (Natural Language Processing) для составления профиля человека по анализу его Twitter. И одного такого исследования явно недостаточно, чтобы делать далекоидущие выводы», – резюмировал он.

Напомним, конференция по информационной безопасности Black Hat USA проходит уже 16 лет подряд и привлекает внимание хакеров, консультантов по безопасности и правительственных агентов по всему миру. В 2013 г. по ее итогам издание ITProPortal составило «топ-10 самых страшных событий Black Hat-2013».

Как известно, в ходе мероприятия большинство исследователей посвящают слушателей во все подробности той или иной уязвимости. Такое публичное раскрытие информации призвано привлечь к проблеме общественное внимание и заставить разработчиков исправить ситуацию ***(Троянец в Android отправит по смс конфиденциальную информацию пользователей // InternetUA (http://internetua.com/troyanec-v-Android-otpravit-po-sms-konfidencialnuua-informaciua-polzovatelei). – 2013. – 24.08).***