СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1–13.07)

2014 № 13

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1–13.07)
№ 13

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

© Національна бібліотека України
імені В. І. Вернадського, 2014

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

В Интернете в настоящее время можно найти много социальных сетей на любой вкус и выбор. Запорожец О. Мелешко решил доказать, что Украина так же способна на создание мощной сети с большой аудиторией. Он разработал проект под названием GetBetUp.

Социальная сеть рассчитана на жителей всех стран. Она не имеет языкового барьера или ориентации на определенную аудиторию. Помимо возможности свободного общения с друзьями, каждому участнику представится на выбор перечень реальный заданий, по типу, найти в своем городе улицу на букву «А», сделать фото в плаще и шляпе в центре города, собрать на одном фото 10 любых кухонных атрибутов. Выполняя их за определенное время, будут начисляться баллы, которые, в свою очередь, определяют уровень и количество опыта пользователя. Чем выше уровень, тем больше привилегий и других интересных возможностей, таких как создание своих собственных заданий, участие в соревнованиях, тотализаторах и т. д.

Кроме того, участники могут организовываться в группы, вместе или по-отдельности принимать участие в батлах, в которых необходимо выполнить одно или несколько заданий. Для этого нужно всего лишь бросить или принять вызов соперников и, конечно же, победить. Создатель проекта отмечает, что это уникальный шанс оторвать интернет-пользователей всей планеты от экранов компьютера и предоставить возможность быть более активными в реальном мире.

Большая часть сайта уже сделана и в настоящее время находится на стадии тестирования.

Проект уже нашел большую поддержку среди украинских и зарубежных пользователей, а официальное открытие планируется в конце августа ***(Житель Запорожья открыл новую соцсеть // ZaБор (http://zabor.zp.ua/www/content/zhitel-zaporozhya-otkryl-novuyu-sotsset). – 2014. – 28.06).***

***

Компания Google заявила о планах закрыть социальную сеть Orkut – один из старейших проектов компании, первую попытку выйти на рынок соцсетей, так и не увенчавшуюся мировым успехом. Об этом сообщается в специальном справочном разделе на сайте Google.

При заходе по адресу orkut.com происходит перенаправление на страницу в справочной службе Google, где говорится о том, что платформа соцсети будет полностью закрыта 30 сентября 2014 г.

До тех пор доступ к аккаунтам будет работать по-прежнему: пользователи смогут заходить в соцсеть, играть в игры и общаться с друзьями, однако завести новый аккаунт стало невозможным уже 30 июня.

Помимо этого, Google удалит официальные приложения Orkut из App Store и Google Play.

Тем, кто хочет сохранить свои данные, предлагается уже сейчас экспортировать свои фотографии в Google+, а также воспользоваться инструментом Google Takeout для сохранения копии всего доступного контента на компьютер. Этот инструмент продолжит свою работу до сентября 2016 г.

Как отмечается в официальном прощальном письме в корпоративном блоге, после создания Orkut у Google появились такие проекты, как YouTube, Google+ и Blogger. Их рост превзошёл развитие Orkut, поэтому компания сконцентрируется на развитии этих сервисов. Представители Google не упоминают Facebook и Twitter в записи, как и не говорят о текущих показателях Orkut по аудитории.

Orkut был создан в 2004 г. в рамках инициативы «20 процентов», по которой сотрудники Google тратили часть своего рабочего времени на сторонние проекты. По своей функциональности – поиск друзей, объединение в группы по интересам – он напоминал MySpace и Facebook.

В Twitter возмущение закрытием Orkut преимущественно испытывают португалоговорящие пользователи.

Известно, что Orkut был преимущественно популярен в Бразилии и других странах с португальским языком. По состоянию на 2008 г. в сервисе было более 120 млн зарегистрированных пользователей, больше половины которых было из Бразилии, следующей по популярности шла Индия. В 2011 г. Facebook обошёл Orkut по популярности в Бразилии, сообщалось в исследовании comScore ***(Google закроет одну из старейших соцсетей Orkut // InternetUA (http://internetua.com/Google-zakroet-odnu-iz-stareishih-socsetei-Orkut). – 2014. – 1.07).***

***

За последние двое суток количество регистраций в «ВКонтакте» из Бразилии увеличилось в три раза, сообщил Г. Лобушкин на своей странице в «ВКонтакте». В настоящее время в социальной сети зарегистрировано почти 300 тыс. бразильских пользователей.

Резкий рост популярности «ВКонтакте» в Бразилии может быть связан с тем, что 30 июня Google заявил о закрытии своей социальной сети Orkut. Она была наиболее популярна именно в этой стране – в 2011 г. ею пользовалась шестая часть населения, сообщает Forbes. Но к концу 2012 г. большинство пользователей перешли на Facebook. Аудитория Orkut в Бразилии сократилась до 4 млн человек ***(«ВКонтакте» стал популярен в Бразилии из-за закрытия Orkut // InternetUA (http://internetua.com/vkontakte--stal-populyaren-v-brazilii-iz-za-zakritiya-Orkut). – 2014. – 3.07).***

***

В Twitter в самом скором времени появится новая функция: публикация ретвитов с развернутыми комментариями. «Опция пока что не доступна для всех, – отметили представители Twitter. – Сейчас мы тестируем развернутые комментарии на ограниченном количестве блогеров. Если не столкнемся с какими-либо ошибками и проблемами – распространим на всех пользователей уже через несколько недель».

В настоящее время у пользователей сервиса микроблогов практически нет никаких возможностей: они могут публиковать твиты, ретвитить их и ретвитить с комментарием. Но комментировать не совсем удобно: чужой твит выглядит как цитата, выделяется кавычками и занимает часть из доступных 140 символов – на то, чтобы добавить свои мысли, места категорически не хватает.

«Развернутые комментарии дадут возможность заменить “цитаты”. Пользователи смогут чужой твит сопровождать полноценным комментарием в 140 символов. И дизайн таких ретвитов будет немножко другим. Оригинальная публикация форматом будет похожа на публикации с различным контентом: со снимками, видео и другими файлами, – говорят представители Twitter. – Пользователи часто жалуются, что 140 символов не хватает, чтобы полноценно выразить свои мысли. Развернутые сообщения помогут частично исправить ситуацию. Но увеличивать длину твитов мы не будем. Это – то, благодаря чему нас любят миллионы людей. Если бы сообщения не имели ограничений – мы стали бы одной из множества одинаковых социальных сетей» ***(У Твиттер появится новый формат ретвитов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/u_tvitter_poyavitsya_novyy_format_retvitov). – 2014. – 1.07).***

***

В одесской мэрии прошла встреча заместителя городского головы З. Цвиринько с победителями чемпионата Украины SAGE, одесскими школьниками, создающими социальную сеть для слабовидящих людей, сообщает пресс-служба муниципалитета.

Как передает «Репортер», одесситы победили в номинации «Лучший социальный проект» среди школьников. Во время встречи одесские школьники Б. Чубин («Приморский» лицей), А. Оганесян (гимназии №1 им. А. П. Быстриной), К. Коляновский (УВК «Гармония») и Э. Эюбов (ООШ №8) представили свой проект «Всемирная социальная сеть для слепых и слабовидящих людей».

Проект разработан с целью объединения всех слепых и слабовидящих людей на единой платформе. По замыслу разработчиков «Всемирная социальная сеть для слепых и слабовидящих людей» должна адаптировать инвалидов в социум и обеспечить комфортное проживание в городском

пространстве. Победители чемпионата планируют в 2014–2015 учебном году реализовать данный социальный проект и привлечь к нему волонтеров.

Также ребята рассказали о подготовке к чемпионату мира по молодежному предпринимательству международной программы SAGE-2014, который пройдет с 8 по 13 августа 2014 г. Победители украинского чемпионата будут готовиться по специальной программе все лето, чтобы достойно представить Украину ***(Одесские школьники разрабатывают соцсеть нового поколения // ИА «Репортер» (http://www.reporter.com.ua/news/mcq/). – 2014. – 7.07).***

***

В самой новой версии «смартфона Microsoft», в операционной системе Windows Phone 8.1, «ВКонтакте» сделают встроенным, базовым, приложением. Этой информацией поделилось руководство компании на официальном сайте.

Первым устройством с «ВКонтакте» станет Lumia 930. «Но это не значит, что предыдущие смартфоны серии не смогут скачать приложение нашей сети, – говорит Г. Лобушкин, пресс-секретарь. – Обновленной программой смогут пользоваться все, у кого есть телефон вплоть до 630 модели».

Смартфон будет исключительно интегрирован с сетью. Так, например, фотографии друзей, их активность, можно будет отслеживать прямо из записной книжки. Список друзей изначально представлен как список контактов. Хотя можно выбрать в настройках и иной вариант: и тогда контакты в устройстве и список друзей будут функционировать отдельно.

Более того, на мобильный «рабочий стол», из «ВКонтакте» можно перетянуть любимые иконки: самых близких друзей, любимые группы и так далее. Можно настроить автоматические обновления: как в целом по новостям, так и по отдельным сообществам, публичным страницам.

«Это глубочайший уровень интеграции, – утверждает Д. Рогозов. – Операционная система создана специальна для ВК. Смартфон дарит столько возможностей – и здорово экономит время, которого постоянно нам не хватает. Да и сам телефон получает невероятные возможности» ***(ВКонтакте будет интегрирована с Windows Phone 8.1 // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vkontakte_budet_integrirovana_s_windows_phone_8_1). – 2014. – 8.07).***

***

Крупнейшая в мире социальная сеть Facebook сообщила, что отныне будет обеспечивать повторное вовлечение пользователей в работу с приложением с помощью AppLinks.

Известно, что к большинству приложений пользователи обращаются лишь один раз, а затем либо удаляют, либо больше никогда не возвращаются

к его контенту. Чтобы несколько исправить ситуацию, Facebook предлагает разработчикам, рекламирующим свои приложения в социальной сети, использовать AppLinks для перенаправления пользователей прямо в интересующие их разделы приложений. Таргетинг будет осуществляться на основе интересов и поведения пользователей мобильных устройств.

Возможность применения функционала уже доступна для тех, кто работает с одним из Preferred Marketing Developers Facebook. В дальнейшем возможно расширение числа «доверенных разработчиков».

Основная цель запуска кросс-платформенной системы глубоких ссылок AppLinks сводилась к тому, чтобы предоставить разработчикам Open source функционал, который позволит сделать переход по ссылкам для пользователей мобильных устройств более прозрачным и удобным.

Добавив всего несколько строчек программного кода, разработчик получит возможность перелинковки мобильных приложений, а пользователи мобильных устройств, кликая по ссылкам, смогут мгновенно осуществлять переходы в нужные разделы приложений.

Для упрощения процесса копирования и размещения тегов разработчики мобильных приложений могут использовать App Links Hosting API . Если же перенаправление в мобильное приложение осуществляется с веб-сайта, разработчику необходимо разместить программный код в хедере.

Согласно внутренней статистике социальной сети, мобильное приложение Facebook Ads for Apps обеспечило клиентам до 350 млн загрузок приложений за апрель. Это очень хороший показатель, демонстрирующий, что Facebook может стать серьёзным источником привлечения пользователей для своих клиентов.

Впервые функционал глубоких ссылок в приложениях был представлен на конференции для разработчиков F8, которая проходила 30 апреля 2014 г., в Сан-Франциско ***(Facebook обеспечит повторное вовлечение пользователей в работу с приложением с помощью AppLinks // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_obespechit_povtornoe_vovlechenie_polzovateley_v_rabotu_s_prilozheniem_s_pomoschyu_applinks). – 2014. – 8.07).***

***

У Росії незабаром буде запущена соціальна мережа для депутатів усіх рівнів, пише газета «Известия». Ресурс буде називатися «Парламентський портал», – portal.parlament.gov.ru, пише Корреспондент.net (http://ua.korrespondent.net/world/russia/3390517-u-rosii-ziavytsia-sotsmerezha-dlia-deputativ).

Проект ініціювали в Держдумі в рамках створення у Росії «електронного парламенту». Крім самих народних обранців, на їхнє запрошення в соцмережі зможуть завести акаунти експерти – юристи, політологи й економісти. Що стосується простих користувачів, то вони

зможуть лише в режимі читання оцінювати ініціативи та обговорювати їх в інших соцмережах.

Як зазначає керівник робочої групи зі створення електронного парламенту, віце-спікер нижньої палати І. Лебедєв, на сьогодні в країні 245 тис. депутатів різного рівня, які недостатньо консолідовані. За його словами, складність політичного порядку вимагає кооперації професіоналів.

І. Лебедєв упевнений, що новий майданчик дає змогу не тільки організувати дискусію з будь-якої ініціативи депутата в режимі реального часу, а й залучити до неї депутатів з різних регіонів Росії.

На сьогодні система допрацьовується, і модератори ресурсу готуються до масової розсилки депутатам інформації про запуск парламентської соцмережі. Ініціатори зазначають, що основна робота має бути з оповіщенням муніципальних депутатів, яких у країні близько 200 тис. осіб.

За інформацією видання, на сайті передбачено серйозні заходи захисту від фейкових акаунтів. Через величезну кількість депутатів муніципальних утворень представники влади, перш ніж завести акаунт, повинні будуть надіслати модераторам підтвердження про депутатство: номер посвідчення, посилання на офіційні сайти або персональні сторінки в соцмережах тощо.

Депутати всіх рівнів повинні будуть розмістити інформацію про себе. Крім того, передбачена можливість додавати посилання на інші соцмережі, якщо там у користувачів вже є свої сторінки.

Система пошуку на сайті передбачає кілька основних фільтрів. Усі депутати розбиваються на рівні: федеральний, регіональний, муніципальний. Також стоїть фільтр розбивки парламентаріїв і експертів за алфавітом, партією і комітетом, у якому вони працюють.

У повноправних користувачів буде можливість розмістити на «Парламентському порталі» готову статтю. Крім того, як обіцяють розробники, на сайті передбачена інтернет-агрегація, і щодо кожного депутата досьє зможе автоматично оновлюватися залежно від його мережевої активності ***(У Росії з'явиться соцмережа для депутатів // Корреспондент.net (http://ua.korrespondent.net/world/russia/3390517-u-rosii-ziavytsia-sotsmerezha-dlia-deputativ). – 2014. – 10.07).***

***

Социальная сеть Facebook представила новую версию приложения Facebook Messenger 7.0, оптимизированного под экран iPad.

Новая версия бесплатного приложения доступна для загрузки пользователями из iTunes и Apple App Store .

Примечательно, что разработчики предпочли сохранить традиционный интерфейс мессенджера, несколько доработав его функционал. Так, в Messenger 7.0 были исправлены программные ошибки, улучшилась функция голосового общения.

Важным нововведением стало появление возможности сохранения видеороликов, снятых с помощью приложения, в разделе «Фотопленка».

Однако функция отправки видеосообщений в версии iPad пока недоступна ***(Facebook представил версию Messenger для iPad // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_predstavil_versiyu_messenger_dlya_ipad). – 2014. – 9.07).***

***

В сети появился новый онлайн-сервис LikeManager, анализирующий данные пользовательских Facebook-аккаунтов. С помощью данного сайта можно получить развернутый список всего, что пользователь когда-либо лайкал в крупнейшей социальной сети. Это своеобразный браузер по таким записям, каждую из которых можно перечитать и получить актуальную информацию о том, сколько лайков, шейров и комментариев она собрала по состоянию на сегодняшний день. Также этими записями можно поделиться и таким образом извлечь их из «Facebook-забытия», пишет AIN.UA (http://ain.ua/2014/07/09/532116).

Все понравившиеся пользователю посты отфильтрованы по рубрикам «Все», «Лайки и линки постов друзей», «Посты, которыми делился я», «Лайки сторонних постов». Таким образом, можно посмотреть выборки по записям во френдленте, собственной истории, и отфильтровать контент сторонних сайтов, который вы оценили посредством социальной кнопки Facebook. Также можно отфильтровать записи по типу контента: статьи, видео, фото и прочее.

Сервис запустила команда португальского стартапа ColorElephant, который занимается бизнес-сервисами в области маркетинга, разработки и техподдержки. LikeManager можно использовать, пройдя аутентификацию через Facebook. Однако бесплатно сервис обрабатывает только 30 лайков в неделю. Чтобы получить больше, придется подписаться на премиум-пакет за 1 евро (1,36 дол.) в месяц.

На первый взгляд, сервис абсолютно бесполезен, ведь вывести на экран все, что вы когда-либо оценили, можно и внутри самого Facebook. Для этого существует раздел «Журнал действий». Однако никто не станет спорить, что LikeManager значительно упрощает эту задачу, хотя и не совсем понятно, чем это может быть полезно бизнесу.

Крупнейшая в мире социальная сеть становится благодатной почвой для создания разнообразных анализирующих сервисов, поскольку является гигантским хранилищем информации о каждом пользователе. Например, с помощью приложения Five Labs можно нарисовать портрет личности по своим постам. А сервис-пузомерка Publicast от украинских разработчиков позволяет узнать степень вашего влияния в Facebook ***(Яровая М. Сервис LikeManager позволяет перечитать все, что вы лайкали в Facebook // AIN.UA (http://ain.ua/2014/07/09/532116). – 2014. – 9.07).***

***

Из 5 новых украинских соцсетей выжило две с половиной

В апреле этого года украинские разработчики анонсировали сразу пять национальных соцсетей, которые, по их словам, должны были составить серьезную конкуренцию ресурсам М. Цукерберга и П. Дурова. Всего в течение двух недель было запущено пять проектов – WEUA.info, Druzi.org.ua, Antiweb.com.ua, Ukrface.net и Combine.pp.ua. С того времени прошло три месяца. AIN.UA решил выяснить, как развиваются «революционные» соцсети и удалось ли их разработчикам воплотить свои планы в жизнь (http://ain.ua/2014/07/11/532263).

WEUA.info

Проект WEUA.info был запущен первым среди украинских соцсетей 1 апреля 2014 г. Разработчики запустили его в надежде, что пользователи откажутся от использования российских социальных сетей, в которых их ждет антиукраинская пропаганда. На сегодня в соцсети зарегистрировано около 160 тыс. пользователей из разных регионов Украины. Каков среди них процент «живых» пользователей – неизвестно, но, как и в любом проекте, здесь хватает ботов и технических аккаунтов. Сразу же после регистрации мы получили семь новых заявок в друзья от торговцев различными товарами и услугами. В целом же, интерфейс соцсети совмещает в себе элементы «ВКонтакте» и Facebook. Что интересно, проект уже переведен на семь различных языков – украинский, русский, английский, арабский, белорусский, крымскотатарский и словенский. По словам создателя сети Б. Олиярныка, в настоящее время проект ищет инвестора и заканчивает работу над редизайном сайта. «Через каких-то 3–4 месяца мы презентуем новый WEUA 2.0. Это будет совершенно новый сайт с новыми возможностями, новыми подходами к программированию и новой сути», – уверен Б. Олиярнык.

Druzi.org.ua

Спустя несколько дней после анонса WEUA на просторах уанета появилась еще одна социальная сеть – druzi.org.ua. Если верить статистике, то на сегодняшний день в новой соцсети зарегистрировано почти 200 тыс. пользователей, и эта цифра постоянно растет. Интерфейс сайта внешне напоминает Facebook и «ВКонтакте». Одним из серьезных отличий является то, что в качестве основного языка страницы можно выбрать только украинский.

Из интересных особенностей – в соцсети присутствует онлайн-ТВ с 16-ю каналами и онлайн-радио (несколько сотен каналов). Кроме того, в «Друзях», неплохой выбор социальных игр. Из минусов – сравнительно большой процент рекламных ботов и рекламы.

Antiweb.com.ua

«Антивеб» позиционировалась как антисоциальная сеть для жителей Ровно. По словам разработчиков, с ее помощью можно будет находить друзей по интересам. Для этого на сайте планировалось создавать встречи и

ставить им определенные метки. Например: «Собираемся на концерт группы Metallica, только парни от 18 лет, встреча без употребления алкоголя». После окончания встречи ее можно будет оценить по пятибальной шкале и опубликовать фотографии.

Судя по всему, планы разработчиков не осуществились – на сегодня в соцсети зарегистрировано всего 170 пользователей, а последнее событие датировано апрелем этого года.

Ukrface.net

Регистрация в этой соцсети должна была начаться 5 апреля в 12:00. По словам ее создателей, проект был нужен стране для объединения востока и запада страны в борьбе против иностранной пропаганды. Запуск соцсети происходил со сбоями – сайт постоянно падал, а на следующий после запуска день и вовсе оказался недоступен. Позже проект переехал на адрес Ukrface.com.ua. В настоящее время в сети зарегистрировано чуть больше 3 тыс. человек, есть общий чат и браузерные игры. Больше, в общем-то, о проекте сказать нечего. Именно этому проекту отведена роль «половины» из заголовка статьи – назвать соцсеть с таким количеством пользователей работающим проектом не поворачивается язык.

Combine.pp.ua

Последняя социальная сеть со сложным названием и не менее сложной судьбой. Проект закрылся спустя несколько дней после запуска.

Кроме вышеназванных соцсетей, в Украине с переменным успехом существует еще около десятка действующих и полузаброшенных проектов. Помимо относительно известных Connect.ua и Friends.ua, есть еще соцсеть «Українці», сайт для «реальных пацанов» vReale, соцсеть для женщин Pink Planet, для ученых – Science-community.org и торговая соцсеть Kb.ua. Не выдержали конкуренции и закрылись соцсеть для шоу-бизнеса Katmary.net, сеть для «тусовщиков» Tuse.ua, соцсеть для профессионалов Profeo.com.ua и Friendin.net, в которую, по словам создателей, инвесторы вложили 1,5 млн дол. ***(Ворона Т. Из 5 новых украинских соцсетей выжило две с половиной // AIN.UA (http://ain.ua/2014/07/11/532263). – 2014. – 11.07).***

***

Сеть микроблогов Twitter будет предоставлять статистику по просмотрам отдельных сообщений и страниц пользователей в целом, сообщается в официальном блоге компании.

Подсчитываться будут просмотры, сделанные через обычную версию сайта twitter.com, а также через приложения для мобильных устройств на базе iOS и Android.

Нововведение поможет сети микроблогов исполнять закон о блогерах, вступающий в силу в России 1 августа. По новым правилам, блогеры, чьи страницы в соцсетях набирают более 3 тыс. просмотров в сутки, должны быть зарегистрированы в специальном реестре Роскомнадзора.

Такие интернет-пользователи обязаны будут публиковать только проверенную информацию, не размещать на своих страницах запрещенную российским законодательством информацию ***(Twitter начнет показывать статистику просмотров блогов // InternetUA (http://internetua.com/Twitter-nacsnet-pokazivat-statistiku-prosmotrov-blogov). – 2014. – 13.07).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Президент України П. Порошенко повідомив, що віднині всі його приватні акаунти переводяться в сторінки, які підтримуватиме його команда, а особисті пости починатимуться з двох літер «ПП».

Про це він повідомив у відеозверненні на своїй сторінці у Facebook.

Президент зазначив, що протягом останніх років спілкування через соцмережі переросло у взаємодію зі всією країною.

«Але з початком моєї роботи на посту Президента України подій і приводів для повідомлень стає все більше, а мій графік не завжди передбачає наявність Інтернету і часу, щоб оперативно вас інформувати», – зауважив П. Порошенко.

Саме тому він вирішив ініціювати процес об’єднання і переведення приватних акаунтів у сторінки, які підтримуватиме його команда, а всі особисті пости починатимуться з двох літер «ПП» – Петро Порошенко.

«Друзі, все тільки починається! Ще раз дякую вам! Разом – сила! Слава Україні!» – додав він ***(Порошенко ініціював процес об’єднання своїх акаунтів у соцмережах // iPress.ua (http://ipress.ua/news/poroshenko_initsiyuvav_protses_obiednannya_akauntiv_u_sotsmerezhah_73486.html). – 2014. – 7.07).***

***

Офіційний Twitter Адміністрації Президента України почав роботу 11 липня ***(Адміністрація Президента України відкрила свій Twitter // Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3391213-administratsiia-prezydenta-ukrainy-vidkryla-svii-Twitter). – 2014. – 11.07).***

***

Министр иностранных дел П. Климкин решил всерьез взяться за реформирование внешнеполитического ведомства Украины.

«У меня есть желание и амбиции создать настоящую европейскую дипломатическую службу, которой мы и каждый украинец сможет гордиться», – сказал П. Климкин, обращаясь к сотрудникам МИД.

«У меня будет отдельный е-мейл, к которому имею доступ только я. Каждый из вас сможет предложить идею, которую вы считаете стоящей для команды, которая будет продвигать реформу МИД», – пообещал П. Климкин.

Для реализации задач в качестве инструментов реализации внешней политики будут использоваться все современные популярные технологии, в частности Skype, Facebook и Twitter и др.

«Давайте используем время, которое у нас есть, чтобы стать действительно европейской дипломатической службой», – отметил П. Климкин ***(МИД реформируют с помощью Skype, Twitter, Facebook и личного e-mail министра // IT Expert (http://itexpert.org.ua/rubrikator/item/36723-mid-reformiruyut-s-pomoshchyu-skype-twitter-facebook-i-lichnogo-e-mail-ministra.html). – 2014. – 2.07).***

***

У соціальній мережі Facebook з'явилася публічна сторінка голови Вінницької облдержадміністрації А. Олійника. У першому пості губернатора йдеться про поновлення АТО на Сході України. Також А. Олійник закликає вінничан не втрачати пильність, а представників влади не зловживати терпінням людей:

«Президент України Петро Порошенко за підсумками засідання Ради Національної Безпеки і Оборони України прийняв рішення зупинити дію режиму одностороннього припинення вогню на Донбасі.

Це означає, що українські силовики знову перейшли у наступ та отримали повноваження від Глави держави для використання усіх потужностей у боротьбі за територіальну цілісність України, за мир та спокій на нашій землі» ***(Губернатор Винничины Анатолий Олийнык открыл свою страницу в Фейсбуке // РЕАЛ (http://real-vin.com/губернатор-винничины-открыл-свою-стр). – 2014. – 1.07).***

***

На Днепропетровщине о децентрализации можно будет узнать на Facebook и в Twitter

Для информирования о децентрализации «продвинутой» части населения, на Днепропетровщине создали специальный сайт комитета по реформированию местного самоуправления.

Во время пресс-конференции в Днепропетровской ОГА советник председателя облгосадминистрации С. Юхименко сообщил о важности информирования населения области о сути децентрализации. Именно с целью разъяснения и информирования был создан интернет-сайт и странички в соцсетях.

«Одним из главных условий успешного проведения децентрализации на Днепропетровщине является желание и готовность общества проводить реформирование и брать на себя за это ответственность, – считает С. Юхименко. – Очень важно, чтобы как можно больше людей на местах

смогли разобраться в сути процесса и узнавать последние новости. Для этого в городах и районах области будет проводиться разъяснительная работа. Уже разработан информационный буклет, где в схематичном виде рассказывается о реформе местного самоуправления».

Советник председателя ОГА напомнил, что в области был создан специальный комитет по реформированию местного самоуправления, куда вошли ведущие специалисты ОГА.

«Для контакта с “продвинутой” частью населения, мы разработали специальный сайт комитета. В процессе разработки страницы на Facebook и в Twitter. Для обслуживания этих страниц будут привлекаться волонтеры. Мы будем активно вести диалог, дискуссию с молодежью через социальные сети, чтобы их привлечь к организации этих реформ, – отметил С. Юхименко.

Чтобы жители сел, где не всегда есть Интернет, могли ознакомиться с предлагаемыми реформами, будет распространяться буклет «Реформа местного самоуправления». Он выпущен тиражом около 1 тыс. экземпляров.

Как мы сообщали ранее, на Днепропетровщине дадут возможность общественности контролировать работу местной власти и участвовать в принятии важных решений, Днепропетровщину учат, как ликвидировать областные и районные администрации ***(На Днепропетровщине о децентрализации можно будет узнать на «Facebook» и в «Twitter» // 0564.ua – Сайт города Кривого Рога (http://www.0564.ua/news/571276). – 2014. – 8.07).***

***

Запорожцы смогут получить консультацию социальных работников, не выходя из дома – через Интернет. Об этом сообщает пресс-служба городского совета.

Одной из последних разработок управления соцзащиты горсовета стало внедрение онлайн-консультаций с использованием программы Skype для граждан, которые проживают в Жовтневом районе. Также этой услугой могут воспользоваться представители общественных организаций и предприятий этого района.

Консультации предоставляются согласно графику, в котором указана фамилия специалиста, в каком отделе он работает, а также его логин в Skype ***(В Запорожье соцработники начнут консультировать по Skype // РепортерUA (http://reporter-ua.com/2014/07/08/v-zaporozhe-socrabotniki-nachnut-konsultirovat-po-skype). – 2014. – 8.07).***

***

Украинские политики сравнительно недавно открыли для себя социальные сети. Оказалось, что формат сухих обращений от пресс-служб нравится народу куда меньше, чем иллюзия человечности и близости, которую так просто создать постами и фото в Facebook, «ВКонтакте» или Twitter (пусть даже над текстом трудился не сам политик, а целый штат

копирайтеров). Редакция AIN.UA предлагает вам подборку нестандартных SMM-приемов, которые используют украинские политики и их пресс-службы, чтобы понравиться народу (http://ain.ua/2014/07/03/531197).

Самые интерактивные

Как ни странно это прозвучит, но один из примеров интерактивности в социальных сетях подал еще прошлый Кабмин: бывший премьер Н. Азаров каждую пятницу проводил сессию «вопросов-ответов», хотя в большинстве «допущенных» на стену вопросов не было критики, а с началом Майдана гневные посты украинцев, вызванные приостановлением евроинтеграции, вычистили со страницы чиновника.

В настоящее время самой интерактивной, пожалуй, можно назвать Facebook-страницу министра МВД А. Авакова, где он не только постит частые отчеты о деятельности своего ведомства, но и отвечает на комментарии.

Причем тексты министра весьма далеки от формального языка релизов, очень эмоциональны и кажутся благодаря этому очень искренними и непосредственными, как будто политик действительно переживает за свое дело. Пользователи такой подход ценят: у Авакова уже почти 200 тыс. подписчиков на странице.

Вообще, формат Facebook-отчетов перед народом сейчас популярен: например, заместитель министра образования И. Совсун постит в сети отчеты за неделю, где перечисляет, чем занималось ведомство.

А министр юстиции П. Петренко недавно выложил целый фотоотчет о том, как без предупреждения ездил по центрам предоставления админуслуг и о том, какие очереди там увидел.

Мэр Львова А. Садовый еще за время Майдана успел прославиться своими взвешенными и продуманными видеообращениями по ситуации. В настоящее время мэр не только ведет популярную (52 тыс. подписчиков) страницу на Facebook, но и записывает регулярные видео для YouTube (например, вот обращение перед выборами президента). Кстати, именно он вдохновил одного из самых известных украинских стартаперов пойти в политику.

Не все политики поступают так же. У недавно избранного Президента П. Порошенко также есть страница в Facebook, но постов там – не очень много. А в профиле не обновлена информация о новом месте работы.

Ботоводы

В украинском политическом SMM уже давно бытует термин «юлеботы»: многочисленные и часто безымянные поклонники Ю. Тимошенко, которые заявляются в комментарии к любой новости с ее упоминанием.

Но Ю. Тимошенко – далеко не единственный политик, чьи PR-специалисты используют такие приемы. В январе журналисты Watcher расследовали внезапный рост популярности аккаунтов В. Медведчука, который недавно опять появился на политической арене. В Twitter, к

примеру, у политика 320 тыс. читателей! Еще в январе добавлялись фоловеры пачками: целый день количество могло не меняться, а за пару часов вырасти на несколько тысяч, пишет издание. Причем некоторые пользователи искренне удивлялись, откуда твиты В. Медведчука взялись у них в ленте.

Самые эпатажные

Самым эпатажным политиком Украины вполне можно назвать депутата О. Ляшко. Но в SMM он прославился еще и тем, что у него из украинских политиков, наверное, больше всего подписчиков во «ВКонтакте» – около 150 тыс.

А самый известный и эпатажный Instagram-аккаунт, конечно же, у харьковского городского главы Г. Кернеса. Его «хипстерские луки», фото занятий спортом, еды и другие любимые народом фотосюжеты собирают по несколько тысяч лайков.

Охотники за призоловами

В этой номинации – пока что только SMM-команда бывшего киевского мэра Л. Черновецкого (теперь он, кстати, в том числе занимается стартапами). В настоящее время на его Facebook-страничке проводится конкурс с призовым фондом в 3000 дол. Пользователям предлагается поделиться конкурсными работами на тему: «Пути и способы преодоления экономического кризиса в Украине». За первое место обещают 1500 дол. ***(Карпенко О. SMM-приемы украинских политиков: хипстер-луки, боты и розыгрыш денег // AIN.UA (http://ain.ua/2014/07/03/531197). – 2014. – 3.07).***

***

Где узнавать новости районов Киева в Facebook и «ВКонтакте»

Социальные сети – не только для селфи, котиков и фото из отпуска. В Facebook и «ВКонтакте» представлены многие районы Киева – в группах Нивок, Борщаговки, Троещины, Позняков общаются их жители, узнают районные новости, помогают друг другу искать врачей или строителей, реализовывать идеи по благоустройству района, бороться с незаконной застройкой и даже искать украденные вещи и пропавших питомцев, пишет AIN.UA (http://ain.ua/2014/07/08/531898).

Сайт DreamKyiv сделал подборку основных сообществ районов города. Предлагаем краткую информацию о том, кто ведет районные сообщества Киева, сколько там подписчиков и какие темы обсуждаются.

Голосеево

Страница была создана осенью 2012 г., в настоящее время у нее около 700 подписчиков. Ее ведет digital-стратег А. Деньга. По ее словам, активность на странице началась с Майдана, когда на Теремках создали блок-пост. В настоящее время страница дает развлекательную и полезную информацию: данные об отключении горячей воды, о перекрытии улиц и т. д.

Нивки

У района есть группа в Facebook – «Нивка – паблик ровного района», созданная в январе 2014 г. Количество подписчиков страницы – 683, над контентом работают 10 человек. Во «ВКонтакте» также есть группа района, количество ее подписчиков – более 2500. Курирует движение «Нивка» А. Можаев, руководитель агентства Wanted.

В пабликах есть проект «Свои для своих» – бесплатная реклама местного бизнеса в обмен на скидки для нивчан, а также фотопроект «Ровные люди» – об активистах района.

Оболонь

Группа Оболони в Facebook работает с октября 2012 г., на нее в настоящее время подписано 2438 пользователя. Группа интересна тем, что здесь часто публикуют старые архивные фото района. Автор проекта – Г. Антоненко, по его словам, идея появилась потому, что местных СМИ у района в то время просто не было.

Здесь публикуется очень разнородная информация: позитивные фото раскрашенной в цвета национального флага Оболонской набережной, фото маньяка, нападавшего на жителей района. В настоящее время, конечно, одна из основных тем, которые волнуют жителей района, – графики отключения горячей воды.

Позняки

Эта группа – проект деятелей искусства из «Фундації Центр Сучасного Мистецтва» «Нам стало интересно, как искусство может влиять на публичные места и отношение к ним людей. Решили начать с Позняков, потому что это типичный спальный район с типичными проблемами», – рассказывает Л. Скринникова, координатор проекта. В июле планируют устроить в парке «Позняки» креативное пространство, где жители района смогут заниматься чем-то вместе: создавать уличные скульптуры, снимать кино о районе и т. д.

Позняки, Осокорки, Харьковский (ПОХ)

Сообщство ПОХ – одно из самых популярных. В Facebook-группе ПОХ – 6600 подписчиков, во «ВКонтакте» – более 10 000. Администрирует сообщество известный маркетолог А. Травкин. На Позняках недавно ночью сожгли одну из достопримечательностей – 6-метровую скульптуру орла. В группах уже собирают деньги на ее восстановление.

Русановка

Эта группа – закрытая, в ней около 800 подписчиков. Она была создана в декабре 2012 г., ее ведет известный предприниматель С. Баранский, который недавно выпустил собственную книгу «Сомнение», о том, как сделать свою жизнь лучше. Он рассказал DreamKyiv, что всегда хотел создать местный канал распространения информации, чтобы можно было найти сантехника на Русановку, придумать районный ивент или совместными усилиями закрыть наглое заведение, которое заняло пол-тротуара.

Дарница

Жители этого района сделали не только группу в Facebook, но и сайт. Основная цель сообщества – бороться с произволом чиновников, просвещать жителей района в правовых вопросах, бороться с незаконными застройками.

Подол

У старейшего района Киева есть и сайт, и группа во «ВКонтакте» (правда, малочисленная). В группе и блоге, который ведет программист Е. Антаков, размещаются новости района (например, о сносе исторических зданий), архивные фото района, отчеты с районных мероприятий, фото красивых граффити – ведь именно на Подоле появилось одно из самых красивых революционных граффити в Украине.

Печерск

Facebook-страница района была создана относительно недавно – в январе 2014 г., подписчиков у нее пока мало. В настоящее время на платформу Pecher.sk, цель которой – привлечь жителей к управлению районом – собирают средства краудфандом. Администратор сообщества, арт-менеджер В. Кадыгроб рассказывает, что его идея зародилась во время Майдана. Осенью на домене Pecher.sk планируют запустить полноценный интернет-ресурс с разными сервисами: контроль власти, районные новости, обсуждения, голосования, сборы средств на реализацию проектов, исследования.

Березняки

У района есть немногочисленная группа в Facebook. Там публикуются новости района, объявления о новых магазинах, утерянных вещах, ретро-фотографии.

Осокорки

У этого района также пока немного поклонников в группе.

Борщаговка

Группа в Facebook создана совсем недавно – в апреле 2014 г. На создание группы частного предпринимателя и жителя района подтолкнула борьба с незаконной застройкой. «В одиночку бороться сложно, а объединившись, можно сделать свой район лучше и дать отпор тем, кто мешает нам спокойно жить», – рассказал он в комментарии DreamKyiv.

Троещина

Еще одна недавняя группа – создана в мае этого года, у нее пока чуть больше 200 подписчиков. Ее администратор С. Полоз рассказывает, что с помощью группы удается повлиять на чиновников: «Бывает, прорвало теплотрассу или лифт сломался, а ЖЭК на это не реагирует. Люди пишут, жалуются, и чиновники начинают шевелиться». В группе огранизовываются субботники для уборки зон отдыха ***(Карпенко О. Где узнавать новости районов Киева в Facebook и «ВКонтакте» // AIN.UA (http://ain.ua/2014/07/08/531898). – 2014. – 8.07).***

***

С 26 июня этого года в Facebook действует пресс-центр АТО, где публикуются новости, фото и видео из районов боевых действий в восточных областях Украины. У страницы уже более 3400 подписчиков. Ведет ее пресс-секретарь Генштаба Вооруженных Сил А. Дмитрашковский. Он же часто выступает как спикер АТО в новостях.

По словам А. Дмитрашковского, в группе публикуются материалы из первых рук, их помогают готовить журналисты и операторы. А. Дмитрашковский не стал уточнять, какие издания они представляют или же являются штатными сотрудниками ВСУ.

Пока читательская активность на странице невысокая. Если посты министра МВД А. Авакова о событиях в районах боевых действий собирают по 200–1000 перепостов и сотни комментариев, то на странице пресс-центра комментариев и перепостов пока немного ***(Официальная страница АТО запустилась в Facebook // IT Expert (http://itexpert.org.ua/rubrikator/item/36721-ofitsialnaya-stranitsa-ato-zapustilas-v-facebook.html). – 2014. – 2.07).***

***

Херсонцы в соцсети «ВКонтакте» создали группу «Сдай сепаратиста». Цели группы определены четко: Тот, кто против Украины, против своей родины, тот предатель и враг украинского народа!!!

Вот, что написано в описании группы:

«В эту группу вылаживаются фото и ссылки на страницы сепаратистов города Херсона, а так же можно вылаживать и с других городов сепаратистов, террористов и диверсантов. Люди должны знать в лицо своих “ГЕРОЕВ”. Огромная просьба, не пишите на их адрес угрозы и оскорбления, мы же нормальные, цивилизованные люди, в отличие от них, и не собираемся кого-то запугивать, вылавливать и устраивать расправу, мы просто будем их тихо ликвидировать без шума и пыли. На счёт ликвидировать, это шутка. Конечно...»

Ссылка: https://vk.com/club73664671 ***(Херсонцы в соцсети Вконтакте создали группу «Сдай сепаратиста» // Херсонська Правда (http://pravda.ks.ua/kherson_ks/important/23616-xersoncy-v-socseti-vkontakte-sozdali-gruppu-sdaj.html). – 2014. – 2.07).***

***

Создателя группы ВКонтакте «Горловка за независимую Украину» в родном городе представители ДНР разыскивают в разы сильнее, чем МВД пытается арестовать лишенного депутатской неприкосновенности О. Царева.

Его имя и настоящую фамилию пытаются выяснить не менее интенсивно, чем украинцы ищут ответ, кто все-таки скрывается в Facebook за псевдонимом Сер 3-М, – национальным разрушителем мифов, выкладывающим в сеть телефоны всех, кто ему не дорог.

Горловчанин снял маски со многих, кто взял оружие в руки и призывает к отделению Донбасса, агитирует в соцсетях за никем не признанную Донецкую народную республику и бахвалится военными «трофеями» – отобранными у бизнесменов автомобилями, ограбленными магазинами и приобретенным оружием.

«Горловка была, есть и будет частью независимой Украины», – написал в предисловии создатель группы…

Не менее интересная и следующая инициатива от патриотов Украины в Донбассе: создание азбуки сепаратистов.

На каждую букву – в ДНР найдется свой претендент, а то и двое. К примеру, Б. Блоха Елена, главный редактор «Муниципальной газеты, поддержка сепаратистов информационное сопровождение ДНР. Здесь же и другой кандидат: Бородай Александр. Российский пиар-технолог, на время ставший премьер-министром Донецкой народной республики...

Взломанная группа «Горловка за независимую Украину» во «ВКонтакте» – на второй день, после появления информации о ней в СМИ – прямое доказательство подконтрольности популярной социальной сети российским ФСБшным структурам.

…Группу возобновили по другому адресу.

Опять во «ВКонтакте» и с новыми историями предательства своей родины… ***(Билинский А Интернет-партизанщина Донбасса // LB.ua (http://ukr.lb.ua/news/2014/07/09/272349_internetpartizanshchina_donbassa.html). – 2014. – 9.07).***

***

Збирати факти щодо причетності Російської Федерації до підтримки терористів на сході України взялися громадські активісти. Для цього вони створили сайт dokaz.org.ua, на якому розміщують відповідні фото та відео.

Дев’яносто відсотків інформації координатори сайту беруть з відкритих джерел – це сторінки в соціальних мережах росіян, на яких ті зізнаються у своїй причетності до заворушень на Донбасі – зокрема, розміщують власні світлини зі зброєю.

Чимало фотографій – російської зброї з відповідним маркуванням та номерами військових частин. Головна мета порталу – збір та систематизація цих фактів, щоб потому Україна в міжнародних судах могла надати всі докази ***(Для збору інформації про причетність РФ до тероризму в Україні створено сайт // InternetUA (http://internetua.com/dlya-zboru--nformac---pro-pricsetn-st-rf-do-terorizmu-v-ukra-n--stvoreno-sait). – 2014. – 9.07).***

***

Активисты в социальной сети Twitter разыскивают сотрудников МТС и «Киевстар», которые готовы нарушить корпоративные правила и предоставить информацию о сепаратистах по мобильным номерам, передает корреспондент proIT.

Так, сообщается, что необходимо идентифицировать около 20 неизвестных, которые имеют непосредственное отношение к финансированию луганских террористов.

Также активисты просят помочь в идентификации владельцев российских мобильных номеров ***(Активисты пытаются «вычислить» сепаратистов по мобильным номерам // InternetUA (http://internetua.com/aktivisti-pitauatsya--vicsislit--separatistov-po-mobilnim-nomeram). – 2014. – 8.07).***

***

В Twitter начали публиковаться правки «Википедии» Конгрессом США

8 июля запущена особая учётная запись Congress-Edits в Twitter, которая сообщает о каждой правке «Википедии», производимой анонимно с IP-адресов Конгресса США. Особый бот, созданный программистом Э. Саммерсом, отслеживает анонимные правки с указанных IP-адресов и сообщает о них автоматически в Twitter.

За три дня с момента запуска с компьютеров Конгресса США трижды вносились правки в статьи «Википедии». Последняя касалась администратора Агентства международного развития Ш. Раджива – была просто исправлена грамматическая ошибка. До этого правка касалась рассказа о забавном случае встречи президента Б. Обамы с человеком в маске в виде лошадиной головы.

Хотя пока правки были вполне невинны, появление такой учётной записи позволит любопытным отследить историю изменений статей «Википедии» сотрудниками Конгресса США. К сожалению, система не позволяет отследить, кто именно производил изменения – были ли это ведущие политики страны или просто стажёры.

Интересно, что в 2006 г. издание The Sun опубликовало статью о том, что сотрудниками Конгресса США была отредактирована страница в «Википедии», касающаяся заседающего в Конгрессе демократа и М. Мигана. В результате правок исчезли упоминания о неисполненных предвыборных обещаниях. Сам М. Миган тогда отверг причастность к инциденту ***(В Twitter начали публиковаться правки «Википедии» Конгрессом США // InternetUA (http://internetua.com/v-Twitter-nacsali-publikovatsya-pravki--vikipedii--kongressom-ssha). – 2014. – 13.07).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Избыточный поток контента и ограниченность информационного пространства в ленте Facebook привели к тому, что компания начала применять фильтрацию сообщений по принципу релевантности интересам и «лайкам» самого пользователя. Однако в сложившейся ситуации многим компаниям, потерявшим органический трафик на своих страницах,

приходится искать новые пути взаимодействия с аудиторией, пишет Marketing Media Review (http://mmr.ua/news/id/issledovanie-5-sposobov-uluchshit-effektivnost-kontenta-v-facebook-40229/).

TrackMaven проанализировали 5804 страницы Facebook, охватывающих в общей сложности 1 578 006 сообщений, чтобы определить наиболее эффективные методы для распространения контента в социальной сети.

1. Время публикации.

Исследователи выявили наиболее эффективное время для публикации сообщений в Facebook. По их мнению, планирование контента на «пиковое» время оборачивается падением количества просмотров, «лайков» и комментариев.

В частности выяснилось, что контент, опубликованный в воскресенье, в несколько раз эффективнее с точки зрения взаимодействия с пользователем, чем публикации, размещенные в среду.

TrackMaven отмечают, что больше всего сообщений в Facebook появляется именно в обеденное время. Поэтому контент, публикуемый в нерабочее время (с 5 вечера до 1 ночи) получает самые высокие показатели взаимодействия.

2. Картинки.

TrackMaven ссылаются на тот факт, что мозг обрабатывает визуальные образы в 60 тыс. раз быстрее, чем текст.

Проведенное исследование показало, что сообщения с прикрепленными фотографиями получают на 37 % больше обратной связи от пользователя (комментариев, «лайков», «репостов»), чем текст без снимка.

3. Пунктуация в сообщениях.

TrackMaven выяснили, что пунктуация вызывает читателей на взаимодействие. Например, мы обнаружили, что использование восклицательных знаков привлекает подписчиков к взаимодействию с постом.

Восклицательный знак редко используется в Facebook – 71,17 % проанализированных сообщений не содержали его. Но сообщения, которые были с этим знаком, получали в 2,7 раза больше взаимодействия.

4. Хэштеги.

«Использование хэштегов в любой социальной сети приносит хорошие результаты», – отмечают исследователи.

Примерно одно из шести сообщений в Facebook содержит хэштег. Компании, которые включает его в свои сообщения, получают по крайней мере на 60 % больше просмотров, отмечают исследователи.

Мы обнаружили, что эффективность сообщения положительно коррелирует с ростом использования хэштегов. Хотя сообщения с одним или двумя хэштегами получают лучшие показатели, чем те, что публикуются с тремя или четырьмя. Однако с количеством хэштегов больше четырех наблюдается пропорциональный рост охвата контента.

5. Длина сообщений.

Около 33 % проанализированных сообщений содержало 10–19 слов. Большинство текстов на Facebook – 57,21 % – не содержит больше 20 слов.

Наши данные показали положительную корреляцию между количеством слов и эффективностью сообщения. В частности, сообщение из 80–89 слов получает в два раза больше участия читателя.

TrackMaven объясняют это психологическим эффектом. Пользователи с большей вероятностью взаимодействуют с длинными сообщениями, потому что считают, что на их написание потрачено больше времени ***(Исследование: 5 способов улучшить эффективность контента в Facebook // Marketing Media Review (http://mmr.ua/news/id/issledovanie-5-sposobov-uluchshit-effektivnost-kontenta-v-facebook-40229/). – 2014. – 1.07).***

***

Рекламодатели продолжают увеличивать бюджеты на рекламу в социальных сетях. По данным последнего опроса среди маркетинговых агентств, 45 % респондентов заявили, что тратят от 1 до 10 % от общего бюджета маркетинга в социальных медиа, а 38 % говорят, что они тратят больше, чем 30 %, пишет Marketing Media Review (http://mmr.ua/news/id/skolko-reklamodateli-tratjat-na-facebook-twitter-i-youtube-40232/).

Facebook до сих пор остается основной социальной рекламной платформой – 84 % респондентов используют рекламный бюджет на него. На Twitter тратят рекламные бюджеты 74 % респондентов, на YouTube – 56 %.

63 % маркетологов говорят, что они ожидают увеличения расходов на Twitter в этом и следующем году, более 59 % сказали, что они будут делать то же самое и на Facebook.

73 % сообщили, что они используют рекламные сервисы Twitter, а 79 % из них используют Promoted Tweets.

65 % при этом отметили, что они тратят меньше, чем 10 % рекламного бюджета на рекламные твиты, предпочитая вместо этого использовать свой бюджет на поддержку и обслуживание аккаунтов.

Рекламодателей также говорят, что ROI для мобильной рекламы на Facebook и Twitter выше, чем на веб-версии ***(Сколько рекламодатели тратят на Facebook, Twitter и YouTube // Marketing Media Review (http://mmr.ua/news/id/skolko-reklamodateli-tratjat-na-facebook-twitter-i-youtube-40232/). – 2014. – 1.07).***

***

Влияние социальных сетей на работу CCO продолжает возрастать

Большинство контент-менеджеров (91 %) считают, что в ближайшие несколько лет социальные сети будут оказывать огромное влияние на их работу. 73 % CCO (Chief Content Officer) уже начали нанимать на работу больше экспертов в области соцмедиа.

Исследование The Rising CCO, основанное на ответах 203 специалистов из Северной Америки, Европы, Азиатско-Тихоокеанского региона и Латинской Америки, показывает, что на втором месте по степени влияния на работу CCO находятся мобильные технологии (73 %), а на третьем – видеопродакшен (69 %).

90 % главных контент-менеджеров сообщили, что размещение контента – стоит на первом месте в их списке дел, 58 % отметили, что сами создают и размещают контент, а 14 % рассматривают такую возможность в будущем.

Кроме того, в отчете сообщается о постепенной интеграции коммуникационной и маркетинговой сфер. 35 % опрошенных контент-менеджеров заявили, что выполняют в том числе и обязанности маркетологов (это на 26 % больше, чем в 2012 г.), а 84 % считают, что корпоративная репутация и репутация бренда становятся единым понятием.

Несмотря на растущее влияние социальных сетей, в ходе исследования также было установлено, что CCO продолжают полагаться на традиционные медиаканалы. Почти две трети респондентов (63 %) сообщили, что социальные сети и традиционные медиаканалы одинаково эффективны, 58 % опрошенных сказали, что каналы равны как в удержании покупателей, так и в привлечении новых клиентов (54 %).

Традиционные медиаканалы рассматриваются как более эффективные с точки зрения публикаций финансовых отчетов (76 %) и повышения узнаваемости руководителей компаний (54 %), тогда как социальные сети более эффективны в привлечении новых талантов (56 %) ***(Влияние социальных сетей на работу CCO продолжает расти // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vliyanie_sotsialnyh_setey_na_rabotu_cco_prodolzhaet_rasti). – 2014. – 2.07).***

***

Сеть микроблоггинга Twitter сообщила о покупке компании TapCommerce, специализирующейся на мобильной рекламе. Технологии TapCommerce применяются на мобильной версии сайта eBay, а также в мобильных играх финской Supercell. Созданные компанией мобильные платформы виртуально подходят для любых типов мобильного контента, включая видео, а также встраиваемое программное обеспечение. Кроме того, TapCommerce имеет в своем портфолио систему виртуальных помощников, которые упрощают работу с мобильным контентом и мобильной рекламой.

Официально сумма сделки не разглашается, но по данным интернет-проекта Recode, она составила около 100 млн дол.

Напомним, что за последнее время Twitter сделала несколько поглощений, связанных с мобильной рекламой и мобильными сервисами. Кроме того, в сентябре прошлого года Twitter сделала крупное мобильное поглощение – за 350 млн дол. была куплена компания MoPub ***(Twitter покупает компанию TapCommerce // InternetUA***

(http://internetua.com/Twitter-pokupaet-kompaniua-TapCommerce). – 2014. – 2.07).

***

Сеть микроблогов Twitter в попытке увеличить собственные доходы добавила в рекламные заметки кнопку Buy Now.

Подобное решение позволит быстро перейти к покупке описываемого в сообщении товара. Впрочем, на данный момент новая функция находится на стадии тестирования, так что нажатие на Buy Now ни к чему не приводит.

Пока что кнопку размещают в рекламных объявлениях о продаже товаров в интернет-магазине Fancy. Предполагается, что после того как Twitter активирует кнопку, количество партнёров существенно увеличится.

Ранее компания Amazon, крупнейшая в мире по обороту среди продающих товары и услуги через Интернет, заявила о запуске нового сервиса, позволяющего совершать покупки в магазине через сервис микроблогов Twitter.

В Twitter будет публиковаться «карточка» товара с коротким описанием и специальными ссылками. Пользователь может добавить понравившийся товар в корзину на сайте Amazon, просто нажав на такую ссылку в ленте сообщений Twitter ***(В рекламных заметках Twitter появилась кнопка «купить» // Блог Imena.UA (http://www.imena.ua/blog/buy-now-buttons-twitter/). – 2014. – 3.07).***

***

Очередное приобретение Facebook – компания анонсировала покупку стартапа LiveRail, который занимается видеорекламой. Среди нынешних клиентов – канал ABC Family и третий по величине в мире видеохостинг Dailymotion. LiveRail объединяет маркетологов и рекламодателей, публикуя на веб и мобильных платформах примерно 7 млрд таргетированных видеороликов ежемесячно.

Сумма сделки соцсетью пока не разглашается, но, по разным данным, она варьируется от 400 до 500 млн дол.

LiveRail основан в 2007 г. и успел заручиться поддержкой крупных клиентов. Основным преимуществом сервиса является система торгов в реальном времени, по сути – это аукцион рекламных объявлений в live-режиме. Стартап занимается не только размещением рекламы, но и полноценной аналитикой, оповещая рекламодателей о том, какой контент приносит им наивысшие показатели. В LiveRail также есть система контроля за контентом, то есть система следит, чтобы рекламу алкоголя, табака и других лимитированных продуктов никогда не увидели дети.

Стартап ранее привлек 12 млн дол. от San Jose’s Pond Ventures, доход LiveRail достигал, по разным оценкам, от 60 до 100 млн дол. в год. В интервью TechCrunch 2013 г. фаундеры заявляли о планах выйти на IPO в 2014 г., но, по всей видимости, у Facebook было более выгодное (и

безопасное) предложение ***(Facebook приобрел Liverail для видеорекламы // Media бізнес (http://www.mediabusiness.com.ua/content/view/39889/126/lang,ru/). – 2014. – 3.07).***

***

Зачем пользователи заходят на страницы брендов в Facebook?

Люди подписываются на страницы брендов в Facebook по разным причинам – начиная от участия в конкурсах и заканчивая любовью к продуктам компании. Но когда пользователь переходит в Хронику страницы, как показывает недавнее исследование Accent Marketing, в большинстве случаев ему нужен клиентский сервис – 82 % людей используют Facebook, чтобы пообщаться с представителем бренда, пишет Marketing Media Review (http://mmr.ua/news/id/zachem-polzovateli-zahodjat-na-stranicy-brendov-v-facebook-40269/).

Кроме того, более 60 % пользователей используют страницы брендов в Facebook для поиска скидок и купонов (80 % из них относятся к поколению бейби бумеров).

47 % пользователей считают, что Facebook – это самый быстрый социальный медиа канал для решения вопросов клиентского сервиса, Facebook является наиболее популярным местом, где пользователи выражают как позитивный (40 %), так и негативный (30 %) опыт взаимодействия с брендом. Около половины пользователей (44 %) ожидают ответ от бренда именно в Facebook, в целом, 29 % потребителей обращаются к социальным медиа, чтобы решать проблемы клиентского сервиса. Тем не менее, только 7 % пользователей считают, что клиентский сервис в соцсетях находится на должном уровне.

Как показывают данные, пользователи все больше и больше относятся к социальным сетям, как к каналу общения с брендом. Соответственно, компаниям пора не просто вести монолог в соцмедиа, а учиться слушать, понимать и отвечать своему потребителю ***(Зачем пользователи заходят на страницы брендов в Facebook?// Marketing Media Review (http://mmr.ua/news/id/zachem-polzovateli-zahodjat-na-stranicy-brendov-v-facebook-40269/). – 2014. – 3.07).***

***

Социальная сеть для профессионалов LinkedIn запустила пилотную программу, предоставив отдельным рекламодателям возможность таргетировать рекламу на пользователей на внешних площадках. Для таргетинга применяются данные о пользователях, которым обладает социальная сеть.

Рекламную программу от LinkedIn уже протестировали такие агентства, как: Xaxis и Dstillery. Что касается отзывов клиентов об эффективности новой программы, то пока их мнения расходятся: одни

рекламодатели остались довольны результатами, другие же считают итоги запуска кампаний недостаточно удовлетворительными. По мнению последних, рекламные возможности, предоставляемые LinkedIn, не способны обеспечить достаточную вовлечённость пользователей в процесс взаимодействия с рекламой.

Еще одним нововведением от LinkedIn стало предоставление брендам доступа к рекламному инвентарю социальной сети через каналы автоматизированной закупки рекламы. Теперь рекламодатели могут покупать показы рекламы определённой аудитории в рамках частного аукциона.

В последнее время на Западе всё чаще говорят об эффективности частных RTB-аукционов ***(LinkedIn позволит таргетировать рекламу на внешних площадках на основе собственных данных о пользователях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_pozvolit_targetirovat_reklamu_na_vneshnih_ploschadkah_na_osnove_sobstvennyh_dannyh_o_polzovatelyah). – 2014. – 8.07).***

***

Как социальные сети влияют на SEO?

SEO стало гораздо сложнее, чем раньше. Если раньше комплексный интернет-маркетинг означал лишь красивое словосочетание, которым любили щеголять спикеры на конференциях, то в настоящее время, действительно, полноценный интернет-маркетинг может быть только комплексным.

Каналы маркетинга работают максимально эффективно в связке. В сегодняшних реалиях лишь комплексная работа может дать эффективную отдачу в конкурентных нишах. SEO уже никогда не будет прежним.

А начнем мы освещение данного вопроса со влияния SMM на поисковое продвижение.

Роль социальных сетей в SEO – устойчивый тренд, чье значение в факторах ранжирования будет только расти.

Мы склонны полагать, что в настоящее время есть четыре важных момента, по которым социальные сети влияют на SEO.

Социальные отклики

Ссылки с социальных сетей и активность в официальных сообществах (лайки, репосты, комментарии, количество подписчиков) формируют набор социальных откликов. Сами по себе ссылки в социальных сетях вряд ли заметно влияют на ранжировании сайта, поэтому краткосрочные маркетинговые решения в данной области (чаще всего речь идет о массовой закупке ссылок в твиттер и vk-аккаунтах) не работают. Но поисковые системы следят за сигналами с социальных сетей, и если данные сигналы будут постоянными – то поисковые системы будут учитывать их в качестве положительного фактора в ранжировании.

Важный фактор для новостной выдачи

Чем активнее пользователи делятся новостью в социальных сетях (со ссылкой на первоисточник), тем лучше для ранжирования в новостной выдаче (в оптимизаторской среде такую выдачу еще называют выдачей быстроробота). Это очень мощный фактор, который нельзя игнорировать новостным порталам.

Быстрая индексация

Как дополнительный бонус можно рассматривать быструю индексацию. Если поисковая система не успела проиндексировать новый материал на сайте, то есть вероятность, что поисковой робот перейдет на нее из социальной сети. А более быстрая индексация, в свою очередь, также положительно играет свою роль в новостной выдаче. Для коммерческих сайтов это означает более быстрый вывод сайта в ТОП.

Дополнительный канал трафика

Поисковые системы обращают внимание на то, как распределена доля поискового трафика от общей посещаемости. Если говорить упрощенно, то положительно, если доля поискового трафика не единственный источник трафика на сайт. И чем больше трафика с других каналов – тем лучше. Социальные сети в этом плане – хороший альтернативный канал трафика.

Решение:

Развивать представительства в социальных сетях, использовать ресурсы сайта для привлечения подписчиков (например, через виджеты, кнопок «Поделиться в социальных сетях» и т. п.). Будет очень кстати повышение квалификации ответственных лиц в направлении SMM (через посещение профильных конференций, семинаров).

Через раскрученные собственные сообщества новые материалы с сайта должны распространяться быстрее, чем через сайт, т. к. механизмы репостинга в социальных сетях – устойчивый пат терн ***(Как социальные сети влияют на SEO? // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/poiskovaya_optimizatsiya/novosti/kak_sotsialnye_seti_vliyayut_na_seo). – 2014. – 8.07).***

***

Facebook начал предоставлять части владельцев публичных страниц статистику ранжирования страницы в социальной сети по определённому региону и сегменту бизнеса. Теперь администраторы пабликов видят, как Facebook ранжирует их страницы по отношению к страницам конкурентами. Это дает возможность понимать, насколько видимой страница окажется в лентах заинтересованных пользователей, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-pokazhet-administratoram-rejting-stranicy-po-otnosheniju-k-konkurentam-40358/).

Возможность отслеживать рейтинг мотивирует владельца страницы делать все возможное для его повышения. Ведь если в общем рейтинге страница бренда занимает не первую строчку – это напрямую указывает на то, что у её владельца есть серьёзные конкуренты.

Так например, если компания, работающая в определённом сегменте бизнеса и в определённом регионе, занимает пятую строчку в рейтинге Facebook – данные об этом буду показаны в соответствующем разделе статистики. При этом посетителям страницы данная информация доступна не будет.

Пока функция работает в тестовом режиме, однако не исключено, что в ближайшее время разработчики запустят её для всех администраторов корпоративных страниц в Facebook.

Около года назад Facebook в тестовом режиме предоставил отдельным администраторам доступ к разделу Pages To Watch («Страницы для наблюдения»). Модуль, интегрированный в панель администраторов, позволяет представителям бизнеса осуществлять прицельный мониторинг за активностью на корпоративных страницах конкурентов.

В конце мая 2014 г. у администраторов пабликов появилась возможность создавать списки похожих страниц, а в последствии сопоставлять их ключевые показатели пользовательской активности со своими. Функция доступна в разделе статистики страницы ***(Facebook покажет администраторам рейтинг страницы по отношению к конкурентам // Marketing Media Review (http://mmr.ua/news/id/facebook-pokazhet-administratoram-rejting-stranicy-po-otnosheniju-k-konkurentam-40358/). – 2014. – 9.07).***

***

Как работают с Twitter самые крупные СМИ мира

Микроблоги воспринимаются как место для коротких записей, обмена интересными ссылками и короткими цитатами. Но на самом деле потенциал у Twitter намного больше, чем привыкли думать большинство пользователей этого социального сервиса, пишет Marketing Media Review (http://mmr.ua/news/id/kak-rabotajut-s-twitter-samye-krupnye-smi-mira-40352/).

Издание The Wall Street Journal публикует в сутки около 500–600 историй и статусов в своём микроблоге. С социальными медиа работают несколько редакторов, которые находятся в Нью-Йорке, Лондоне и Гонконге. Контент издания публикуется в разных соцсетях. У одного этого СМИ – 80 собственных профилей в Twitter, связанных с брендами редакции. Почти все их ведут лично редакторы, остальные автоматически наполняются контентом, ретранслируемым из ленты публикаций на основном сайте.

Крупные медиа-компании, такие как ABC News, агентство Associated Press, CNN, NBC News, The New York Times, USA Today и WSJ ведут свои микроблоги по-разному, но у каждого проекта Twitter – важная часть коммуникационной платформы.

Э. Карвин, редактор социальных медиа в AP, говорит, что агентство не использует автоматизацию для новостных аккаунтов. Основной принцип одного из самых известных новостных агентств – подводка для новости в социальной сети и заголовок с лидом на сайте не обязательно должны

совпадать. Заголовок и подводку никогда не дублируют, учитывая, что виджет Twitter Card показывает заголовок рядом с ссылкой. Автоматизацию иногда используют, но в основном контент оптимизируют и публикуют вручную.

В CNN соцмедиа-менеджер А. Гонзалез говорит, что весь контент с сайта транслируется на профили телеканала в соцсетях Twitter и Facebook. За размещение и редактирование постов отвечает команда из трех человек, но ещё редакция прибегает к помощи так называемых «социальных адвокатов» – добровольных помощников из числа поклонников и постоянных зрителей телеканала. Крайне редко публикуется просто заголовок с сайта и ссылка – так происходит только тогда, когда новость срочная, и нет времени придумывать подводку.

Чтобы контент хорошо воспринимала целевая аудитория, постоянно происходит сравнительное тестирование, ведутся разные эксперименты с контентом. Редакция уделяет много внимания подбору удачных заголовков, анализирует самые читаемые твиты и те, которые собирают наибольший отклик у читательской и зрительской аудитории.

Рост качественных результатов от публикуемого контента, который пишется и размещается вручную, отмечают и в медиа-группе NBC – CNBC. Работа с аккаунтами ведётся круглосуточно.

В издании The New York Times есть отдельный редактор, который курирует работу с основным профилем (здесь контент публикуется автоматически) и со страницами в других социальных сетях, помимо Twitter. Иногда в микроблоге публикуются статусы или ссылки на материалы, которые выбиваются из общего контекста, но отвечают текущим наиболее обсуждаемым темам. Это могут быть фотографии с места событий или инфографика; резонансная цитата известного публичного деятеля или комментарии сторон к опубликованной новости.

Как говорят в редакции издания, твиты, публикуемые вручную, набирают намного больше откликов и просмотров, чем те, которые размещают сервисы отложенной публикации. Редакция постоянно пробует новые форматы, заголовки, другие варианты подачи новостей и статей для аудитории микроблогов. Ньюзрум активно включён в работу с социальными сервисами, и Twitter – не исключение.

В USA Today говорят, что предпочитают публиковать и модерировать контент самостоятельно, не прибегая к сервисам автоматизации. Плановый тематический контент в микроблоге разбавляется за счёт использования горячих новостей и оперативных сводок, большое внимание уделяют фотоконтенту. В издании отмечают, что наибольший пользовательский отклик находят публикации в Facebook, хотя в Twitter ежесуточно публикуется намного больше материалов.

Самое известное деловое издание планеты The Wall Street Journal публикует записи в своём официальном микроблоге, также, вручную. Редакторы круглосуточно, посменно, контролируют работу с профилем в

Twitter, дают туда не только оперативные новости, но и ссылки на тематические рубрики и плановые ежедневные материалы. При этом стараются сохранять баланс между подборками и сводками, отдельными большими статьями и короткими новостями из общей ленты публикаций на основном сайте. Работа с контентом на основе тщательной модерации и публикации вручную приносит свои плоды. Если летом 2012 г. у WSJ было 1,5 млн подписчиков в Twitter, то к маю 2014 г. их число превысило 4 млн человек.

Помимо основного аккаунта издание ведёт несколько собственных региональных учётных записей, за которые отвечают редакторы в конкретных регионах, таких как Азия, Европа. Кобрендинговые аккаунты агентства без привязки к регионам или странам обычно автоматизированы: туда публикуются новостные ленты по соответствующим тематикам. В дополнение к текстовым статусам и ссылкам в Twitter издания периодически появляется инфографика, фотоснимки с места событий и другой релевантный медиа-контент.

А вот в ABC News используют гибридную технику создания и модерирования контента для микроблогов. Все посты и статусы здесь пишут сотрудники редакции вручную. А для публикации используют отложенный механизм размещения контента при помощи TweetDeck, аналогично поступают и с публикациями на официальной странице в Facebook. Для конкретных тематик или статей выбирается определённый промежуток времени, с учётом часовых поясов или времени активности той или иной целевой аудитории. Пиковыми периодами считаются утро и вечер – в это время новостная редакция ABC старается публиковать оперативные сводки, выпуски новостей и ссылки на эксклюзивный видео-, аудио- и текстовый контент.

Представители всех крупных СМИ сходятся в одном: неважно, насколько часто на протяжении дня вы публикуете новости или ссылки. Важен качественный подход, ручная модерация ответов и ретвитов, а также грамотная работа с целевой аудиторией, использующей микроблоги. И тогда результат будет не просто соответствовать ожиданиям главного редактора и менеджмента СМИ, но и превзойдёт их ***(Как работают с Twitter самые крупные СМИ мира // Marketing Media Review (http://mmr.ua/news/id/kak-rabotajut-s-twitter-samye-krupnye-smi-mira-40352/). – 2014. – 9.07).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Социологи из Гарвардского университета назвали одну из разновидностей «селфи» – «релфи» (relationship selfie), то есть автопортрет с любимым человеком, самым раздражающим типом фотографий из всех, которые пользователи публикуют в социальных сетях. Об этом сообщает Mirror Online, ссылаясь на исследование The Science of Relationships.

Эксперты, которые занимаются проблематикой современных любовных отношений, пришли к выводу, что «релфи» вызывает негативные эмоции у большинства подписчиков пользователя. Они отмечают, что публикация таких фотографий может даже привести к потере «френдов». В то же время выяснилось, что для друзей «релфи» – это признак начала серьезных отношений.

К такому мнению социологи под руководством доктора Б. Ли из Университета Хаверфорд пришли, проведя онлайн-эксперимент с участием 200 добровольцев.

На первом этапе исследования 200 испытуемых должны были просмотреть профили в Facebook с размещенными «релфи», романтическими статусами и без них. В итоге подавляющее большинство участников эксперимента заявили, что первый романтический статус о каком-либо человеке, указание его в качестве постоянного партнера в своем профиле, а также размещение «релфи» означает начало серьезных отношений.

Во время второго этапа 100 испытуемых просмотрели профили вымышленных людей. Одни из них часто публиковали «релфи» и статусы о своих чувствах к партнеру, а в других профилях такие записи и фотографии отсутствовали. Участники теста отметили, что профили с совместными «селфи» вызвали у них раздражение, а страницы без романтических автопортретов – симпатию.

Недавно вышло еще одно исследование, посвященное восприятию фотографий пользователями соцсетей. Эксперимент провел онлайн-сервис для туристов Top10.com. В итоге 44 % опрошенных добровольцев выбрали «селфи» как один из самых неприятных видов отпускных фотографий. При этом выяснилось, что автопортреты раздражают пользователей все же меньше, чем скриншоты прогноза погоды в месте пребывания. Против таких фото проголосовал 51 % испытуемых.

Замыкает тройку лидеров вид снимков под названием hot dog legs [дословно «ноги – хот-доги» – прим. Руформатор]. Дело в том, что многие любят фотографировать свои загорелые конечности на фоне моря, бассейна и так далее. «Ноги-сосиски» в соцсетях портят настроение настроение 32 %

опрошенных ***(Совместные «селфи» признали самыми раздражающими снимками в соцсетях // InternetUA (http://internetua.com/sovmestnie--selfi--priznali-samimi-razdrajauasximi-snimkami-v-socsetyah). – 2014. – 3.07).***

***

Facebook знає про вас більше, ніж ви могли собі уявити

Днями Facebook оголосив про те, що тепер рекламодавці зможуть налаштовувати таргетовану рекламу в соціальній мережі з урахуванням історії інтернет-активності користувачів. Це викликало бурю обурення серед захисників прав на приватність. Чи не перегинає Facebook палицю, вторгаючись в наші життя? Щоб розвіяти ілюзію права на приватне життя в Інтернеті, автори The Wall Street Journal розповіли про речі, які Facebook знає про нас.

1. Які сайти ви відвідуєте.

Відстежуючи дані cookies, Facebook отримує інформацію про те, які сайти ви переглядаєте. Наприклад, якщо ви шукали собі годинник в інтернет-магазині, то не дивуйтеся, якщо Facebook «вгадає» ваші бажання і почне вам показувати рекламу годинників.

Мобільна версія Facebook також використовує дані інших додатків, встановлених на вашому смартфоні. Це нововведення викликало чимало обурення з боку користувачів. У своє виправдання Facebook стверджує, що показ реклами, яка цікава користувачам, робить їх перебування на сайті більш приємним.

2. Як ви виглядаєте.

Багато легковажно використовують Facebook як сховище особистих фотографій. Але чи знаєте ви, що Facebook вміє розпізнавати обличчя на фотографіях не гірше нас із вами? Тобто якщо хто-небудь завантажить фотографію з вами або з зображенням людини, схожої на вас, Facebook запропонує йому зазначити вас на цій фотографії.

До речі, схожу технологію також використовує і Google, який спеціально для цього у 2011 р. придбав компанію, що спеціалізується на розпізнаванні осіб.

3. Куди ви ходите.

Якщо ви виходите в соціальні мережі зі свого смартфона, Facebook може відстежити ваше місце розташування і отримати інформацію про те, де ви працюєте, живете, робите покупки і відпочиваєте. У Facebook навіть існує функція «Друзі поблизу», за допомогою якої ви зможете отримувати повідомлення кожного разу, коли хто-небудь з ваших друзів буде перебувати недалеко від вас.

Інформацію про місцезнаходження Facebook також використовує для персоналізації реклами. Якщо ви часто чекінитесь у магазині морозива, рекламодавці будуть знати, що ви ласун.

4. Ваші стосунки.

Facebook групує ваших друзів за списками, серед яких родичі, друзі по університету, колеги тощо. Причому багато користувачів самостійно вказують свої зв'язки з іншими людьми, додаючи в профайлі батьків, сестер / братів, а також тих, з ким перебувають у романтичних стосунках. Просто перейшовши на сторінку користувача, ви зможете дізнатися про нього достатньо інформації, включаючи ім'я, вік, дату народження, членів сім'ї, місце проживання, місце роботи та багато іншого. Facebook також знає, кого ви шукали в соцмережі і як часто.

5. Чим ви цікавитеся.

Facebook пильно стежить за вашими інтересами, у тому числі за улюбленими фільмами, музикою, книгами тощо. Ви лайкнули пост про нову серію «Ігри престолів»? Не дивуйтеся, якщо Facebook почне показувати вам рекламу книг у жанрі фентезі.

Ви навіть не уявляєте, скільки інформації про вас можна отримати, просто відстежуючи ваші лайки. Facebook може навіть зробити висновки про ваші політичні погляди, якщо ви, приміром, будете лайкать пости демократів і ігнорувати республіканців.

Багато хто відчуває себе в Інтернеті набагато розкутіше, ніж у реальному житті, наївно вважаючи, що за монітором вони, як за кам'яною стіною. Але чи так це насправді? Передивіться ваші профайли в соціальних мережах. Чи не занадто багато особистої інформації ви виставляєте на загальний огляд? ***(Фейсбук знає про вас більше,ніж ви могли собі уявити // Інформаційний портал «Стик» (http://styknews.info/novyny/polityka/2014/07/09/feisbuk-znaie-pro-vas-bilshenizh-vy-mogly-sobi-uiavyty). – 2014. – 9.07).***

***

Исследователи из Агентства передовых оборонных исследовательских проектов (DARPA), входящего в состав Министерства обороны США, провели глобальное исследование, в ходе которого подвергло анализу записи пользователей в Twitter, Facebook, Digg, Reddit, Pinterest и на других популярных ресурсах с высокой пользовательской активностью. Об этом пишет The Guardian.

Исследованию подвергались как блоги обычных пользователей, так и страницы знаменитостей, включая Леди Гагу и Джастина Бибера, с целью понять, как именно распространяется информация в блогосфере и как она влияет на блогеров. В ходе анализа публикаций ученые изучили процесс появления интернет-мемов, а также нашли закономерности в поведении пользователей, в том числе – как и почему люди лайкают записи друг друга, репостят их и добавляют друг друга в друзья.

В DARPA отмечают, что анализу подвергались лишь те записи, которые были опубликованы в открытом виде, в то время как «подзамочные» публикации остались нетронутыми. Исследование может иметь большое значение для деятельности Министерства обороны США, говорят в

агентстве, поскольку оно раскрывает механизмы распространения информации и объединения людей по интересам ***(Военные США узнали, как рождаются мемы и ставятся «лайки» // InternetUA (http://internetua.com/voennie-ssha-uznali--kak-rojdauatsya-memi-i-stavyatsya--laiki). – 2014. – 10.07).***

***

Нещодавно створений шлюб може бути зруйнований через конфлікт у соціальній мережі, передає lenta-ua.net.

Такого висновку дійшли американські експерти, провівши детальний аналіз профілів користувачів в аудиторії, рівний півмільйону людей.

Так, з точки зору експертів-аналітиків, найбільшу небезпеку несе сварка віртуального характеру, яка виникає при листуванні молодого подружжя, які перебувають за різними комп'ютерами.

Найбільш значні проблеми, як вважають учені, формує відвідування людьми сторінок у соціальних мережах Twitter і Instagram.

Водночас відзначається, що під час нетривалого дослідження вчені зробили висновок, що тривалі за часом шлюби, укупі з дружніми романтичними зв'язками, не можуть бути зруйновані соціальною мережею ***(Соцмережі руйнують сім'ї // Фонд Рідна країна (http://kyiv.ridna.ua/2014/07/sotsmerezhi-rujnuyut-simji/). – 2014. – 9.07).***

***

Два года назад тысячи пользователей Facebook получили сообщение, что им запрещен доступ в социальную сеть, так как компания считает их ботами или подозревает в использовании подложных имен, повествует The Wall Street Journal. «Чтобы снова войти в сеть, пользователи были обязаны доказать, что они существуют на самом деле», – пишет обозреватель Р. Альберготти.

На деле Facebook знал, что большинство этих пользователей – реальные люди. «Сообщение было проверкой, направленной на совершенствование антимошеннических мер Facebook. В итоге ни один пользователь не лишился доступа навсегда», – сообщает газета.

Эксперимент был разработан отделом Data Science Facebook. «Это группа из трех дюжин исследователей, имеющих беспримерный доступ к одной из богатейших информационных сокровищниц мира: данным о передвижениях, размышлениях и эмоциях 1,3 млрд пользователей соцсети», – говорится в статье.

Внимание к этому отделу было привлечено на днях, когда стало известно об эксперименте, проведенном в 2012 г. «Новостные ленты без малого 700 тыс. пользователей Facebook подверглись манипуляциям: одни показывали больше позитивных записей, другие – больше негативных. Из эксперимента был сделан вывод: пользователи, которые видят больше

позитивного контента, с большей вероятностью пишут позитивные записи, и наоборот», – говорится в статье.

2 июля Ш. Сендберг, главный операционный директор Facebook, заявила, что эксперимент был «частью продолжающихся исследований, которыми компании занимаются для испытаний различных продуктов», а также что об эксперименте «сообщили неудачно».

Компания пообещала: после реакции на этот эксперимент «мы очень внимательно присматриваемся к процессу, чтобы внести новые усовершенствования».

По словам некого бывшего сотрудника отдела и сторонних экспертов, до последнего времени Data Science действовала почти без ограничений. Университетские исследователи, вероятно, были бы обязаны заручиться согласием участников эксперимента. «Но Facebook полагался на согласие пользователя относительно "Правил обслуживания", где в то время говорилось, что данные могут быть использованы для усовершенствования продуктов Facebook. Теперь правила гласят, что данные пользователей могут быть использованы для исследований», – говорится в статье.

«Процесса ревизии как такового не существует», – говорит Э. Ледвина, который с февраля 2012 г. по июль 2013 г. работал в Facebook исследователем данных. По словам Э. Ледвины, «любой в этой команде мог провести проверку». «Они вечно пытаются изменить поведение людей», – добавил он.

Facebook заявляет, что со времен исследования эмоций ужесточил регламент исследований в отделе Data Science.

Data Science был создан в 2007 г. и за это время провел сотни экспериментов. Газета перечисляет: изучались механизмы общения родственников, причины одиночества, распространение «социальных моделей поведения» через социальные сети. «В 2010 г. группа замерила, как "политические мобилизационные сообщения", разосланные 61 млн человек, побуждали пользователей соцсетей голосовать на выборах в Конгресс США в 2010 г.», – говорится в статье.

Ведущий автор исследования об эмоциях, социальный психолог А. Крамер заявил в интервью в 2012 г., что пришел в Facebook, так как это «крупнейшее полевое исследование в истории планеты», передает издание ***(СМИ: эксперименты «Фейсбука» проводились почти без ограничений // DailyUA (http://www.daily.com.ua/news/10/2014-07-193683.html). – 2014. – 3.07).***

Маніпулятивні технології

На Facebook зарегистрировали резкий наплыв украинских пользователей. Мистика какая-то, буквально несколько дней назад украинских пользователей социальной сети Facebook насчитывалось 2,6 млн

открытых аккаунтов, а 6 июля их стало уже на 200 тыс. больше и составило 2,8 млн. Почему открытых аккаунтов, а не пользователей, спросит пытливый читатель, а дело в том, что «живой» или активный пользователь и зарегистрированный аккаунт, который учитывает статистика Facebook, – две большие разницы.

Что такое 7,7 % прироста пользователей за короткий промежуток времени в каком-то социальном сегменте – это всплеск и серьезный. А если учитывать те 20,2 % прироста за последних шесть месяцев (470,2 тыс.) по сравнению с текущей неделей (200 тыс.), то напрашивается вывод – народ усиленно начал готовиться к выборам после отпускного периода.

Безусловно – в этих всплесках прироста украинского пользователя Facebook, кроме политического, есть и коммерческие замыслы, «проталкивание» своих товаров и услуг в социальные и народные массы. По всей видимости, большая половина руководителей наконец-то начала понимать реальную отдачу продвижения в соцсетях.

Однако за такой короткий период времени не может быть такого ажиотажа паломничества в Facebook – скорее всего 80–90 % этих аккаунтов предназначены для политиражирования несуществующих или нереальных людей, работа у них такая, «человек-оркестр» в социальных сетях.

С развитием соцсетей, их популярности и проникновения в страны, растут и побочные эффекты – пользователь соцсети просто обязан изучать азы своей информационной безопасности. Не только изучать, но и использовать. И вовсе не потому, что его личные данные могут стать «вооружением» или даже «оружием» в чужой игре для создания фейковых аккаунтов, а в большей степени потому, как уже реальные пользователи сами, не понимая того, выносят на социальные вершины солдат политических лагерей ***(На Фейсбуке зарегистрировали резкий наплыв украинских пользователей // Lenta-UA (http://lenta-ua.net/novosti/obschestvo/65015-na-feysbuke-zaregistrirovali-rezkiy-naplyv-ukrainskih-polzovateley.html). – 2014. – 7.07).***

***

«Черный» SMM: кто подставил Олега Ляшко?

Интернет и социальные сети превратились в мощное оружие политической борьбы. Один пост может привлечь к политику преданную армию фанатиков, или же, наоборот, сильно подпортить репутацию. Недавний случай по управлению репутацией в социальных сетях касается одного из самых эпатажных украинских политиков – О. Ляшко. Еще три года назад в сеть попало несколько компрометирующих его видеороликов. Недавно неизвестные пиарщики решили напомнить о них довольно необычным способом, пишет AIN.UA (http://ain.ua/2014/07/11/532317).

Началось все в начале июля, когда на адреса десятка украинских PR-, SMM- и онлайн-маркетинговых агентств поступило письмо, подписанное Н. Лысенко. В нем содержалось предложение поработать подрядчиком для

восстановления деловой репутации О. Ляшко. В частности, агентству предлагалось отмониторить и вычистить из YouTube порочащие политика ролики. Текст письма «засветился» в Интернете – его, к примеру, опубликовал известный интернет-маркетолог М. Кукуруза.

Первой реакцией маркетологов и пиарщиков стало удивление таким методам работы с социальными сетями. Учитывая, что с начала июля прошли уже недели, а публикаций так и не появилось, очевидно, ни одно агентство не прельстила такая работа. 9 июля оказалось, что новость о том, как пиарщики О. Ляшко хотят чистить YouTube от компрометирующих роликов, таки заинтересовала несколько сайтов.

Больше всего это похоже не на корявую работу пиарщиков с Интернетом, а на обычный «вброс», считает известный украинский PR-специалист В. Дегтярев, возглавляющий агентство Newsfront. По мнению В. Дегтярева, в нем есть все признаки фейка: несуществующий отправитель, странные формулировки задач, ссылка на компрометирующее видео политика. «Очевидно, что целью письма было привлечь внимание и раздуть скандал, если/когда эта информация вышла бы наружу», – считает он. Исполнитель ждал реакции в виде новостей «Ляшко пытается зачистить интернет», но, когда этого не вышло, начал работать с тем, что было.

Какая именно политическая сила решила так сыграть – неизвестно. Публикации появились лишь на двух не очень известных двух сайтах. Кроме того, новость с оскорбительным комментарием разместил у себя в Facebook глава кировоградской организации партии «Свобода» И. Степура ***(Карпенко О. «Черный» SMM: кто подставил Олега Ляшко? // AIN.UA (http://ain.ua/2014/07/11/532317). – 2014. – 11.07).***

Зарубіжні спецслужби і технології «соціального контролю»

Президент России В. Путин подписал закон, которым вводятся тюремные сроки за финансирование экстремистской деятельности, а также за призывы к экстремизму в Интернете.

Документ под названием «О внесении изменений в отдельные законодательные акты Российской Федерации», принятый Государственной думой 20 июня и одобренный Советом Федерации 25 июня, пишет NEWSru.com.

Введение закона ужесточает меры по контролю за контентом в Интернете. Отныне распространение в сети экстремистской информации – уголовно-наказуемая деятельность.

При этом, судя по последним событиям, достаточно поставить лайк или сделать репост какой-либо провокационной записи (в январе текущего года за подобный проступок сотрудники ФСБ задержали доцента философского факультета МГУ В. Дмитриева, отпустив позднее под подписку о невыезде).

Наказание за публичные призывы к экстремизму в Интернете – принудительные работы или лишение свободы до пяти лет.

Аналогичным образом дополняется и известная статья 282 («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») – под нее теперь также будут попадать соответствующие преступления, совершенные в информационном пространстве, например в сети ***(Путин одобрил введение уголовной ответственности за «экстремистские» лайки и репосты // InternetUA (http://internetua.com/putin-odobril-vvedenie-ugolovnoi-otvetstvennosti-za--ekstremistskie--laiki-i-reposti). – 2014. – 1.07).***

***

Агентство национальной безопасности (АНБ) США назвало сайт журнала Linux Journal «форумом экстремистов», в связи с чем за его участниками и читателями ведётся пристальное наблюдение. Об этом издание узнало из публикаций немецких СМИ.

Известно, что для слежения за деятельностью пользователей Интернета (чтения переписки по почте, просмотр историй посещений веб-страниц в браузере и т. п.) АНБ использует программу XKeyScore. Для выявления потенциальных угроз безопасности ведётся поиск по ключевым словам. Из обнародованного исходного кода XKeyScore стало известно о том, что в фильтре на перехватываемый АНБ трафик оказалось правило, где соседствовали ключевые слова Tails (ОС для анонимного интернет-сёрфинга), Tor (анонимная сеть) и почему-то linuxjournal.com/content/linux*.

Если кто-то из пользователей просто просматривает Linux Journal или упоминает в обсуждениях Tor или Tails, он автоматически может попасть под слежку властей.

По всей видимости, АНБ решило контролировать пользователей Tails и Tor на сторонних сайтах из-за того, что окончательно скомпрометировать сеть Tor, которую используют правозащитники и диссиденты по всему миру, не получается ***(АНБ следит за любителями Linux и Tor // InternetUA (http://internetua.com/anb-sledit-za-luabitelyami-Linux-i-Tor). – 2014. – 5.07).***

***

Начиная с 1 сентября 2016 г. россияне не смогут получать доступ к таким сайтам, как Twitter, Facebook и Booking.com. Дело в том, что 4 июля Госдума РФ приняла во втором и третьем (окончательном) чтениях законопроект, обязывающий интернет-компании хранить персональные данные россиян только в России.

За принятие документа с текстом закона, разработанного первым замглавы информационного комитета ГД В. Деньгиным (ЛДПР), членом комитета А. Ющенко (КПРФ) и замглавы комитета по безопасности А. Луговым (ЛДПР), проголосовало 325 депутатов. Против инициативы выступило 65 человек.

По утверждениям А. Ющенко, на сегодняшний день, если учетная запись, например, в Twitter, существует более трех месяцев, то данные о пользователе перенаправляются на сервер, расположенный в другом государстве, в том числе в США. «Поверьте мне, большинство россиян хотят, чтобы их данные оставались на территории Российской Федерации», – подчеркнул В. Деньгин.

Последний также отметил, что серверы зарубежных стран получают информацию о гражданах России. Помимо прочего, в распоряжении заграничных ведомств якобы находится переписка пользователей, фотографии и пр.

Депутаты, работавшие над созданием законопроекта, уверены, что до 1 сентября 2016 г. крупные заграничные интернет-компании успеют открыть представительства в России и перенести на территорию государства свои серверы ***(Россияне не смогут пользоваться Twitter и Facebook // IT Expert (http://itexpert.org.ua/rubrikator/item/36797-rossiyane-ne-smogut-polzovatsya-twitter-i-facebook.html). – 2014. – 6.07).***

***

Жителю Дніпропетровська 1981 р. народження загрожує п’ять років в’язниці за заклики створити «Українську автономну республіку» у складі Російської Федерації. Про це повідомляє прес-служба прокуратури Дніпропетровської області, пише Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3388029-zhytel-dnipropetrovska-zaareshtovanyi-za-separatyzm-vkontakte).

Зокрема, чоловікові повідомлено про підозру у скоєнні кримінального правопорушення, передбаченого ч.1 ст. 110 Кримінального кодексу України – посягання на територіальну цілісність і недоторканність України.

Як зазначають у прокуратурі, з метою здійснення сепаратистських закликів вказаний громадянин зареєструвався в соціальній мережі «ВКонтанкте», вибрав собі «нік» і вступив до тематичної групи користувачів, які обмінювалися між собою інформацією зі зміни конституційного ладу і кордонів території України.

Вказаного громадянина співробітники слідчого управління прокуратури області взяли на «гарячому» в одному з ресторанів м. Дніпропетровськ, коли той, використовуючи мобільний телефон, здійснив підключення до соціальної мережі і розмістив повідомлення, у якому містилися заклики до населення України щодо зміни меж території держави як порушення порядку, встановленого Конституцією України, шляхом проведення незаконного референдуму, вчинення інших дій радикального характеру з метою створення суверенного державного утворення – «Українська автономна республіка» у складі Російської Федерації, ідеться в повідомленні.

Обвинувальний акт у кримінальному провадженні направлений до суду. Санкцією зазначеної статті йому загрожує покарання у вигляді

позбавлення волі на строк від трьох до п’яти років ***(Житель Дніпропетровська заарештований за сепаратизм ВКонтакте // Корреспондент.net (http://ua.korrespondent.net/ukraine/politics/3388029-zhytel-dnipropetrovska-zaareshtovanyi-za-separatyzm-vkontakte). – 2014. – 4.07).***

***

Агентство національної безпеки (АНБ) США здійснювало незаконний контроль над листуванням в Інтернеті пересічних американців та іноземних громадян, повідомила за підсумками власного розслідування газета The Washington Post. Мало того, що більшість об’єктів спостереження не були цікаві спецслужбам, часто перехоплення стосувалися листування інтимного характеру.

WP проводила розслідування протягом чотирьох місяців. Журналісти опиралися на матеріали, надані колишнім співробітником американських спецслужб Е. Сноуденом, який викрив програму електронного стеження.

«Дев’ять з десяти власників інтернет-акаунтів, дані про які містяться в базі масштабної перехопленої інформації, не були бажаними об’єктами для стеження. Співробітники розвідки “взяли їх на приціл” заради того, щоб стежити за кимось ще», – наголошується в матеріалі. За свідченням видання, «багато з цих людей є американцями».

Між тим, як неодноразово запевняли громадськість представники адміністрації, стеження ніколи не велося за громадянами США або людьми, які перебували в той момент на території країни.

При цьому WP підкреслює, що відстеження листування дало змогу спецслужбам розкрити ряд випадків витоку секретної інформації та визначити підозрюваних у скоєнні і підготовці терактів. Проте, пише видання, часто перехоплення стосувалося виключно приватного листування і інтимного характеру: «Історії любові і розбитих сердець, сексуальних зв’язків, крах надій, політичне та релігійне листування».

«Приблизно половина з усіх виявлених файлів, а це дуже високий показник, містили імена, електронні адреси та інші деталі, які АНБ позначало як ті, що належать громадянам або жителям США», – зазначається в тексті. Там зазначається, що аналітики АНБ приховали, або «мінімізували» 65 тис. подібних згадок. Журналісти виявили ще близько 900 електронних адрес і незасекречених файлів, які так чи інакше пов’язані з американцями або людьми, які проживають в США.

Автори матеріалу пообіцяли не розкривати деталей «найбільш цінних відомостей, щоб уникнути шкоди триваючим (розвідувальним) операціям». Однак, за їхніми словами, там містяться відомості «про секретний ядерний проект в одній із зарубіжних країн, нечесну поведінку одного з союзників США, загибелі військових в одній з недружніх (США) держав, а також відомості про хакерів, які атакували американські комп’ютерні системи».

За даними видання, «триваюче протягом місяців стеження за більш ніж 50 акаунтами безпосередньо призвело до затримки в 2011 р. у пакистанському місті Абботабад Мохаммада Тахира Шахзада, який створював бомби, а також Умара Патека, який підозрювався в причетності до теракту в Індонезії в 2002 р.».

Були й інші приклади, що газета не стала публікувати на прохання ЦРУ ***(АНБ стежило за листуванням пересічних американців, включаючи інтимне // Дзеркало тижня (http://dt.ua/WORLD/anb-stezhilo-za-listuvannyam-peresichnih-amerikanciv-vklyuchayuchi-intimne-146386_.html). – 2014. – 6.07).***

***

Спецслужбы Российской Федерации контролируют украинский сегмент социальной сети Facebook. Об этом сообщил советник министра обороны Украины А. Данилюк на своей странице в соцсети.

«ВНИМАНИЕ!!! ПЕРЕПОСТ!!! Я уже писал несколько раз о вмешательстве русских спецслужб в нормальное функционирование украинского сегмента Facebook. Как это работает: при внешне сохранении нормального интерфейса пользователя, количества друзей и подписчиков, реальный круг вашего общения ограничивается количеством пользователей, определенным динамическим алгоритмом. Это легко заметить по существенном уменьшении активного реагирования друзей и подписчиков на ваши посты: уменьшению лайков и комментариев.

При этом сеть перестает быть единой. Зато она разбита на закрытые кластеры, из которых информация не может быть переданной дальше. В прошлый четверг, после моих многочисленных жалоб служба технической поддержки Facebook возобновила нормальное функционирование, однако несколько дней тому назад проблема повторилась.

Фактически, речь идет о диверсии против одного из основных средств коммуникаций, которое не зависит от позиции контролируемых СМИ», – написал он.

Напомним, ударовец С. Каплин заявил, что телефонные разговоры украинских солдат прослушиваются российскими спецслужбами.

А Д. Тымчук уверен, что украинской армии необходима люстрация и адекватная работа контрразведки, поскольку в настоящее время Генштаб наводнен российской агентурой ***(Российские спецслужбы контролируют украинский Facebook, – советник министра обороны Украины // ТРАСТ.УА (http://www.trust.ua/news/97546-rossijskie-specsluzhby-kontroliruyut-ukrainskij-Facebook---sovetnik-ministra-oborony-ukrainy.html). – 2014. – 11.07).***

***

Издание Sydney Morning Herald сообщило, что австралийские федеральные и государственные правоохранительные органы приказывают

телефонным провайдерам собирать личную информацию о тысячах владельцев мобильных телефонов, независимо от того, находятся ли эти люди под следствием.

По информации австралийского издания, данный факт подтверждает использование агентствами техники под названием tower dump. Она позволяет полиции получить данные о личности, ее действиях и местоположении с любого телефона, подключенного к целевым телефонным башням. Информация, как правило, поступает в течение 1–2 часов.

Под действие tower dump попадают некоторые телефонные вышки и мобильные провайдеры. Помимо этого, технология позволяет получать данные с миллионов сотовых телефонов. Tower dump обычно используется в тех случаях, когда полиции необходим мощный инструмент для отслеживания преступников. Тем не менее, правозащитники утверждают, что в то время как такая технология может быть полезна для полиции, она также направлена против тысяч невинных людей и не подлежит правовому контролю. В дополнение к этому, правозащитники также задаются вопросом, куда деваются собранные данные.

Австралийские телефонные провайдеры не предоставили комментариев по данному вопросу ***(Полиция Австралии использует телефонные вышки для сбора даннях // InternetUA (http://internetua.com/policiya-avstralii-ispolzuet-telefonnie-vishki-dlya-sbora-dannih). – 2014. – 10.07).***

Проблема захисту даних. DDOS та вірусні атаки

Глава отдела Security Research Group компании IBM Р. Хэй объявил об обнаружении уязвимости в сервисе Android KeyStore, которая затрагивает 86 % мобильных устройств на базе операционной системы от Google. Брешь в системе позволяет хакерам заполучить доступ к информации о банковских картах, узнать пароли и даже PIN-код блокировки экрана смартфонов и планшетов.

Эксперты выявили баг еще в сентябре прошлого года, о чем сообщили команде по безопасности Android Security Team, однако, публично раскрыли ее только в настоящее время. «Учитывая фрагментарный характер Android, а также тот факт, что уязвимость позволяла выполнение кода, мы решили подождать с раскрытием», – сообщил Р. Хэй.

Уязвимости подвержена область, отвечающая за хранение криптографических ключей Android KeyStore. Под угрозой взлома находятся аппараты под управлением Android 4.3 и ниже. Как заявляют специалисты, это около 86 % гаджетов. Пользователи могли бы обезопасить себя от вредоносных приложений, если бы использовали устройства на последней версии Android.

Д. Уолаxx, программист, специализирующийся на безопасности Android в Университете Райса (США, Хьстон), настоятельно рекомендует пользователям «гуглофонов» активировать файервол:

«Если под угрозой взлома стоит KeyStore, то мошеннику открывается доступ к любой службе от имени администратора. Конечно, украсть доступ, к примеру, от вашего Twitter-аккаунта, будет куда проще. На всех Android-устройствах ниже 4.4 мы рекомендуем активировать файервол».

Ранее уязвимости встречались в Android неоднократно, причем баг KeyStore – не самый распространенный. Осенью прошлого года эксперты обнаружили уязвимость, затрагивающую около 99 % устройств, находящихся в эксплуатации ***(Обнаружена опасная уязвимость, затрагивающая 86 % Android-устройств // InternetUA (http://internetua.com/obnarujena-opasnaya-uyazvimost--zatragivauasxaya-86--Android-ustroistv). – 2014. – 1.07).***

***

В воскресенье, 29 июня 2014 г., 17-летним хакером была совершена кибератака на операционную систему Tails.

Tails является операционной системой на базе ядра Linux с высоким уровнем безопасности. Она была специально разработана и оптимизирована для обеспечения анонимности и конфиденциальности пользователей. Хакеру, который назвал себя Sum guy, удалось получить доступ к веб-сайту Tails с правами администратора и отредактировать содержание главной страницы, разместив на ней следующее сообщение:

«Вы были взломаны 17-летним хакером по воле случая. Пожалуйста, простите меня! Случайно я вошел в учетную запись как кто-то важный и изменил сайт, не понимая, что мои изменения сохранятся. Простите… Надеюсь, у вас есть запасной план. Между прочим, я обожаю вашу операционную систему! Искренне ваш, Sum guy».

Тем не менее, остальные страницы сайта Tails продолжают работать, хотя пока не ясно, изменил ли хакер образ ОС. Так, пользователям рекомендуется не скачивать ОС Tails с сайта по крайней мере в течение нескольких дней ***(Операционная система Tails была взломана неизвестным хакером // InternetUA (http://internetua.com/operacionnaya-sistema-Tails-bila-vzlomana-neizvestnim-hakerom). – 2014. – 30.06).***

***

Какими уловками пользуются хакеры для кражи личных данных

Мы часто слышим заявления, что онлайн-счет частного лица или даже крупной компании был взломан. Но как это происходит на самом деле? Важно иметь общее представление о том, как действуют злоумышленники в сети. Это поможет значительно повысить уровень вашей личной безопасности. Тем более счета, как правило, взламываются достаточно простыми способами, доступными для понимания обычного пользователя.

Мы рассмотрим самые часто используемые хакерами методы, которые помогают им взламывать личные аккаунты.

1. Метод социальной инженерии.

Суть данного эффективного вмешательства в вашу частную жизнь заключается в особенности психологии пользователя в Интернете. Злоумышленники прибегают к нему для того, чтобы вы сами сообщили им свои конфиденциальные сведения. Проявляться это может в разных формах и существует с момента массового распространения интернета. Вы можете получить электронное письмо, ссылка внутри которого приведет вас на поддельную страницу вашего интернет-банкинга, где вам будет предложено заполнить поле пароля. Или же вы получите письмо в социальной сети от человека, представляющегося администратором и просящего данные вашей учетной записи. Угрозой может стать и сайт, предлагающий получить некий приз. Для этого будет предложено опять же сообщить личную информацию. Данный способ воздействия нашел тысячи воплощений в Интернете. Как правило, они достаточно тривиальны, и пользователи редко попадаются на подобные дешевые трюки. Тем не менее, до тех пор, пока социальная инженерия существует, будут появляться и жертвы. Поэтому совет в данном случае очень прост: быть внимательным к тем предложениям, которые звучат слишком заманчиво для того, чтобы быть правдой, и не переходить по ссылкам из электронных писем.

2. Использование «кейлоггеров».

Другой вариант сбора вашей личной информации известен как «клавиатурный шпион» или «кейлоггер». Он представляет собой попадание на ваше устройство вредоносного ПО, работающего в фоновом режиме, регистрирующего каждое нажатие клавиши, а после отправляющего набранные вами символы нарушителю вашего частного пространства. Зачастую «шпион» используется для получения пароля от интернет-банкинга и доступа к не менее важным учетным данным. Стать несчастливым обладателем кейлоггера можно, используя устаревшую версию Java или скачав программу с неизвестного ресурса. Чтобы обезопасить себя, следует использовать достойную антивирусную программу (Malwarebytes, ESET Online Scanner и т. д.), поддерживать ваше ПО в актуальном состоянии и избегать использования «Java» и потенциально опасных ресурсов.

3. Взлом с помощью подбора пароля.

Самый распространенный способ проникновения недоброжелателей в вашу частную жизнь – использование вашей же непредусмотрительности. Очень часто мы слышим о необходимости применять различные пароли для нескольких сервисов, сайтов и так далее. Многие пренебрегают данным советом, полагая, что используют достаточно сложный набор символом в качестве основного пароля. Но опасность кроется не только лишь в легкости подбора букв в сочетании с годом вашего рождения. Настоящая угроза заключается в незащищенности баз данных тех самых сервисов, которым вы доверяете свою личную информацию. Даже крупные сайты (например,

LinkedIn) встречали на своем пути проблему утечки пользовательских сведений. Вследствие этого пароли и электронные адреса оказываются в общем доступе. И несложно догадаться, что, заполучив ваши сведения, злоумышленники смогут попробовать использовать их и на других популярных сервисах. По большому счету, недоброжелателю достаточно добиться доступа к вашей электронной почте для того, чтобы разом завладеть всеми вашими аккаунтами. Есть и иной способ нарушения целостности чужой безопасности. Он осуществляется при помощи секретных вопросов, которые различные сервисы используют в качестве очередного рубежа повышения надежности пароля. Как правило, эти вопросы достаточно просты: девичья фамилия матери, название школы и т. д. Но, что гораздо опаснее, на них легко получить ответ, изучив профиль человека в социальных сетях или во время специально спланированного диалога в сети. Поэтому следует избегать использования распространенных секретных вопросов.

Многие люди уверены, что подбор случайных паролей относится к категории взлома ваших личных данных. На самом деле, это неправда. Кроме того, такой способ не используется вовсе. Большинство сервисов защищены от данного вмешательства. Когда кто-то пытается угадать пароль к учетной записи в Интернете, как правило, после определенной попытки возникает временная блокировка доступа, лишающая злоумышленника возможности продолжать подбор дальше. Подобные грубые методы могут сработать только лишь по вине самого пользователя, который выбрал в качестве пароля настолько очевидный набор символов, что его без дополнительных инструментов смог угадать посторонний человек.

Для того, чтобы повысить уровень вашей сетевой безопасности, вы можете прибегнуть к использованию двухступенчатой аутентификации. Ее суть заключается в том, что вы становитесь обладателем сразу двух рубежей защиты. Даже, если злоумышленник получит доступ к вашему основному паролю, он встретит новое препятствие в виде формы, запрашивающей еще и одноразовый пароль. Такой способ в ходу у различных финансовых структур, но вы можете обратиться к нему и для защиты иных видов информации. Например, существует приложение Google Authenticator, использующее двухступенчатую аутентификацию для доступа к аккаунтам Google, LastPass, Dropbox. С помощью вышеназванной программы от Google и одноименного плагина для WordPress можно обезопасить и доступ к собственному веб-сайту. Microsoft предлагает двойную защиту для сервисов, связанных с игровой консолью Xbox, облачным хранилищем SkyDrive и почтовыми службами. Blizzard предлагает аналогичный способ повышения безопасности игровых учетных данных с помощью специального приложения Battle.net Authenticator app.

Проанализировав список основных способов взлома личных учетных данных и методов защиты, можно сделать вывод, что все эти способы прямолинейны, а охранные системы находятся в открытом доступе и не

представляют собой сложное ПО для профессионалов, а, наоборот, являются ориентированными на обычного пользователя, который зачастую сам виноват в утечке сведений. Поэтому в разрезе разговора о безопасности личных данных можно выделить два основных совета: оставаться внимательным в любой ситуации и пользоваться всеми доступными средствами для того, чтобы защитить свои пароли от краж ***(Какими уловками пользуются хакеры для кражи личных даннях // InternetUA (http://internetua.com/kakimi-ulovkami-polzuuatsya-hakeri-dlya-kraji-licsnih-dannih). – 2014. – 30.06).***

***

«Приватбанк» опровергает заявление хакерской группировки Green Dragon о взломе системы «ПриватБанка» и краже данных карт пользователей, передает корреспондент «proIT».

В банке подчеркивают, что имела место обычная DDoS-атака, из-за чего 30 июня сайт банка и интернет-сервис «Приват24» были временно недоступны.

Банк также заявляет, что сервисы и онлайн-банкинг не были взломаны и работают в штатном режиме.

«Информация о том, что «хакерами» украдены коды доступа клиентов к онлайн-банкингу, база кредитных и дебетовых карт – это просто вранье. На сайт банка 30 июня прошла DDoS-атака – уже не первая за последнее время», – сообщают в «ПриватБанке» ***(«ПриватБанк» опровергает хищение данных: зафиксирована лишь DDoS-атака // proIT (http://proit.com.ua/news/internet/2014/07/01/095448.html). – 2014. – 1.07).***

***

Управление полиции Греции по борьбе с киберпреступностью предупредило граждан, использующих интернет-банкинг, о появлении новых вредоносных компьютерных программ, направленных на несанкционированный доступ к их банковским счетам (Banking Malware).

«Новая вредоносная программа названа EMOTET, и она быстро распространяется через письма по электронной почте. Программа может собирать данные интернет-банкинга (логин и пароль пользователя), информацию о передаче данных (сетевом трафике), красть конфиденциальные данные», – говорится в сообщении департамента по борьбе с электронной преступностью.

По данным полиции, вирус распространяется по электронной почте через письма, в которых говорится о переводе некоторых сумм на банковский счет пользователя и которые содержат ссылку для получения дополнительной информации по вопросу банковского перевода. Когда пользователь переходит по ссылке в электронной почте, начинается процесс установки вредоносных программ, сообщает полиция.

«Вредоносная программа способна обходить протоколы безопасности передачи данных HTPPS, и это создает большой риск перехвата данных для входа e-banking в то время, как пользователи считают, что их банковские онлайн-операции проходят безопасно», – говорится в сообщении.

Полиция предлагает гражданам, получившим электронные письма с аналогичным содержанием, не переходить по ссылке и не открывать файлы, содержащиеся в письмах. «В каждом случае пользователю рекомендуется подтвердить в банковском учреждении достоверность электронной почты прежде, чем они предпримут дальнейшие действия», – говорится в сообщении.

Если пользователь «кликнул» ссылку в подобном письме, рекомендуется переустановить операционную систему, сообщает полиция Греции ***(Новый ход киберпреступников // InternetUA (http://internetua.com/novii-hod-kiberprestupnikov). – 2014. – 1.07).***

***

Троян для получения удаленного доступа RAT использует Dropbox для управления целевой атакой на тайваньское правительство, считает аналитик по безопасности М. Менридж.

По словам М. Менриджа, модернизированная версия трояна PlugX RAT является первым вредоносным ПО с использованием Dropbox для контроля управлением и параметрами в отличие от других вредоносных программ и троянов-вымогателей, которые используют популярный сервис облачного хранилища с целью заражения компьютеров жертв вредоносными файлами.

PlugX II обманул антивирусные системы Dropbox и замаскировался под поддельный домен. Злоумышленники, управляя командованием, могли мигрировать по корпоративным сетям, используя различные инструменты, чтобы избежать обнаружения.

Код включает в себя такие инструменты, как для восстановления пароля, сетевые утилиты, сканеры портов и утилита HTran, способствующая проведению кибератак путем перенаправления TCP трафика на альтернативные хосты.

Троян регистрирует нажатия клавиш пользователя, отмечает порты и открывает дистанционные оболочки для облегчения дальнейшей кражи данных и их эксплуатации. Аналитик добавил, что кража данных производится таким образом, чтобы жертва еще долгое время не подозревала о совершении преступниками злонамеренных действий ***(Троян RAT использует Dropbox для совершения кибератаки на тайваньское правительство // InternetUA (http://internetua.com/troyan-RAT-ispolzuet-Dropbox-dlya-soversheniya-kiberataki-na-taivanskoe-pravitelstvo). – 2014. – 1.07).***

***

Эксперты компании «Доктор Веб» зафиксировали в сети новую вредоносную кампанию, организованную для распространения троянского вируса Smoke Loader. Согласно данным ИБ-экспертов, для распространения вредоносного ПО злоумышленники организовывают обычную рассылку электронных писем. Правда, в этом случае они отправляют сообщения от имени интернет-компании Amazon.

В письмах сообщается о поступившем заказе, информацию о котором можно прочесть в прикрепленном файле. Однако вместо обещанной детализации покупки и счета-фактуры корреспонденция содержит архив со Smoke Loader.

По данным компании, злоумышленники рассылают письма с одинаковым текстом на английском языке. В письме изменяются только дата и номер заказа.

«Назначение данного троянца заключается в загрузке на инфицированный компьютер других вредоносных приложений, благодаря чему незащищенная антивирусной программой система может превратиться в настоящий заповедник для различных угроз», – пишут специалисты в блоге «Доктор Веб».

После первого запуска троян проверяет систему на наличие «песочницы» или виртуальной машины. Затем Smoke Loader создает свою копию в одной из папок на диске компьютера, регистрируется в отвечающей за автозагрузку ветви реестра Windows и встраивается в ряд системных процессов. Кроме того, при наличии доступа к сети вирус загружает другие вредоносные программы и запускает их ***(Вирус Smoke Loader распространяется при помощи поддельных писем от Amazon // InternetUA (http://internetua.com/virus-Smoke-Loader-rasprostranyaetsya-pri-pomosxi-poddelnih-pisem-ot-Amazon). – 2014. – 1.07).***

***

Facebook заблокував акаунт С. Цеголка, який нещодавно очолив прес-службу Президента України, пише Zaxid.net (http://zaxid.net/news/showNews.do?pressekretar_poroshenka_zalishivsya_bez_akaunta_u_facebook&objectId=1313614).

При переході на його профіль користувачам повідомляють, що такого акаунта не існує.

До видалення, С. Цеголко входив до ТОП-20 найпопулярніших українських користувачів Facebook, зазначає Watcher.

С. Цеголко також є популярним у Twitter, його акаут twitter.com/STsegolko читає близько 25 тис. користувачів.

В Україні досі немає представництва Facebook, і більшість організаційних питань вирішується через московський офіс соціальної мережі. Процедура блокування відбувається, як правило, унаслідок організованих дій великої групи користувачів, які скаржаться на акаунт.

Імовірно, С. Цеголко постраждав від дій однієї з груп ботів, які працюють на російський уряд ***(Прес-секретар Порошенка залишився без акаунта у Facebook // ZAXID.NET (http://zaxid.net/news/showNews.do?pressekretar_poroshenka_zalishivsya_bez_akaunta_u_facebook&objectId=1313614). – 2014. – 2.07).***

***

Международная корпорация Symantec, занимающаяся вопросами кибербезопасности, заявила о существовании группы хакеров, располагающей ресурсами, размером и организацией, которые предполагают поддержку со стороны правительства.

Атаки злоумышленников направлены на операторов электросетей, генерирующие компании и другие стратегические значимые компании энергетического сектора. Более половины случаев внедрения вредоносного программного обеспечения данной группой приходится на США и Испанию. Следы атак обнаружены также в Сербии, Греции, Румынии, Польше, Турции, Германии, Италии и Франции.

В настоящее время не представляется возможным определить, прямо ли правительство причастно к деятельности преступной группы или же группа предлагает властям свои услуги.

Хакеры работают с 9 часов утра до 6 часов вечера с понедельника по пятницу во временном поясе GMT+4, который соответствует Москве или некоторым восточноевропейским странам, говорится в докладе корпорации.

Программное обеспечение, внедренное злоумышленниками в ряде случаев, позволяет получать доступ к промышленным системам управления компаний, в результате чего под угрозой может оказаться энергоснабжение в указанных странах, предупреждает Symantec, которая пристально отслеживает активность данной группы хакеров с 2012 г. ***(Symantec: хакеры из Восточной Европы атакуют западные энергокомпании // InternetUA (http://internetua.com/Symantec--hakeri-iz-vostocsnoi-evropi-atakuuat-zapadnie-energokompanii). – 2014. – 2.07).***

***

Блоггер П. Кашаяп обнаружил в сети эксплоит, с помощью которого можно взломать учетную запись в Facebook за 20 секунд.

Информацию об эксплоите блоггер получил в письме электронной почты. В сообщении утверждалось: «Мы обнаружили уязвимость, которая позволяет неавторизованным пользователям удалить или проникнуть в профили на Facebook. Для этого был создан эксплоит ... Вся процедура длится не более 20 секунд ... Для установки требуется загрузить Selenium / WebDriver и войти в вашу учетную запись, используя Firefox или Chrome...» Письмо заканчвалось фразой «Используйте эксплоит на свой страх и риск».

Эксплоит обойдется в 5 биткоинов. ID электронной почты и адрес передачи биткоинов был также прислан по почте.

П. Кашаяп не пытался воспользоваться присланным ему в сообщении эксплоитом. Вполне вероятно, что хакеры таким образом рассылают пользователям вредоносное ПО. Их целью может быть компрометация целевой системы, хищение конфиденциальной информации и пр. ***(Хакеры предлагают эксплоит для взлома учетной записи в Facebook // InternetUA (http://internetua.com/hakeri-predlagauat-eksploit-dlya-vzloma-ucsetnoi-zapisi-v-Facebook). – 2014. – 2.07).***

***

Отдел цифровых преступлений Microsoft (Digital Crimes Unit) раскрыл данные сразу о двух семействах вредоносного ПО – Jenxcus и Bladabindi. По данным специалистов компании, авторами вирусов являются Н. Мутаири, также известный как njQ8, и М. Бенабделла – он же Houdini.

Как следует из записи, опубликованной в блоге Microsoft, данные о семьях вредоносов были раскрыты с целью предотвратить дальнейшее их распространение авторами.

Активность вирусов семейства Bladabindi была зафиксирована еще в июле 2012 г., а Jenxcus появился ближе к декабрю того же года. В течение прошедшего года злоумышленникам удалось при помощи этих программ инфицировать почти 7,5 млн компьютеров под управлением ОС Windows.

Вирусы обоих видов способны устанавливать на системы бэкдоры, благодаря чему злоумышленники могут перехватывать содержащиеся на ПК данные и выполнять ряд других действий. В частности, Bladabindi регулярно делает снимки и записывает видео без ведома или разрешения пользователя. Этот вирус также предоставляет хакерам возможность удаленно управлять системой жертвы.

В большинстве случаев вредоносное ПО загружает дополнительные компоненты и вредоносные программы. Кроме того, они соединяются с хостами (в большинстве случаев это сервис динамического DNS), такими как NO-IP, поскольку это усложняет процесс отслеживания источник угрозы.

По данным экспертов техногиганта, вирусы распространяются при помощи техник социальной инженерии. К примеру, Bladabindi может установиться на систему жертвы при посещении взломанного сайта, переходе по вредоносной ссылке из сообщения в соцсети и пр. Jenxcus, в свою очередь, заражает компьютеры при помощи торрентов и сайтов, на которых видео и другие программы содержат вирус. Кроме того, зафиксировано несколько случаев, когда вредонос устанавливался под видом обновления Flash ***(Microsoft раскрыла данные о двух семействах вредоносного ПО // InternetUA (http://internetua.com/Microsoft-raskrila-dannie-o-dvuh-semeistvah-vredonosnogo-po). – 2014. – 2.07).***

***

Специалист по информационной безопасности Б. Калин обнаружил, что длинные cookie-записи могут быть использованы для совершения DDoS-

атак на блоговые платформы. Атака произойдет в том случае, если сервер будет получать cookie-записи с установленным большим значением, что спровоцирует ошибки в его работе.

Б. Каллин подтвердил свою гипотезу на примере блоговой платформы Google Blog Spot. В последующих экспериментах он обнаружил, что если веб-браузер устанавливает одновременно большое количество cookie-записей, без установленного срока действия, и устанавливая указатель на корневой домен блога, то пользователю не будут отображаться блоги.

Таким образом, если cookie-записи переполняют память браузера, то появляется уведомление об ошибке 400 – «Ваш браузер послал запрос, который сервер не может обработать. Размер поля заголовка запроса превышает лимит сервера».

DDoS-атака осуществляется в результате установки длинных cookie-записей, заставляя браузер формировать очень длинный запрос. Такие запросы являются тяжелыми для обработки сервером, поэтому пользователь получает уведомление об ошибке ***(Длинные cookie-записи могут спровоцировать DDoS-атаку // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/07/03/too-long-cookies.html). – 2014. – 3.07).***

***

Компания Trend Micro предупреждает: в тройку наиболее популярных вредоносных программ, атакующих бизнес, входит червь, который использует уязвимости устаревшей операционной системы Windows XP. Червь DOWNAD, известный также как Conficker, может инфицировать сети через вредоносные URL, спам, съемные устройства хранения. Для Windows XP он представляет наибольшую угрозу, поскольку для исполнения вредоносного кода использует уязвимость MS08-067 в службе Server.

В DOWNAD предусмотрен собственный алгоритм генерации доменных имен (domain generation algorithm, DGA) который позволяет случайным образом создавать URL и связывать их с загружаемыми файлами. По данным Trend Micro, с DOWNAD связано 175 IP-адресов, использующих разные порты. Во II квартале 2014 г. более 40 % спама, связанного с вредоносами, доставлялось компьютерами, инфицированными DOWNAD, в частности, они использовались для проведения спам-кампаний FAREIT, MYTOB, LOVGATE.

В число крупнейших источников спама также входит ботнет CUTWAIL, который ранее использовался для загрузки вредоноса Gameover ZeuS (GoZ), а теперь – UPATRE или вариантов ZBOT с P2P-функциональностью ***(В числе тройки популярных вредоносов, атакующих бизнес, – червь для Windows XP // InternetUA (http://internetua.com/v-csisle-troiki-populyarnih-vredonosov--atakuuasxih-biznes----cserv-dlya-Windows-XP). – 2014. – 4.07).***

***

Так называемая Cridex, вредоносная программа, созданная для хищения данных, она же Feodo и Bugat, теперь имеет автоматизированный способ заражения компьютеров жертв, сообщили исследователи из Seculert. Как только новая версия вредоносного ПО, получившая название Geodo, попадает на компьютер пользователя, она загружает вторую часть вируса. Последний получает команды от C&C-сервера и содержит более 50 тыс. украденных учетных записей серверов электронной почты SMTP.

Далее вредоносная программа рассылает электронные письма с настоящих адресов электронной почты другим потенциальным жертвам с целью их дальнейшего распространения. По словам А. Раффа, технического директора Seculert, это позволяет зараженному боту продолжать распространение вируса. Жертвам червя стоит опасаться не только хищения личных данных, но также интеллектуальной собственности, сообщили в компании.

На сегодня большинство жертв – жители Германии, поскольку 46 % всех украденных учетных данных приходятся на немцев.

Ранее Cridex распространялся через съемные носители, однако новые версии вредоносной программы начали загружаться через эксплоиты Blackhole, говорят в Trend Micro. Также существуют версии вредоносных программ, которые используют алгоритм генерации доменных имен (DGA), чтобы скрыть свои URL-адреса от исследователей и сотрудников правоохранительных органов.

А. Рафф говорит, что группа хакеров, скорей всего, не спонсируется властями отдельного государства. Тем не менее, они пытаются похитить как можно больше информации у своих жертв ***(Новая версия червя Cridex похищает данные через почту // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/07/03/geodo-new-cridex-version-combines-data-stealer-and-email-worm.html). – 2014. – 3.07).***

***

Эксперты «Лаборатории Касперского» зафиксировали возвращение вредоносного ПО под названием Miniduke. Специалисты обнаружили бэкдор еще в 2013 г., сообщая об атаке вредоносного ПО на компьютерные системы правительственных органов. Предполагалось, что вредоносное ПО осуществляло атаки с начала 2000-х годов.

Злоумышленники после длительного периода времени снова вернулись в киберпространство. Вирусописатели «старой школы» умеют разрабатывать изощренные вирусы. В настоящее время злоумышленники применили свои знания, чтобы создать обновленную версию забытого вредоносного ПО и осуществить атаку на государственные и научно-исследовательские организации в ряде стран.

Обновленный Miniduke, известный под названием CosmikDuke, может похищать большое количество информации. Бэкдор маскируется под

известные приложения, используя оригинальные иконки официальных программ, их описание, а также оригинальные имена файлов. Для того чтобы лучше замаскировать CosmicDuke под официальное ПО, злоумышленники искусственно увеличили его размер.

Miniduke или CosmicDuke использует для запуска собственный мини-сервис или Планировщик Заданий ОС Windows. Даже если пользователь не работает за компьютером, бэкдор может запуститься при помощи системы активации скринсейвера. Вредоносное ПО может похищать информацию файлов с таким расширением: .exe, .ndb, .mp3, .avi, .rar, .docx, .url, .xlsx, .pptx, .ppsx, .pst, .ost, .psw, .pass, .login, .admin, .sifr, .sifer, .vpn, .jpg, .txt, .lnk, .dll, .obj, .ocx, .js.

CosmicDuke использует алгоритм кодирования аналогичный более ранним версия трояна, однако, формат сообщения с адресом центра управления изменился. Троянец применяет особый обфускатор, а также имеет большой размер файла. Вредоносное ПО запускает два модуля, один из которых полученный с центра управления.

CosmicDuke защищен специальным обфусцированым загрузчиком, который дает большую нагрузку на процессор устройства в течении 3–5 минут, чтобы выполнить основной код. Такая схема работы троянца утяжеляет процесс его обнаружения антивирусным ПО. Наибольшее количество случаев инфицирования троянцем CosmicDuke зафиксировано в Грузии, России, а также США ***(Эксперты «Лаборатории Касперского» обнаружили «старый» Miniduke // InternetUA (http://internetua.com/eksperti--laboratorii-kasperskogo--obnarujili--starii--Miniduke). – 2014. – 6.07).***

***

ИБ-эксперты из MetaIntell обнаружили серьезную уязвимость в последней версии Facebook SDK, которая ставит аутентификационные маркеры пользователей соцсети под угрозу компрометации.

Использование Facebook SDK для Android и iOS является наиболее простым способом интегрировать мобильные приложения с платформой Facebook. Набор программных инструментов для разработчиков позволяет облегчить процесс считывания и написания на Facebook API и пр.

Механизм «Зайти с Facebook» (Login as Facebook) является весьма защищенным способом авторизации пользователей в сторонних приложениях, поскольку сам пароль вводить не нужно. После того как пользователь соглашается на предоставление данных, требуемых программой, Facebook SDK реализует поток OAuth 2.0 User-Agent для изменения данных в Facebook от имени пользователя.

Несмотря на то что токены нельзя никому раскрывать, хранятся они в незашифрованном виде в библиотеке Facebook SDK. Это означает, что доступ к файлу с маркером можно получить даже на невзломанном Android- или iOS-устройстве.

Опасность состоит в том, что абсолютно каждое приложение, имеющее право доступа к файловой системе устройства, можно использовать для удаленного похищения аутентификационных маркеров. Это позволит злоумышленнику осуществить вход в учетную запись жертвы в Facebook ***(В Facebook SDK обнаружена уязвимость // InternetUA (http://internetua.com/v-Facebook-SDK-obnarujena-uyazvimost). – 2014. – 6.07).***

***

Китайская группа хакеров, похищавшая данные аналитических центров США, внезапно поменяла цель своего нападения в прошлом месяце. Теперь злоумышленники сосредоточились на Ближнем Востоке – в Ираке, сообщает компания CrowdStrike.

Группа киберпреступников под названием Deep Panda изменила направление кибератак из-за конфликта группировки «Исламского государства Ирака и Леванта» с Багдадом, а также из-за поражения силовиков Ирака на севере и западе страны, сообщает аналитик CrowdStrike Д. Альперович.

Д. Альперович отметил, что радикальное смещение интересов группировки произошло 18 июня, в день, когда суннитские экстремисты захватили крупнейший нефтеперерабатывающий завод Ирака. Китайская группа хакеров, обычно, была заинтересована американской стороной, сказал аналитик. Однако в прошлом месяце группировка вдруг обратила свое внимание на людей, имеющих связи с Ираком и Ближним Востоком.

Потребность Китая в природных ресурсах резко возросла с подъемом экономики страны, и ей приходится все чаще обращаться к Ближнему Востоку, чтобы удовлетворять свои энергетические потребности, говорят в CrowdStrike. Китай обогнал США и стал крупнейшим в мире импортером нефти и других жидких видов топлива еще в сентябре прошлого года. Соответственно, Китай является крупным инвестором нефти в Ирак.

Эксперты компании говорят, что проникновение в компьютерные системы организации может предоставить доступ к важной секретной информации и позволить злоумышленникам использовать взломанные учетные записи электронной почты, чтобы получить доступ к другим целям.

Участники Deep Panda часто охотятся за личной информацией политиков, некоторые из которых до сих пор представлены в правительствах государств. Впоследствии они составляют фишинговые письма электронной почты и отправляют их этим политикам в надежде, что открытие вложения из письма скомпрометирует систему жертвы и откроет доступ к еще большему количеству конфиденциальной информации ***(Китайские хакеры осуществили взлом аналитических центров Ближнего Востока // InternetUA (http://internetua.com/kitaiskie-hakeri-osusxestvili-vzlom-analiticseskih-centrov-blijnego-vostoka). – 2014. – 8.07).***

***

Компания Facebook обезвредила греческий ботнет, которому удалось взломать 50 тыс. учетных записей, а также инфицировать около 250 тыс. компьютеров. Целью операторов ботнета было хищение криптовалюты, информации об учетных записях электронной почты, банковских данных, а также осуществление спам-рассылки.

Ботнет под названием Lecpetex распространял вредоносное ПО, включая троян DarkComet, который позволяет получить удаленный доступ к информации на компьютере жертв. Помимо этого операторы ботнета использовали вредоносные программы для кражи электронной валюты Litecoin.

Правохранительные органы Греции провели обыск в домах злоумышленников. В результате было установлено, что мошенники похитили большое количество паролей и взломали 114 электронных кошельков. В рамках обыска было изъято четыре ноутбука, USB-накопители, девять жестких дисков, а также два стационарных компьютера.

Принцип действия ботнета Lecpetex выглядел следующим образом:

1. Пользователь получает личное сообщение, как правило с текстом ”lol” и прикрепленным архивом ZIP.

2. Пользователь открывает прикрепленный архив и извлекает архив Java (исполнительный файл).

3. Файл JAR осуществляет загрузку главного модуля Lecpetex с файлообменного сервиса и внедряет его в Windows Explorer.

4. Основной модуль получает инструкции с командных и контрольных сайтов, включая:

– обновление основного модуля;

– загрузку, установку и запуск ПО для кражи Litecoin;

– загрузку и запуск спам модуля для Facebook;

– загрузку и запуск произвольного исполняемого файла (DarkComet RAT).

5. Спам модуль Facebook взламывает учетную запись пользователя посредством хищения cookie-файлов браузеров. Это позволяет получить доступ к списку друзей жертвы. Затем каждому другу из списка отправляется личное сообщение с прикрепленным ZIP архивом, содержащим вредоносное ПО.

Эксперты по информационной безопасности из Menlo Park сообщили, что в период с декабря прошлого года по июнь текущего года 31-летний и 27-летний создатели ботнета осуществили около 20 спам-кампаний. Злоумышленников арестовали на прошлой неделе ***(Facebook обезвредила ботнет, похищающий Litecoin // InternetUA (http://internetua.com/Facebook-obezvredila-botnet--pohisxauasxii-Litecoin). – 2014. – 10.07).***

***

Около 41 % компаний в мире пострадали от распределённых атак типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) в 2013 г. Из них 78 % зафиксировали два подобных хакерских нападения или более, сообщается в исследовании, проведенном британским телекоммуникационным оператором BT Group. Эксперты опросили ИТ-менеджеров компаний в 11 странах мира.

58 % организаций, принявших участие в опросе, выразили свою озабоченность DDoS-атакам, тогда как в Великобритании эта проблема волнует 36 % местных компаний. Половина британских организаций имеет четкий план реагирования во время атак на свои вычислительные системы. Однако лишь каждый десятый респондент сказал о том, что его компания обладает достаточными ресурсами для противодействия информационным нападениям.

В исследовании сообщается, что после DDoS-обрушения количество жалоб и различных вопросов со стороны клиентов пострадавшей компании возрастает более чем на треть. На восстановление работы в среднем организациям нужно около 12 часов. Представляющие Туманный Альбион компании утверждают, что после хакерских атак их системы, как правило, не работают в штатном режиме более 6 часов ***(Почти половина компаний в мире стали жертвами DDoS-атак // InternetUA (http://internetua.com/pocsti-polovina-kompanii-v-mire-stali-jertvami-DDoS-atak). – 2014. – 12.07).***

***

Эксперты компании FireEye обнаружили ботнет под названием BrutPOS. Вредоносное ПО, используемое операторами ботнета, компрометировало компьютерные системы, вследствие чего осуществлялись атаки на POS-терминалы. Специалисты высказали мнение о том, что злоумышленники воспользовались весьма простым механизмом осуществления атаки.

Большинство предприятий используют протокол удаленного рабочего стола (RDP) Microsoft в качестве неотъемлемой части проведения ежедневных бизнес-операций. При помощи RDP пользователь может выполнить удаленный вход в систему Windows. К примеру, администратор при помощи удаленного доступа может обновить программное обеспечение.

Злоумышленники пользуются этой функцией для достижения преступных целей. Вредоносное ПО BrutPOS компрометирует POS-терминалы, используя RDP. Вредоносное ПО осуществляет хищение данных с платежных карт клиентов, которые ранее использовали POS-терминалы.

Для осуществления такого рода атаки злоумышленникам не нужно создавать сложный и изощренный код, так как система RDP предоставляет им все необходимое инструменты для совершения преступления.

Компании могут обезопасить себя от ботнета BrutPOS, придерживаясь ряда правил. Для этого необходимо придерживаться основополагающим принципам информационной безопасности. В масштабах организации сотрудники должны придерживаться политики аутентификации и авторизации.

По данным FireEye, в состав ботнета входили 5622 компьютера в 119 странах. Эксперты обнаружили 60 RDP-систем, причем 51 из них расположена в США ***(FireEye обнаружила ботнет BrutPos, похищающий данные клиентов POS-терминалов // InternetUA (http://internetua.com/FireEye-obnarujila-botnet-BrutPos--pohisxauasxii-dannie-klientov-POS-terminalov). – 2014. – 11.07).***

***

Эксперты по безопасности из Websense Security Labs выявили варианты Zeus, реализующие информационные кражи. Новые версии вредоносных программ, отслеживаемые в течение нескольких месяцев, в настоящее время используются для кражи финансовых данных пользователей. Новые варианты Zeus используют дроперы для задействования исполняемых файлов с расширением PIF. Это расширение было очень популярным несколько лет назад и теперь, кажется, возвращается.

Эксперты из Websense ThreatSeeker Intelligence Cloud после отслеживания нового вредоносного ПО сделали вывод, что оно является более прогрессивным вариантом Zberp – вируса, созданного на основе Zeus и Carberp.

В рамках своей деятельности авторы Zeus PIF рассылали пользователям письма электронной почтой. Они содержали в себе URL-ссылку на ZIP-файл, который содержит в себе дропер и исполняемый файл с расширением PIF. Одним из прямых преимуществ файла PIF является то, что расширение скрыто, даже если система настроена на то, чтобы показывать расширения наиболее распространенных типов файлов. После установки на компьютер пользователя вредоносное ПО ищет необходимые ему данные, похищает их и передает их на C&C-серверы, используя HTTPS. Согласно данным Websense Security Labs, C&C-серверы обладали подлинным и подписанными сертификатами, выданными компанией Comodo Essential SSL ***(Троян Zeus используется для целевых атак по электронной почте // InternetUA (http://internetua.com/troyan-Zeus-ispolzuetsya-dlya-celevih-atak-po-elektronnoi-pocste). – 2014. – 11.07).***

***

Sophos зафиксировала распространение злоумышленниками макровирусов, которые были особенно популярны в 90-х годах. В тот период времени злоумышленники писали вредоносное ПО на языке программирования под названием VBA (Visual Basic for Applications). В

настоящее время VBA используется злоумышленниками для создания вредоносного ПО, которое чаще всего затрагивает файлы Excel и Word.

Количество макровирусов, написанных на VBA, резко снизилось в 2000-х годах. Макровирусы встраиваются в системы обработки данных, зачастую – в текстовые редакторы. VBA-вирусы прячутся в текстовых документах, тайно выполняя функции приложений внутри Office, таких как AutoOpen (в Word) или Auto_Open (в Excel).

На сегодняшний день эксперты Sophos обнаружили макровирусы со следующим принципом действия: когда пользователь открывает инфицированный файл, вредоносное ПО внедряется в файлы шаблонов Office, после чего вирус распространяется в другие файлы офисной программы. Мошенники часто подчеркивают то, что присутствие макросов в документах делает файл более безопасным и защищенным.

Злоумышленники зачастую пытаются ввести пользователей Сети в заблуждение, сообщая, что наличие макросов в документе обеспечивает ему защиту от вредоносного ПО. Мошенники подчеркивают в своем уведомлении, что пользователю необходимо разрешить макросы для загрузки необходимого файла. Стоит отметить, что макросы не влияют на корректное отображение файлов и зачастую злоумышленники берут во внимание неосведомленность пользователей.

Более половины атак VBA-вирусов осуществляется благодаря обману пользователей Интернета. Эксперты по обеспечению информационной безопасности подчеркивают, что в случае, когда пользователь получает уведомлении о включении макросов, скорее всего он является потенциальной жертвой нападения ***(Злоумышленники снова используют макровирусы // InternetUA (http://internetua.com/zloumishlenniki-snova-ispolzuuat-makrovirusi). – 2014. – 10.07).***

***

30 тыс. интернет-пользователей из Германии стали жертвами атаки, в рамках которой они получали письма о якобы нарушениях с их стороны авторских прав. В сообщение вкладывался файл с расширением zip, содержащий троян.

Письма электронной почты рассылались якобы от имени компаний MI, Sony, DreamWorks и Paramount. В теле письма указывалось, что пользователь нарушил авторские права на композиции следующих исполнителей и музыкальных коллективов: Jay-Z, R Kelly, Д. Бланта, Bullet for My Valentine, Sepultura и Children of Bodom. В письме пользователям предлагают уладить дело в досудебном порядке, заплатив штраф в размере от 200 до 500 евро в последующие 48 часов.

Текст одного из писем выглядит следующим образом:

«7.06.2014 вы нарушили пункт 19а закона об авторских правах. Музыкальный альбом Temper Temper группы Bullet For My Valentine был загружен с вашего IP-адреса 8.149.94.13 в 3:40:24. Такие действия нарушают

пункт 19а закона об авторских правах. Об этом нужно уведомить окружной суд. Только быстрый платеж на сумму в 400,88 евро позволит избежать этого (обращения в суд. – Ред.). Мы ожидаем оплаты в последующие 48 часов. Для того чтобы ознакомиться с деталями дела, просмотрите прикрепленный файл».

На самом деле файл с расширением zip в письме содержит в себе вирус. Его действие нацелено на кражу банковской информации пользователей. Впоследствии пользователь может стать жертвой связанного с онлайн-банкингом мошенничества, а также кражи личности ***(30 тыс. пользователей получают уведомления о нарушении авторских прав, содержащие троян // InternetUA (http://internetua.com/30-tis--polzovatelei-polucsauat-uvedomleniya-o-narushenii-avtorskih-prav--soderjasxie-troyan). – 2014. – 10.07).***

***

Специалисты международной организации Electronic Frontier Foundation заявили о наличии в операционной системе Android уязвимости, которая позволяет получить данные о точках Wi-Fi, к которым подключался смартфон.

Эта недоработка была найдена в функции Preferred Network Offload, которая впервые появилась в версии Android 3.1. Суть функции заключается в подключении смартфона к Wi-Fi при выключенном экране. Благодаря получению списка точек Wi-Fi, злоумышленник может легко следить за пользователем, даже если тот отключил функцию геолокации.

Apple и Google объявили патентное перемирие. Также Electronic Frontier Foundation решила подать иск к Агентству национальной безопасности и разведки США, требуя разъяснить, использовали ли эти организации эту уязвимость в программе глобальной слежки.

В свою очередь Google уже выпустил патч wpa_supplicant, который должен ликвидировать проблему ***(Из-за уязвимости Android злоумышленники могут узнать местонахождение пользователя // InternetUA (http://internetua.com/iz-za-uyazvimosti-Android-zloumishlenniki-mogut-uznat-mestonahojdenie-polzovatelya). – 2014. – 10.07).***

***

История и перспективы хакерского движения Anonymous

Мало найдётся людей, которые ни разу не слышали о хакерской группировке Anonymous и ее фракциях LulzSec и AntiSec. Пик их популярности пришёлся на период между 2008 и 2012 г., когда они обнародовали массу электронной почты из корпоративной и правительственной переписки, выяснили некоторые секреты АНБ и коммерческих структур. Казалось, что этих людей никто не остановит, но потом они внезапно затихли, и их молчание длится второй год. Что же произошло?

Закат публичной деятельности группы хакеров начался с ареста Г. Монсегура в 2011 г., который после этого стал правительственным информатором и помог засадить за решётку нескольких главных участников Anonymous в 2011–2012 гг. Аресты привели к тому, что активность группировки заметно сократилась: кроме атаки на несколько правительственных сайтов в США и на сайты университета MIT в память покончившего с собой программиста А. Шварца, Anonymous больше не предпринимали никаких шагов.

Поговаривают, что сдерживающим фактором стало предательство Г. Монсегура, ранее занимавшего один из ключевых постов в сообществе. Другие же эксперты и рядовые хакеры полагают, что группировка просто наращивает силы и готовит какую-то новую акцию.

В управлении кибербезопасности США говорят, что организация может вернуться, хотя и не рассчитывают на то, что атаки ее будут масштабными. Во многом потому, что в действиях «Анонимусов» есть очень много схожего с флешмобом: появление новых участников и действий нельзя спрогнозировать, основываясь только на законах логики, как нельзя и засадить абсолютно всех за решётку, чтобы прекратить атаки и появление новых хакеров.

В скрытых личностях и быстрой самоорганизации Anonymous – не только сила, но и уязвимость этой структуры. Чтобы движение было эффективным, а атаки – скоординированными, участникам сообщества приходится хоть немного, но общаться друг с другом, оставлять о себе данные (помимо никнеймов) и выходить на контакт не только с «тёмной стороной» Интернета.

Сама группировка появилась спонтанно и непредсказуемо. Примерно в 2006 г. в ветке популярного форума 4chan и в IRC-канале для хакеров-энтузиастов организовались первые участники сообщества, которые развлечения ради решили взломать что-нибудь. Первые взломы и DDoS-атаки были на коммерческие сайты, а к более серьезным проектам хакеры перешли в 2008 г. Первую публичную акцию группа хакеров назвала Operation Basement Dad: группа создала в микроблогах учётную запись @basementdad и публиковала там новости о Д. Фритцле, австрийце, который 24 года держал в подвале и насиловал собственную дочь. Полмиллиона фолловеров в Twitter аккаунт набрал за считанные дни, но администрация сервиса его закрыла.

От скандальных микроблогов хакеры решили перейти к атаке на так называемую Церковь Саентологии – популярную авторитарную секту, которая оказала давление на YouTube с требованием удалить видео с Т. Крузом, одним из адептов учения. «Анонимусы» принялись высмеивать саентологов на фоне усилившегося потока статей и сообщений о том, как влиятельная секта «промывает» мозги своим адептам, манипулирует информацией и наказывает тех, кто подвергает сомнению ключевые догматы саентологов. Новый проект группировки назывался Project Chanology и

включал в себя не только антипиар, но и атаки на ключевые веб-сайты «Церкви». Именно тогда и появились первые видео от Anonymous с анонсами будущих атак и намерений хакеров, а также, слоганом «Мы – Anonymous; имя нам – Легион» и маской Г. Фокса, как символа движения анонимных хакеров.

Небольшой период затишья продлился с 2009 до 2010 г., когда из-за иска против файлообменников и давления со стороны американских правообладателей «Анонимусы» решили подготовить новые атаки. А самой громкой стала «Операция “Расплата”» – серия DDoS-атак обрушилась на корпоративные сайты PayPal, Visa и MasterCard за отказ обслуживать взносы в пользу WikiLeaks после утечки правительственных секретов от экс-военнослужащего Челси Мэннинга (ныне сменившего пол и отбывающего наказание в федеральной тюрьме США).

Атаки в защиту WikiLeaks привлекли к группировке внимание СМИ. В публичном канале чата, где «анонимусы» общались с поклонниками и журналистами, активность выросла с 700 до 7 тыс. человек.

Именно тогда и возникли первые разногласия между хакерами: часть из них считали, что не было смысла атаковать сайт PayPal. Тогда же появилась новая платформа для координации атак и согласования действий всей группировки под названием AnonOps. В 2011 г. появляется вторая группа, под названием Lulzsec – эта команда предпочитала заниматься не политическими акциями, а взломами и атаками из чисто «спортивного» интереса к выявлению уязвимостей.

Anonymous долгое время были полностью децентрализованы, и все решения принимались коллективно. В скором времени у них появился хакер с ярко выраженными лидерскими качествами и идеологической платформой – Г. Монсегур, более известный в сообществе, как Sabu. Оставим в стороне его гремучую смесь политических взглядов (включая поддержку социальных революций на Востоке) и сосредоточимся на том, как он создал группировку LulzSec внутри «Анонимусов» в 2011 г.

Всего за 50 дней группа сумела нанести удары по правительственным структурам, медиа-компаниям, частному корпоративному бизнесу и гигантам вроде Sony Pictures Entertainment. Всё это время Г. Монсегур не скрывал успехов LulzSec, публикуя детали в Twitter.

Г. Монсегур стал иконой для многих хакеров и своего рода символом движения Anonymous: заурядный 28-летний безработный с навыками в IT, заботящийся о двух несовершеннолетних кузинах, в Интернете стал харизматичным лидером самого опасного и разыскиваемого сообщества, которым интересовались в ФБР и ЦРУ.

Хакеры-новички и увлечённые сторонники «анонимусов» охотно сливали информацию одному из организаторов, что в последствии сыграло с движением злую шутку: лидер-одиночка летом 2011 г. был арестован, а его познания о структуре сообщества и основных информаторах очень пригодились людям в костюмах и тёмных очках с бейджами «федералов».

Сами агенты говорят, что большая часть участников Anonymous – не хакеры в классическом понимании этого слова. У них нет даже осознания того, что информаторы и «кроты» – один из ключевых компонентов хакинга, как такового.

Сообщество «анонимусов» оказалось более гибким и масштабируемым, чем «хардкорные» хакеры из прошлого, с которыми ранее сталкивались американские спецслужбы. Это единственное, что уберегло группировку от ликивдации и распада. Хотя в 2012 г. медиа-удар по группировке нанесла редакция Fox News, обнародовав тот факт, что Г. Монсегур стал информатором американского правительства. С тех пор активность движения хакеров пошла на спад: Anonymous перестали доверять так, как раньше, хотя в телефонном разговоре с репортерами Г. Монсегур заявил, что ФБР даёт информаторам иммунитет от ареста, а сами правоохранительные структуры крайне коррумпированы. Мол, ему предлагали взламывать иностранные ресурсы в интересах американского правительства, а когда он отказался это делать – осудили и упекли в тюрьму. Арест ключевых участников сообщества на 1,5 года приостановил активность хакерской группировки.

«Двадцать вторая уловка» в случае с Anonymous заключается в том, что для успешности им нужно много внимания, а внимание привлекает не только поклонников и адептов, но и спецслужбы.

В настоящее время у движения хакеров – сложные времена, вызванные подорванным доверием, отсутствием чёткого руководства, единого лидера и опасениями, что новая «верхушка» движения снова попадёт в руки ФБР.

Правда, в самих американских спецслужбах говорят, что длительное затишье в Anonymous не означает, что движение пошло на спад. Такова специфика этого объединения хакеров. Кроме того, у Интернета довольно «короткая память»: не пройдёт и пары лет, и многие из тех, кого обвинили в сотрудничестве с ФБР, могут опять вернуться в движение в новой роли ***(История и перспективы хакерского движения Anonymous // InternetUA (http://internetua.com/istoriya-i-perspektivi-hakerskogo-dvijeniya-Anonymous). – 2014. – 12.07).***

***

Согласно информации CSIS Security Group of Denmark, программный код вредоносного ПО Tinba, который ориентировано на online-счета клиентов различных банков, снова просочился в сеть.

Вредоносное ПО, известное под названием Tinba или Zusy, было впервые обнаружено в середине 2012 г. Троян инфицировал в тот период времени тысячи компьютеров по всей территории Турции. Размер вредоносного ПО всего лишь 20 килобайт, однако оно может оказать такой же негативный эффект, как и более масштабные трояны.

На прошлой неделе специалисты компании CSIS обнаружили пост, опубликованный на подпольном форуме, который содержал исходный код

Tinba, аналогичный тому, который эксперты CSIS обнаружили несколько лет назад. Об этом сообщает технический директор компании П. Крузе.

Предполагается, что злоумышленники могут воспользоваться утечкой вредоносного кода для достижения преступных целей. Преступники могут создать новое вредоносное ПО взяв за основу Tinba. Аналитики компании CSIS высказали мнение о том, что код Tinba был продан мошенникам для его совершенствования и выпуска новых троянов.

Tinba может нарушить корректную работу интернет-банкинга. Троян создает новые поля, которые пользователь должен заполнить при использовании сервиса интернет-банкинга. Вследствие этого, банковские счета пользователей могут быть скомпрометированы ***(Исходный код трояна Tinba снова просочился в Сеть // InternetUA (http://internetua.com/ishodnii-kod-troyana-Tinba-snova-prosocsilsya-v-set). – 2014. – 13.07).***