СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(11–23.03)

2014 № 6

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(11–23.03)
№ 6

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Інтернет асоціація України оприлюднила своє свіже лютневе дослідження інтернет-аудиторії України, яке щомісяця виконує дослідна компанія Factum Group Ukraine.

Згідно з останніми даними, щоденна аудиторія Twitter становила 5 % – близько 600 тис. користувачів (загальна денна аудиторія в Україні – 12 млн користувачів). Місячна аудиторія Twitter (частка людей, які хоча б один раз на місяць заходили на Twitter) – 21 %. Це близько 4 млн користувачів (місячна аудиторія користувачів в Україні – близько 20 млн).

Варто зауважити, що багато твітерян користуються Twitter виключно через мобільний додаток цього сервісу, і вони не включені в дослідження ***(В лютому 4 млн українців заходили на Твітер // UkrainianWatcher (http://watcher.com.ua/2014/03/19/v-lyutomu-4-mln-ukrayintsiv-zahodyly-na-tviter/). – 2014. – 19.03).***

***

Во «ВКонтакте» появился виджет, позволяющий встраивать посты пользователей соцсети на сторонние сайты. Об этом Lenta.ru 12 марта сообщил пресс-секретарь «ВКонтакте» Г. Лобушкин.

Чтобы добавить на интернет-страницу пост или комментарий из «ВКонтакте», теперь достаточно вставить на сайт специальный код со ссылкой на запись. Найти код для вставки можно рядом с самим постом, нажав на кнопку «поделиться» и в открывшемся окне выбрав ссылку «экспорт записи». Подробное описание того, как встроить виджет на сайт или в блог, можно найти в разделе документации «ВКонтакте».

При этом виджет позволяет не только ознакомиться с самим постом, но также поставить ему лайк и поделиться ссылкой с друзьями, не покидая страницы использующего его ресурса. Кроме того, как отметил Г. Лобушкин, виджет обладает «широкими мультимедийными возможностями». Иными словами, в нем сохраняются все прикрепленные к посту фотографии, аудио- или видеозаписи.

Ранее виджеты для экспорта контента из «ВКонтакте» позволяли вставлять на сторонние сайты только видео, блоки с информацией о том или ином сообществе, а также ссылки на опросы в соцсети и различные кнопки «ВКонтакте» («мне нравится», «подписаться» и др.) ***(Во «ВКонтакте» появился виджет для экспорта постов // InternetUA (http://internetua.com/vo--vkontakte--poyavilsya-vidjet-dlya-eksporta-postov). – 2014. – 12.03).***

***

Сервис микроблогов Twitter запустил поддержку новых доменных зон в самоей социальной сети и ее приложении Tweetdeck. Теперь записи типа

nic.berlin или fire.plumbing автоматически превращаются в кликабельные сслыки. Эта функция доступна еще не для всех доменов, запущенных по программе New gTLD.

Возможно, из-за чрезмерного шума, поднятого рекламой, техподдержка социальной сети не спешит с освоением доменов, запущенных в последние недели, и в дальнейшем будет их подключать с некоторой задержкой.

Но в любом случае, поддержка новых доменных зон со стороны Twitter с его аудиторией в 232 млн пользователей – большой шаг вперед. Люди уже привыкли к тому, что для того, чтобы дать ссылку на сайт, не нужно копировать URL полностью.

Также кликабельные ссылки на домены в новых зонах сделают их более узнаваемыми. Без них многие пользователи не будут воспринимать их как название сайта ***(Twitter начал поддерживать New gTLD (IT Expert (http://itexpert.org.ua/rubrikator/item/34385-twitter-nachal-podderzhivat-new-gtld.html). – 2014. – 11.03).***

***

В США создают единую государственную сеть для нужд полиции, пожарной службы и других государственных структур.

Единая коммуникационная сеть FirstNet покроет всю территорию страны. Предполагается, что сеть будет изолирована от обычного Интернета, но при этом обеспечит надёжность связи и будет гарантированно работать в любых условиях.

Посредством FirstNet полиция США будет передавать служебную информацию в пределах страны. Разработчики отмечают, что сеть не будет присоединена к Интернету хотя бы потому, что в любой критической ситуации из-за наплыва пользователей он может дать сбой.

Офицер полиции, сфотографировав подозреваемого, сможет оперативно запросить из центральной базы данных досье на него. В свою очередь пожарные службы смогут координировать работу, что особенно важно в чрезвычайных ситуациях, например, при тушении лесных пожаров.

Сеть FirstNet строится на базе технологии 4G. Она успешно прошла тестирование в нескольких штатах. В 2014 г. её планируют запустить в национальном масштабе ***(В США создают специальную сеть для координации работы госслужб // InternetUA (http://internetua.com/v-ssha-sozdauat-specialnuua-set-dlya-koordinacii-raboti-gosslujb). – 2014. – 15.03).***

***

Многие пользователи украинского сегмента Facebook в среду, 19 марта, получили уведомления об изменении работы с почтой.

Если ранее при регистрации в Facebook автоматически создавался новый адрес (и по умолчанию именно на него должны были приходить письма), то теперь соцсеть внесла изменения. И признала очевидное: люди

предпочитают почтовые ящики, которые наиболее часто используют – gmail и т. д.

Теперь все письма будут перенаправляться именно на указанные в профиле адреса не родного «фейсбучного» почтового сервиса.

О планах по постепенному закрытию почтового сервиса стало известно в последних числах февраля. Тогда в компании подтвердили, что окончательно электронные почтовые ящики @facebook.com будут удалены в марте ***(Facebook меняет адреса // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_menyaet_adresa). – 2014. – 19.03).***

***

Если человека спрашивают, представляют ли два разных лица одну и ту же персону, он отвечает с точностью 97,53 %. Новое программное обеспечение Facebook показывает почти идентичный результат 97,25 % независимо от освещения или направления лица. Это беспрецедентная точность распознавания для систем искусственного интеллекта, которые традиционно справляются с подобными задачами значительно хуже людей. Исследователям удалось также на 25 % снизить количество ложных срабатываний по сравнению с аналогичными разработками конкурентов.

Новая технология под названием DeepFace создана в научно-исследовательском подразделении Facebook с целью улучшить движок автоматического распознавания чужих лиц на личных фотографиях, которые пользователи загружают на сайт социальной сети. Хотя такая практика признана незаконной в некоторых странах, компания Facebook все равно продолжает исследования. Разработки могут найти применение далеко за пределами социальной сети. Например, в системах наружного наблюдения, которые в ближайшие годы должны покрыть почти всю территорию большинства мегаполисов.

Исследователи из Facebook использовали самообучаемую нейросеть, которую тренировали на большой базе данных из реальных фотографий. Facebook обладает архивами фотографий, где пользователи сами помечают имена друзей на разных фотографиях, предоставляя уникальную возможность проанализировать одни и те же лица в разных ракурсах. Для тренировки нейросети использовали крошечную часть этой базы: 4,4 млн фотографий от примерно 4030 человек.

DeepFace анализирует лица по многоступенчатой схеме. Сначала нужно определить наличие лица на фотографии и выделить его контуры. Затем составляется схема по 67 ключевым точкам на лице. После этого схема трансформируется в 3D-маску, которую можно вращать во всех плоскостях и сравнивать с такими же масками, полученными при анализе других фотографий, а также самостоятельно генерировать 2D-снимки лица под любыми ракурсами и под любым освещением.

Научная работа DeepFace: Closing the Gap to Human-Level Performance in Face Verification будет опубликована в журнале IEEE Conference on Computer Vision and Pattern Recognition в июне 2014 г. ***(Нейросеть Facebook распознает лица с беспрецедентной точностью // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/19/fb-face-recognition.html). – 2014. – 19.03).***

***

Корпорация Google (владеет YouTube) работает над версией видеосервиса, предназначенной для использования детьми младше 10 лет.

Содержимое «детского» YouTube будет тщательно фильтроваться, чтобы защитить маленьких зрителей от вредных и опасных видео и комментариев – например, содержащих нецензурную лексику. На YouTube уже реализована функция, позволяющая сделать просмотр видео более безопасным для детей. При ее активации пользователю перестает демонстрироваться потенциально вредное содержимое, пишет «Российская газета» ***(Youtube разрабатывает версию для детей // Клерк.Ру (http://www.klerk.ru/soft/news/363718/). – 2014. – 19.03).***

***

Facebook постоянно тестирует новые функции на небольшой группе людей до того, как выпустить нововведения в массы.

Одна из таких функций – постоянная панель уведомлений, которая стала доступной для некоторых пользователей Android в прошлом году. Социальная сеть приняла решение ее вернуть, добавив небольшое обновление: фото вашего профиля появиться рядом со знакомыми пиктограммами. Facebook-бар станет частью панели управления независимо от того, есть ли у вас новые сообщения или заявки на добавление в список друзей.

Готовьтесь к тому, что каждый раз, когда вы заходите в панель уведомлений, вы будете видеть свое фото.

Пока лишь небольшое количество пользователей имеет доступ к нововведению, которое можно отключить в настройках смартфона ***(Экспериментальное меню уведомлений Android вмещает ваше фото из Facebook // Vido.com.ua (http://vido.com.ua/article/8209/ekspierimiental-noie-mieniu-uviedomlienii-android-vmieshchaiet-vashie-foto-iz-facebook/). – 2014. – 20.03).***

***

В настоящее время избранные тестеры Twitter имеют возможность опробовать в действии новую возможность системы – так называемую Fave People. Это просмотр «твитов» только от избранных пользователей. Данная функциональная надстройка появилась совсем недавно в «альфа»-версии

приложения Twitter для Android. Когда же случится полноценная реализация – пока не известно. Журналисты веб-сайта TechCrunch опубликовали несколько скриншотов с запущенной Fave People.

Напомним, что еще в декабре прошлого года для Android-приложения Twitter было выпущено специальное обновление, которое позволяло выделять из общего числа пользователей, на которых была сделана подписка, тех индивидов, за сообщениями которых было особенно интересно следить. Очень удобно, если общее число подписанных каналов превышало все разумные пределы. Уведомления появлялись всякий раз, когда такой избранный пользователь публиковал свой твит. Теперь же Fave People позволит сделать отдельную новостную ленту из подобных сообщений ***(Twitter позволит отслеживать сообщения от избранных пользователей // InternetUA (http://internetua.com/Twitter-pozvolit-otslejivat-soobsxeniya-ot-izbrannih-polzovatelei). – 2014. – 20.03).***

***

Twitter подумывает о том, чтобы значительно упростить технический «язык», используемый для общения в соцсети. Это должно облегчить новичкам освоение сервиса микроблогов, однако наверняка оттолкнет опытных пользователей. Журналистам удалось заполучить скриншоты нового экспериментального интерфейса.

О возможном нововведении заявила глава новостного отдела Twitter В. Шиллер. Она отметила, что система хештегов (кодовые слова, начинающиеся со значка #) и реплаев (ответы другим пользователям, включающие их Twitter-имя со значком @) может быть плохо понятной для новичков. Представитель соцсети намекнула, что Twitter подумывает отказаться от этих функций в пользу более простого в освоении интерфейса.

Издание BuzzFeed получило у Twitter комментарии по поводу данного высказывания В. Шиллер. В соцсети отметили, что позиция главы новостного отдела совпадает с позицией главы компании Д. Костоло, который активно занимается упрощением «технической» части взаимодействия пользователей с Twitter.

«Выдвигая отображение контента в Twitter на первый план и сглаживая сложности взаимодействия с языком Twitter, мы сумеем улучшить взаимодействие пользователей с ресурсом. Благодаря обновлениям новые пользователи, даже если они оказались на сайте случайно, смогут быстро освоиться и начать считать сервис незаменимым», – отметил глава соцсети.

Журналисты полагают, что в скором времени Twitter откажется от ответов со значком @ и заменит их на систему, при которой будет отображаться только непосредственно имя пользователя. Примерно то же самое уже реализовано в Facebook.

Тем не менее, В. Шиллер так и не дала прямого ответа на вопрос о том, что Twitter будет делать с хештегами и реплаями. На вопросы журналистов представитель компании уклончиво посоветовала следить за новостями,

отметив, что команда Twitter активно работает над тем, чтобы сделать ресурс более интуитивным.

Напомним, что ранее Twitter уже облегчал язык сайта для того, чтобы упростить взаимодействие. К примеру, в первое время существования сервиса для того, чтобы сделать ретвит записи другого пользователя, необходимо было вручную дописать к ней RT. Позже в Twitter решили сделать для этого специальную клавишу, что сильно упростило жизнь всему Twitter-сообществу.

Несмотря на проделанную Twitter работу, многие пользователи по-прежнему с трудом обучаются работе в сервисе микроблогов. В соцсети сложился собственный, иногда малопонятный чужим людям жаргон, активно использующий сокращения. Система реплаев и хэштегов по сути своей логична, однако поначалу кажется весьма непривычной практически каждому новому пользователю. В настоящее время Twitter приходится именно осваивать, причем зачастую с чьей-либо помощью ***(Twitter задумал отменить хештеги и реплаи // InternetUA (http://internetua.com/Twitter-zadumal-otmenit-heshtegi-i-replai). – 2014. – 21.03).***

***

Соцсеть Facebook представила новый язык программирования Hack – модификацию языка PHP, на который компания уже перевела значительную часть кода соцсети, говорится на официальном сайте компании, посвященном языку Hack.

Для Facebook, число пользователей которой превышает 1,2 млрд человек, ключевым требованием к языку программирования должна быть возможность быстро прописывать большие объемы кода, а также его гибкость, чтобы оперативно исправлять возможные ошибки. Язык Hack проходил внутреннее тестирование в Facebook около года, руководят проектом его создатели – разработчики Б. О'Салливан, Д. Верлаге и А. Менгхраджани.

«Hack – это язык программирования для использования на виртуальной машине HHVM, который совместим с PHP. Hack сочетает быстрый цикл разработки PHP с упорядоченностью, которую вносят статические переменные», – отмечается в описании языка.

Напомним, что статические языки (например, Java) требуют проверки ошибок в процесс написания кода, тогда как более современные динамические языки (PHP) позволяют писать код с ошибками, а исправлять их уже при исполнении программы. Таким образом, замысел Hack – сочетать быстроту разработки и возможность «отловить» и исправить ошибку на ранней стадии.

Язык Hack – Open Source-проект, его исходные коды будут открыты для участников сообщества, которые смогут не только внедрять его в свои разработки, но также помогать в его улучшении ***(Facebook представила собственный язык программирования Hack // InternetUA***

(http://internetua.com/Facebook-predstavila-sobstvennii-yazik-programmirovaniya-Hack). – 2014. – 22.03).

***

Приложение #Music так и смогло привлечь внимание пользователей сервиса Twitter. 21 марта его убрали из App Store, но те, кто установил его на компьютер, смогут продолжить пользоваться ресурсом до 18 апреля. Twitter начнёт работать над другим музыкальным контентом, так как этот проект смог продержаться ровно год. Его создатели продали новинку системе, но он так и не смог «прижиться» в сети. Изначально приложение было предназначено для поиска интересной музыки. Альбомы и исполнители должны были выбираться на основе того, что предложит Twitter. Все треки были собраны в одно место, они брались, в основном, у партнёров – Spotify и Rdio. Также их можно было приобрести через iTunes. Информация о том, что #Music будет закрыт, появилась после того как в компании остался только основатель приложения – С. Филлипс ***(Twitter закрыл своё музыкальное приложение #Music // Bit-news.ru (http://bit-news.ru/categories/internet/20589-twitter-zakryl-svojo-muzykalnoe-prilozhenie-music). – 2014. – 22.03).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Євромайдан, який розпочався в листопаді 2013 р. і перетворився з мирного протесту на збройне протистояння населення з режимом В. Януковича, кардинально змінив взаємодію людей з новинарною інформацією.

Ще у вересні 2013 р. лише близько 10–15 % денної аудиторії українського Інтернету читали хоча б одну новину суспільно-політичної тематики. Тобто новини щодня переглядало не більше 1,5–2 млн українських користувачів Інтернету.

На сьогодні ситуація інакша. 1,5–2 млн – це аудиторія в окремі дні лише однієї «Української правди», а загальна денна аудиторія українських ЗМІ вже наближається до 7 млн – це унікальна аудиторія (тобто якщо користувач відвідав сьогодні і УП, і ТСН.ua, то ми рахуємо його як одного користувача).

Одну з ключових ролей для такого різкого зростання трафіку відіграли соціальні мережі.

Якщо в жовтні 2013 р., згідно з даними Liveinternet, денний трафік із соцмереж на сайти українських ЗМІ становив 180–200 тис. переходів, то в лютому – березні 2014 р. ця цифра зросла до 2–2,5 млн переходів щодоби.

Суттєво зріс трафік із Twitter. У жовтні 2013 р. більшість українських новинарних сайтів узагалі не розглядали Twitter як джерело трафіку, а нині він генерує щодоби 150–250 тис. переходів.

Цікаво також подивитись, як за останні два роки Facebook та Twitter «з'їли» «ВКонтакте». Ще на початку 2012 р. частка «ВКонтакте» в загальному трафіку на новинарні ЗМІ становила близько 60 %. На сьогодні – уже менше 30 %.

Зростають переходи з Facebook не лише на новинарні, а й на всі інші сайти. У січні – березні 2014 р. уперше за весь час вимірів частка трафіку з Facebook на сайти Уанету перевищила трафік із «ВКонтакте» ***(За останні 5 місяців переходи з соціальних мереж на сайти ЗМІ зросли у 8-10 разів // UkrainianWatcher (http://watcher.com.ua/2014/03/17/za-ostanni-5-misyatsiv-perehody-z-sotsialnyh-merezh-na-sayty-zmi-zrosly-u-8-10-raziv/). – 2014. – 17.03).***

***

Ініціативна група російських інтернет-користувачів запустила в соціальних мережах Facebook та «ВКонтакте» спільноту «Антипропаганда», повідомляє AIN.UA.

Активісти аналізують відео російських медіа на предмет пропаганди, перекручування фактів, фейків та ін. Аналіз відбувається на основі тематичних досліджень, наприклад «Міжнародна енциклопедія пропаганди» Р. Коула.

Волонтери-аналітики пояснюють аудиторії, які методи пропаганди були використані, подаючи ці відомості у вигляді інфографіки.

Волонтери пропонують також відеоаналіз новинних повідомлень.

Одним із засновників групи є московський депутат М. Кац, який свого часу працював у виборчому штабі О. Навального, а також мав спільні проекти з відомим російським блогером І. Варламовим.

За словами М. Каца, у проекті «Антипропаганда» є четверо осіб, за гроші працює лише дизайнер. «Його робота обійшлася в 15 тис. р., але він дав відстрочку з платежем до того часу, коли ми налагодимо збір грошей», – сказав засновник ініціативи.

Він також пояснив, чому аналізує лише російські випуски новин і не бере до уваги іноземні. За словами М. Каца, його в першу чергу турбує те, що населення РФ «обробляють з екранів телевізорів мерзенними пропагандистськими прийомами, які в книжках про пропаганду описані». Активіст каже, що існування подібного явища в інших країнах не виправдовує того жаху, який відбувається в Росії.

Нині у спільноти «Антипропаганда» в соцмережі «ВКонтакте» майже 7 тис. передплатників, у Facebook – майже 12 тис.

Раніше в Україні вже створили інтернет-ресурс для розвінчування російської пропаганди – StopFake.org, а також блог fakecontrol.org, який спростовує неправдиві повідомлення про Україну ***(Росіяни започаткували***

інтернет-проект аналізу кремлівської пропаганди // «Телекритика» (http://osvita.mediasapiens.ua/material/28682). – 2014. – 17.03).

***

Міністерство оборони України просить журналістів, блогерів та пересічних громадян обережно ставитися до публікування інформації про переміщення українських військ, адже нею може скористатися ворог. Про це повідомляється на Facebook-сторінці міністерства від імені представника регіонального медіацентру Міноборони в м. Львів І. Крочака.

«Ваша діяльність щодо донесення до громадян України своєчасної та об'єктивної інформації щодо подій у нашій державі є дуже важливою та потрібною, – каже І. Крочак. – Проте, у зв'язку з оголошенням часткової мобілізації, потрібно зважати на те, що з допомогою мережі Інтернет Ваші повідомлення, матеріали, фото-, відеодокументи можуть переглядати і недруги України».

За словами військовослужбовця, вони не бажають обмежити доступ до об'єктивної інформації, однак деякі відомості просять повідомляти максимально обережно, дозовано, залежно від необхідності. Ідеться про чисельність, нумерацію, укомплектованість військових підрозділів, маршрути їх пересування, а також прізвища командирів і начальників.

Автор звернення пояснює, що таку інформацію можна сміливо використовувати, якщо вона поширена прес-службою Міноборони. Якщо ж комусь довелося стати очевидцем пересування військовослужбовців чи військової техніки, то треба добре подумати, перш ніж фотографувати та публікувати побачене, наголошує І. Крочак.

«Звичайно ж, питання військової цензури є складними і вони важко співставляються з принципами відкритої журналістики, але навіть у найпередовіших демократичних державах світу: США, Великобританії, Франції та ін., інформація про пересування та боєготовність збройних сил має серйозні обмеження до її поширення», – зазначається у зверненні.

У міністерстві просять громадян здійснювати інформаційну діяльність, враховуючи інтереси національної безпеки України ***(Міноборони просить не розповідати у соцмережах про переміщення українських військ // «Телекритика» (http://osvita.mediasapiens.ua/material/28760). – 2014. – 19.03).***

***

На сьогодні в соцмережах з'являється більше інформації, ніж її видає Рада національної оборони і безпеки. Про це в ефірі Еспресо.TV заявив політолог О. Кошель.

Зокрема, коментуючи заяву віце-адмірала І. Кабаненка щодо підготовки Росією масштабного наступу на Україну, О. Кошель зазначив, що РНБО в нинішніх умовах має бути єдиним інформаційним центром ***(О. Кошель: РНБО зараз менш потужний інформаційний центр, ніж соцмережі //***

Espreso.tv (http://espreso.tv/new/2014/03/12/koshel_rnbo_maye_buty_yedynym_informaciynym_centrom). – 2014. – 12.03).

***

В сети Facebook объявили акцию «Крутой пацан? Купи аккумулятор для военных». Инициаторы приглашают предпринимателей и патриотов пополнить склад гарнизонов в Харьковской области. Собирают шины, аккумуляторы, топливо и радиостанции.

Приглашают скидываться деньгами или покупать готовые шины и батареи.

«Объединенные потребности по Харьковской области, которые требуют нашей с вами срочной помощи. Я уверена, у вас много крепких предпринимателей и патриотов. Наша задача – просто передать эту информацию, и ребята начнут постепенно оказывать столь нужную поддержку», – сообщает в Facebook активистка Татьяна.

В сообщении уточняют, что за короткое время проведения акции планируют собрать 400 аккумуляторных батарей, 600 колес и 250 т горючего для военной техники ***(В соцсетях объявили акцию по сбору шин и топлива для военных в Харькове // infa.kharkov.ua (http://infa.kharkov.ua/v-socsetyax-obyavili-akciyu-po-sboru-shin-i-topliva-dlya-voennyx-v-xarkove/). – 2014. – 17.03).***

***

Бойкот «Одноклассников» и «ВКонтакте»: украинцы запускают социальную сеть WEUA

Через 10 дней в Украине появится собственная социальная сеть – такая же, как Facebook в США или «ВКонтакте» в России. Называться она будет WEUA, а выглядеть – почти так же, как ресурс М. Цукерберга, только цветовая гамма у украинского аналога будет не сине-серой, как в Facebook, а черно-зеленой, пишет Marketing Media Review (http://mmr.ua/news/id/bojkot-odnoklassnikov-i-vkontakte-ukraincy-zapuskajut-socialnuju-set-weua-38890/).

Пока по адресу WEUA.info находится страница с презентацией соцсети под слоганом «Я переезжаю». В этом суть запуска: авторы надеются, что пользователи откажутся от использования российских социальных сетей, в которых их ждет антиукраинская пропаганда. «Команда WEUA 19.03.2014 года объявляет всеукраинский бойкот российских социальных сетей “ВКонтакте” и “Одноклассники”. Просим присоединиться всех неравнодушных», – пишут создатели в презентации WEUA.

Чтобы присоединиться к бойкоту, предлагается опубликовать на своей странице фотографию с текстом «Бойкот “ВКонтакте”и “Одноклассники”», а когда украинский аналог этих соцсетей заработает, удалить свои страницы на российских ресурсах, указав причину «Мы за украинское – Мы на weua.info».

Разработчики, похоже, предусмотрели в своей социальной сети все возможности, к которым мы так привыкли в популярных аналогах. Справа на главной странице расположены ссылки для быстрой навигации, как «ВКонтакте»: друзья, фотографии, аудиозаписи и так далее, а по центру – вся информация о пользователе.

Пользователь украинской соцсети сможет загружать в нее фото и видео так же, как и в популярных аналогах. Он сможет публиковать их у себя на странице и показывать в ленте своих друзей.

Под видео, фото и текстовым контентом можно ставить лайки, писать комментарии, делиться и т. д. Здесь также отображается количество просмотров. Правда, сама страница просмотра выглядит немного хмуро.

Работа с фотографиями и альбомами в WEUA будет происходить по аналогии с «ВКонтакте». Об автоматической синхронизации фотографий из смартфона и других устройств в презентации не сказано – возможно, в первой версии украинской социальной сети она пока не предусмотрена.

На странице «Мои друзья» также доступны фильтры для удобного поиска новых контактов: область, пол, возраст. Нет фильтра «страна», возможно, авторы считают, что в WEUA должны быть зарегистрированы только украинцы.

То, ради чего многие пользователи все еще не могут покинуть «ВКонтакте» – удобный музыкальный сервис – будет и здесь. Все необходимые функции в плеере есть, и даже предусмотрены оценки в виде звездочек.

Личные сообщения реализованы так же, как во «ВКонтакте». Есть и стандартные смайлы, однако не известно, будет ли у WEUA предусмотрена технология быстрых сообщений или же для того, чтобы написать другу, придется переходить на специальную страницу.

Лента новостей выглядит очень похожей на хронику в Facebook. Здесь пользователи увидят большие картинки с текстом слева. Внизу под записями кнопки лайк, поделиться и поле для комментариев.

В WEUA будут и сообщества – куда ж без них. SMM-специалисты соцсети «ВКонтакте» будут чувствовать себя здесь уютно, ведь принцип работы с группами в украинской сети, судя по всему, почти полностью скопирован с сети П. Дурова.

Запуск WEUA запланирован на 31 марта 2014 г.

В прошлом году И. Ашманов рассказывал на iForum о цифровом суверенитете – по его словам, в современном мире господство в Интернете можно сравнить с господством в небе во время Второй мировой войны. И защитить себя на просторах сети от антинациональной пропаганды может только та страна, у которой есть своя интернет-инфраструктура. А именно – своя поисковая система, свои социальные сети и т. д. Во всем мире только три страны могут похвастаться такой роскошью: США, Китай и Россия. И Украине стоит примкнуть к одной из них, если она хочет сохранить свою независимость, подчеркнул И. Ашманов.

И. Ашманов, известный своими политическими взглядами на «русский мир», призвал украинцев присоединиться к России, поскольку из трех вышеперечисленных стран нашему народу ближе всего именно она. Однако, если WEUA все же успешно запустится и сможет конкурировать с «ВКонтакте», «Одноклассниками» и даже Facebook, для выстраивания собственного цифрового суверенитета украинцам, по сути, не будет хватать только поисковика. Дело за малым? ***(Бойкот Одноклассников и ВКонтакте: украинцы запускают социальную сеть WEUA // Marketing Media Review (http://mmr.ua/news/id/bojkot-odnoklassnikov-i-vkontakte-ukraincy-zapuskajut-socialnuju-set-weua-38890/). – 2014. – 21.03).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Новое исследование от компании Kentico Software выявило ряд проблем, с которыми сталкиваются бренды при продвижении в Facebook и других соцсетях. Результаты показали, что более 300 респондентов старше 18 лет обычно не обращают внимания на брендовые посты.

Kentico обнаружила, что 68 % опрошенных всегда или почти всегда игнорируют брендовые посты в Facebook, Twitter и Instagram, но при этом всего лишь 5 % отписываются от страницы или аккаунта.

Другие результаты исследования:

72 % респондентов сказали, что они никогда или почти никогда не покупают товар, рекламу которого они увидели в социальных сетях;

35 % доверяют рекомендациям и отзывам в сети и покупают продукт;

73 % заявили, что реклама в социальных сетях никогда или почти никогда не влияет на их мнение о бренде;

40 % вообще не подписываются на брендовые страницы в Facebook;

39 % подписаны на 10 страниц;

7 % – на 11–20 страниц;

6 % – 21–30 страниц;

39 % пользователей подписались на брендовые страницы в Facebook, чтобы быть в курсе спецпредложений и акций, 12 % – следуя рекомендациям друзей, а 8 % искали информацию о бренде.

Самые популярные причины, почему пользователи отписываются – неинтересный брендовый контент (32 %) и переизбыток постов (28 %).

Основатель и генеральный директор Kentico П. Палас: «Может быть исследование Digital Experience Survey не принесло многим хороших новостей, но оно еще раз доказывает, что успех брендов должен измеряться показателями вовлечения и активностью пользователей в сообществе, а не лайками и количеством фолловеров. Не менее важным фактором успеха является брендовый контент, благодаря которому и интерес людей поддерживается и приумножается» ***(Пользователи стали менее***

восприимчивы к брендовому контенту // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/polzovateli_stali_menee_vospriimchivy_k_brendovomu_kontentu). – 2014. – 11.03).

***

Американский предприниматель Г. Миллингтон запустил сервис Tiltor, который предлагает услуги по устранению уличных беспорядков. Об этом сообщает издание The Daily Dot.

Tiltor называет себя посредником между «нанимателем» и «исполнителями». Нанимателем является лицо, заинтересованное в разгоне беспорядков, – например, правоохранительные органы или частные компании. В роли исполнителей выступают обычные люди, оказавшиеся в центре беспорядков.

«Наниматель», который хочет, чтобы толпа разошлась, через Tiltor предлагает денежную награду. Сервис формирует задание и через социальные сети извещает о нем «исполнителей». Если в ходе установленного срока беспорядки сошли на нет, то средства выплачиваются «исполнителям», если нет – остаются на счету «нанимателя».

Размер вознаграждения фиксирован; оно в случае успеха делится поровну между всеми «исполнителями», которые оказались в нужном географическом районе и подписались на выполнение задания. Три процента от общего размера премии, вне зависимости от исхода событий, Tiltor удерживает в свою пользу.

Какими именно способами «исполнителям» предлагается усмирять толпу, на сайте Tiltor не уточняется. Тем не менее, слоган сервиса – «Остановить беспорядки без применения насилия» – позволяет предположить, что «исполнители» должны воздействовать на участников беспорядков мирным путем.

Изначально Tiltor планировал извещать «исполнителей» о заданиях через специальное приложение. Однако создатели сервиса пришли к выводу, что такой способ небезопасен, так как позволяет легко вычислить «нанимателей» в толпе. В результате было решено рассылать уведомления через социальные сети, которые многие читают с телефона.

Сервис рекомендуется использовать для «рассеивания» беспорядков, возникших по «неидеологическим» причинам: например, после концерта или проигрыша спортивной команды. Tiltor сам выбирает партнеров: так, он отказал изданию Slon.ru, которое хотело протестировать сервис во время митинга у Посольства России в Лондоне, сочтя мероприятие «мирным» ***(Владельцам смартфонов предложили плату за усмирение беспорядков // InternetUA (http://internetua.com/vladelcam-smartfonov-predlojili-platu-za-usmirenie-besporyadkov). – 2014. – 13.03).***

***

Крупнейшая социальная сеть мира Facebook представила новый вид рекламных объявлений Premium Video Ads – видеоролики, встроенные прямо в ленту пользователя. С 14 марта он доступен некоторым американским рекламодателям, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-videoreklamu-v-lente-novostej-38776/).

Premium Video Ads представляет из себя 15-секундный видеоролик, который показывается пользователю в специальном блоке в его ленте новостей. При скролле видео начинает автоматически проигрываться без звука, при нажатии на превью можно посмотреть его целиком в полноэкранном режиме. В промо-блоке будут присутствовать несколько роликов.

Видеореклама на Facebook, по заверению представителей социальной сети, будет схожа с телевизионной. При этом для оценки аудитории, которая увидела объявление, будет использоваться аналитика третьей стороны – компании Nielsen Online Campaign Raitings (OCR), а рекламодатели будут платить только за ту аудиторию, которая им действительно нужна.

При этом Facebook совместно с компанией Ace Metrix будет оценивать креативность каждого видео ещё до публикации, пытаясь предположить потенциальную вовлечённость пользователей. Таким образом, социальная сеть действительно намерена добиться телевизионного качества публикуемой видеорекламы.

Функция Premium Video Ads будет медленно выкатываться на определённое количество людей, при этом Facebook будет активно мониторить и анализировать, как пользователи на неё реагируют.

Источники Bloomberg сообщают, что стоимость такой рекламы будет немалой: от 1 млн до 2,5 млн дол. в день. При этом каждый пользователь Facebook увидит каждое видео не более трёх раз в день, а сами объявления будут таргетироваться по возрасту и полу.

Тестирование видеорекламы Facebook начала ещё в 2013 г. Первыми её смогли попробовать верифицированные селебрити: журналисты, музыканты, актёры, но не страницы брендов. Изначально предполагалось, что, возможно, видео можно будет подгружать из Instagram ***(Facebook запускает видеорекламу в ленте новостей // Marketing Media Review (http://mmr.ua/news/id/facebook-zapuskaet-videoreklamu-v-lente-novostej-38776/). – 2014. – 14.03).***

***

Компания Socialbakers опубликовала результаты исследования рекламы в социальных сетях за 2014 г. По итогам опроса, в котором приняли участие более 500 маркетологов из 82 стран мира, выяснилось, что даже крупные компании в этом году не планируют тратить деньги на рекламу в соцсетях,

пишет Marketing Media Review (http://mmr.ua/news/id/reklama-v-socialnyh-setjah-v-2014g-38787/).

Конкуренция постов в новостной ленте Facebook растёт. Всё меньшее число пользователей видят органические посты брендов, поэтому в практике SMM становится традицией увеличение охвата с помощью рекламы. Но, видимо, многие маркетологи считают социальную рекламу напрасной тратой средств или стараются на ней сэкономить. Как показал опрос, 14 % компаний с количеством сотрудников более 5 тыс. человек не запланировали бюджет на рекламу в соцсетях.

Впрочем, даже те маркетологи, которые дают рекламу, всё ещё не до конца разбираются в её форматах и особенностях рекламных платформ. Например, многие маркетологи уверены, что объявления в новостной ленте Facebook являются наиболее эффективными, но слабо представляют различия трёх типов размещения рекламы в новостной ленте (объявления, показанные в новостной ленте на десктопных устройствах, на мобильных устройствах и десктопных и мобильных устройствах).

Ещё большая путаница у маркетологов с рекламной платформой Twitter. Специалисты не видят её привлекательности, несмотря на появление новых возможностей (расширенный таргетинг, кнопка призыва к действию и т. д.). Большинству брендов проще адаптироваться к рекламе в LinkedIn, YouTube и Facebook.

Опрос показал, что крупные компании работы по SMM предпочитают отдавать на аутсорсинг. Впрочем, когда дело доходит до продвижения постов, то многие маркетологи предпочитают заниматься созданием и размещением контента самостоятельно, а на аутсорсинг отдают управление рекламой.

В среднем, согласно результатам опроса, маркетолог ведёт 13,5 страниц компании в социальных сетях. При этом для управления рекламой большинство предпочитает использовать собственные платформы соцсетей, не прибегая к использованию специальных инструментов и приложений ***(Реклама в социальных сетях в 2014 г. // Marketing Media Review (http://mmr.ua/news/id/reklama-v-socialnyh-setjah-v-2014g-38787/). – 2014. – 14.03).***

***

Twitter придумывает всё новые и новые способы привлечь рекламодателей. Сервис микроблогов начал тестирование кнопки Click-To-Call, сообщает западное издание Digiday. Кнопка Click-To-Call будет встроена в твит и позволит любому пользователю одним нажатием на неё совершить звонок рекламодателю.

«Мы всегда были сильны в верхней части воронки продаж, достижении бренд-ориентированных целей: вовлечение, узнаваемость, фиксация событий и мгновений жизни. Реклама прямого действия подразумевает работу с нижней частью воронки и достижение целей, ориентированных на

конверсию», – прокомментировал новую функцию вице-президент по глобальным онлайн-продажам Twitter Р. Альфонси.

И действительно, до настоящего времени реклама в Twitter в основном была ориентирована на повышение узнаваемости бренда и получение большего числа подписчиков аккаунта. Кнопка Click-To-Call может мотивировать аудиторию совершить покупку.

Эксперты полагают, что новая возможность будет полезна брендам, которые занимаются прямыми продажами B2C, и в особенности локальным компаниям. Например, местные рестораны могут рекламировать таким образом спецпредложения в пределах определенного местоположения пользователей.

Пока неизвестно, какие бренды принимают участие в тестировании новой возможности, и когда она станет доступна всем рекламодателям. Предположительно, выглядеть объявление с кнопкой Click-To-Call будет также, как и реклама с кнопкой призыва к действию ***(Twitter начал тестировать кнопку Click-To-Call // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_nachal_testirovat_knopku_click_to_call). – 2014. – 14.03).***

***

Рекламная кампания Coca-Cola в социальной сети показала впечатляющие результаты, превысив показатель эффективности ROI телевизионной рекламы.

Как сообщает AdAge, главный операционный директор Facebook Ш. Сэндберг недавно заявила Wall Street Journal, что во Франции окупаемость инвестиций Coca-Cola в Facebook оказалась выше, чем ROI от ТВ-рекламы.

В I квартале 2013 г. было принято решение вернуть уже полюбившихся зрителям белых медведей в рекламную кампанию Coca-Cola. Р. Скотт создал шестиминутное видео, которое было разбито на 30-секундные рекламные ролики, показанные в прайм-тайм на телевидении. Компания также размещала дисплейную рекламу, связанную с видео, в течение трех дней на Facebook.

Результаты, сообщенные Facebook и подтвержденные подразделением Coca-Cola во Франции, выглядели действительно впечатляюще.

По информации Kantar Worldpanel, каждый евро, потраченный на Facebook, принес компании аж 2,74 евро. И это в 3,6 раз выше, чем ROI от ТВ-рекламы. В целом, 27 % дополнительных продаж Coca-Cola Kantar приписывает именно рекламной кампании в Facebook. Kantar Worldpanel опросили 10 тыс. человек из 20 тыс. своих постоянных респондентов, которые еженедельно присылают им отчеты о приобретении товаров народного потребления. Восемь тысяч из десяти оказались интернет-пользователями.

Однако Coca-Cola отнюдь не собирается перебрасывать все свои активы из телевидения в Интернет. Директор по маркетингу Coca-Cola М. Берке сообщил, что ТВ остается одним из ключевых рекламных каналов компании ***(Реклама в Facebook снова обошла ТВ-рекламу по ROI ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/reklama_v_facebook_snova_oboshla_tv_reklamu_po_roi). – 2014. – 14.02).***

***

Стартап Memeoirs предлагает пользователям Facebook распечатать книгу из своей переписки в соцсети. Итальянская типография Pozzoni уже вложила в проект свыше 300 тыс. дол. и надеется вернуть их сторицей.

Проект Memeoirs был запущен в Италии еще в 2010 г., однако ранее он предлагал исключительно создание книги на основе электронной почты в Gmail или Outlook. Сервис автоматически извлекал из ящиков переписку, в то время как пользователь выбирал дизайн книги, переплет и отсеивал ненужные письма.

Книга в мягком переплете обходится покупателю в 40 евро, за твердую обложку придется доплатить еще 20 евро. Размер книги ограничен 450 страницами, на обложке можно печатать любые изображения.

Вложенные Pozzoni средства Memeoirs направит на разработку системы, позволяющей превращать в книжную верстку диалоги из Facebook. Позже проект надеется добраться и до других соцсетей.

Стартапы по превращению соцсетевой активности в книги уже существуют. К примеру, сервис Walnuts позволяет за 10 евро создать небольшую книжку из самостоятельно выбранных высказываний на Facebook. Тем не менее, в техническом плане это куда менее сложный процесс, чем преобразование в книжную верстку переписки ***(Стартап напечатает книгу с перепиской из Facebook // InternetUA (http://internetua.com/startap-napecsataet-knigu-s-perepiskoi-iz-Facebook). – 2014. – 14.03).***

***

Заказать билет на самолет в Киеве стало возможным через Facebook и Twitter. Во всяком случае, такая возможность предоставляется тем, кто пожелает лететь самолетами голландской авиационной компании KLM. Более того, пользователи могут корректировать свой предварительный и заказ, то есть изменять свою дату вылета или номер места в салоне самолета.

Порядок заказа билетов максимально упрощен. Для этого нужно зайти на сайт самой авиакомпании и оформить запрос о наличии свободных билетов. Вход на сайт можно сделать через свой профиль в Facebook https://www.facebook.com/KLM или Twitter https://twitter.com/KLM. При наличии свободных билетов заказчик автоматически попадает на страницу оплаты стоимости перелета. После оплаты немедленно выдается подтверждение от агента KLM о покупке билета.

Благодаря такому нововведению, компания KLM стала получать порядка 35 тыс. заказов в неделю ***(Заказать билет на самолет в Киеве стало возможным через Facebook и Twitter // IT Expert (http://itexpert.org.ua/rubrikator/item/34509-zakazat-bilet-na-samolet-v-kieve-stalo-vozmozhnym-cherez-facebook-i-twitter.html). – 2014. – 17.03).***

***

Twitter изучил поведение пользователей, выяснил, что твиты с включением видео, тегов и фотографий ретвитят значительно чаще, и составил рекомендации для представителей различных профессиональных сфер.

Д. Мейсон из Twitter проанализировал более 2 млн твитов верифицированных пользователей из США, занятых в таких областях, как политика, музыка, спорт, новости и телевидение. Задачей его исследования было выяснить, действительно ли дополнительный контент положительно влияет на число ретвитов отдельных записей в микроблогах.

За отправную точку в исследовании были взяты конкретные измеримые дополнения к тексту твита: фотографии, хэштеги, ссылки, видео, цифры (например, спортивные счета или официальная статистика).

Исследование продолжалось в течение месяца, и на основании его результатов было установлено, что число ретвитов действительно значительно возрастает при включении дополнительного контента.

При этом рост числа ретвитов зависит от области, в которой действует владелец конкретного микроблога: цитаты для аккаунтов, связанных с телевидением, увеличивают число ретвитов на 53 %, а для политиков и спортсменов немалое значение имеют хэштеги.

Для каждого из пунктов был составлен гайд с удачными примерами и рекомендациями.

Например, работникам телевидения Twitter порекомендовал цитировать сериалы и шоу, публиковать «подслушанные» фразы, цитировать удачные высказывания – собственные и коллег. Полезно также выкладывать видеоанонсы грядущих выпусков и изображения, чтобы мотивировать своих подписчиков чаще делать ретвиты.

Новостникам было рекомендовано реагировать на наиболее резонансные поводы и предлагать фолловерам делиться своими фотографиями по теме.

Представители музыкальной индустрии могут давать ссылки на свежие клипы и закулисные видео и фото, а при помощи хэштегов им будет проще привлечь к обсуждению других пользователей Twitter.

Политикам и их представителям Twitter также рекомендует чаще использовать фотографии и хештеги, чтобы «помочь понять мир власти и более тесно взаимодействовать со своими избирателями». Кроме того, поддержание политической дискуссии в Twitter нуждается в точных данных и цифрах.

Спортсмены и другие люди, профессионально связанные со спортом, могут помочь болельщикам увидеть те места, в которых сами болельщики никогда бы не побывали – Twitter советует выкладывать больше фотографий с необычных ракурсов и снимков «за кадром».

Авторы исследования подчеркнули, что для выстраивания верной стратегии ведения микроблога необходим комплексный подход, а не только оптимизация отдельных постов: «Хотя меры, описанные выше, могут принести немедленную выгоду, это не конец истории. Это разница между тем, чтобы прочесть одну страницу или весь роман» ***(Twitter рассказал, как собирать больше ретвитов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_rasskazal_kak_sobirat_bolshe_retvitov). – 2014. – 17.03).***

***

Китайская социальная сеть Weibo намерена выставить свои акции на продажу на Нью-Йоркской фондовой бирже. Это позволит ей привлечь в своей развитие около 500 млн дол. США.

Социальная сеть Weibo является собственностью корпорации SINA. Как стало известно, за последние три месяца 2013 г. социальная сеть принесла прибыль в размере 3 млн дол. Стоит отметить, что уровень доходов возрос на 167 % в сравнение с аналогичным периодом 2012 г. Кроме этого, ожидается, что доход с рекламы составит около 56 млн дол.

Большинство прибыли компании приносит реклама. Можно было бы, конечно, взимать плату с пользователей социальной сети, но пока это не планируется.

Weibo является самой большой социальной сетью в мире. Помимо этого, количество пользователей постоянно растет. В настоящее время общая аудитория составляет 614 млн пользователей, данные конца декабря 2013 г. В сентябре их число составляло 589 млн. Согласно официальным данным ежемесячно социальную сеть посещает около 129 млн пользователей. Weibo есть еще куда расти. Её главный конкурент Twitter ежемесячно посещает около 241 млн пользователей.

Остается неизвестным только одно, сколько акций будет выставлено на торги на Нью-Йоркской фондовой бирже, а также их ценовой диапазон ***(Китайская социальная сеть Weibo выходит в мир // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kitayskaya_sotsialnaya_set_weibo_vyhodit_v_mir). – 2014. – 18.03).***

***

Группа Mail.ru приобрела Bullion Development Limited (Bullion), которая является собственником 11,9996 % VK.Com Limited (социальная сеть «ВКонтакте»). Об этом сообщается в пресс-релизе Mail.ru.

Таким образом, доля группы возросла почти до 52 %. «Изменений в операционном контроле над “ВКонтакте” не предполагается.

Соответственно, после завершения приобретения Mail.Ru Group не будет консолидировать “ВКонтакте” в финансовой отчетности», – отмечается в сообщении.

Владельцем Bullion является гендиректор «МегаФона» И. Таврин. Он продаст компанию за денежные средства и получит право выкупить HeadHunter у Mail.Ru в течение трех месяцев.

И. Таврин купил акции «ВКонтакте» у основателя соцсети П. Дурова в декабре 2013 г. ***(Mail.ru выкупила 12 процентов акций «ВКонтакте» у главы «МегаФона» // InternetUA (http://internetua.com/Mail-ru-vikupila-12-procentov-akcii--vkontakte--u-glavi--megafona). – 2014. – 18.03).***

***

Социальная сеть Facebook приступила к тестированию инструмента Business Manager. Новинка призвана облегчить жизнь администраторам страниц брендов, которые ведут сразу несколько проектов в крупных агентствах или являются представителями большого бизнеса

Специальная панель управления, разработанная в рамках инструмента Business Manager, предполагает возможность управлять большим количеством страниц брендов и различными коммерческими аккаунтами, используя единый интерфейс. Это в значительной степени сокращает затраты времени менеджера на администрирование коммерческих и рекламных страниц и аккаунтов.

Кроме того, возможности инструмента Business Manager позволяют администратору коммерческого аккаунта управлять правами доступа к корпоративным страницам и рекламным аккаунтам.

В настоящее время доступ к Business Manager имеет лишь ограниченное число компаний. Чтобы получить возможность оценить инструмент менеджеру крупной компании можно оставить свой e-mail на специальной странице или обратиться к торговому представителю Facebook ***(Facebook тестирует инструмент Business Manager для агентств и крупного бизнеса // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_testiruet_instrument_business_manager_dlya_agentstv_i_krupnogo_biznesa). – 2014. – 18.03).***

***

Стоит ли брендам платить за рекламу в Facebook

Н. Эллиотт, аналитик Forrester, написавший в октябре прошлого года спорный доклад, в котором порекомендовал рекламодателям «не выделять средства на платную рекламу в Facebook», нанес очередной удар, пишет Marketing Media Review (http://mmr.ua/news/id/stoit-li-brendam-platit-za-reklamu-v-facebook-38846/).

На сей раз, в посте в своем блоге он написал, что недавние изменения, проведенные в Facebook, имели целью снизить «органический охват» постов

рекламодателей – то есть количество подписчиков, которые могли видеть эти посты, – и, таким образом, платить за рекламу в социальной сети стало бессмысленно.

Есть ли какие-то сомнения в том, что Facebook ушла из социального маркетинга, и что платная реклама в этой сети больше не приносит большинству маркетологов положительные результаты?

Исследование агентства Ogilvy показывает, что брендированные страницы добиваются внимания лишь 6 % от общего числа их подписчиков. А страницы, у которых свыше полумиллиона поклонников – всего 2 %.

Проблема в том, что в новостной ленте среднего пользователя Facebook появляется около 1,5 тыс. информационных сообщений в день. Если бы эти сообщения появлялись сразу же – по мере того как ваши друзья их вывешивают, – ваша новостная лента превратилась бы в бессмысленную мусорную свалку (если вам захочется узнать, что такого вы «пропустили» в своей ленте, загляните на своем домашнем компьютере в ленту действий Facebook в правом верхнем углу). Поэтому у Facebook есть алгоритм, позволяющий показывать посты, под которыми есть комментарии или «лайки» ваших друзей. Таким образом, вы можете видеть сначала наиболее важные посты, а не последние. Это значит, что большинство людей попросту не видят большинство публикаций.

Единственный способ добиться того, чтобы ваши посты видели подписчики, это заплатить за их продвижение, т. е. попросту купить рекламу!

И, как говорит Н. Эллиотт, рекламодатели от этого приходят прямо-таки в ярость: «Бренды и агентства в открытую говорят о своем недовольстве. Каждый день я разговариваю с представителями брендов, разочаровавшихся в Facebook и сделавших ставку на другие соцсети – но лишь немногие готовы говорить об этом “под запись”. Правда, в последнее время все больше агентств и брендов рассказывают в СМИ о том, что Facebook им не по зубам. Один бывший рекламодатель сети назвал Facebook самой прибыльной разводкой всех времен».

Маркетологом, сказавшим это, был Д. Дел, глава контент-студии Gawker. Вот что он сказал Digiday: «Судя по всему, Facebook можно назвать одной из самых прибыльных разводок всех времен. Во-первых, они смогли убедить бренды платить за подписчиков и лайки, хотя все знают, что любовь не купишь. Во-вторых, Facebook продолжила обдирать те же самые бренды – но уже за то, чтобы их посты появлялись в лентах людей, чьи симпатии они только что купили».

Ладно, Gawker, на самом деле, не является одним из главных корпоративных клиентов социальной сети, как American Express, BP, Ford или IBM. И как раз поэтому студия должна больше всего переживать о Facebook, ведь Social@Ogilvy – digital-агентство, представляющее все эти крупные компании, тоже поносит Facebook. Управляющий директор агентства М. Мэнсон недавно сказал AdAge, что «Facebook все чаще говорит

о том, что мы должны смириться с мыслью, что однажды органический охват станет равен нулю».

MRY – еще одно крупное нью-йоркское агентство – тоже «катит бочку»: «Мы снизили наши ожидания в отношении партнерства и сотрудничества с Facebook. Хотя мы и привыкли к этой сети. Facebook – все равно что троечница, которая вас не подведет, но она точно не отличница, способная стать лидером класса», – сказал глава отдела распространения MRY Д. Мелтон.

Когда Facebook была еще совсем молодой компанией, рекламные агентства любили жаловаться на то, что ее сотрудники чрезвычайно высокомерны – некоторые из них даже не перезванивали своим клиентам. Появление в 2011 г. на посту вице-президента по маркетингу К. Эверсон изменило ситуацию, и у социальной сети появилась команда рекламных агентов, приносящих компании до 2,6 млрд дол. в квартал.

Большинство из этих продаж построены на технологии «прямого ответа», что означает – пока они будут предлагать дополнительные варианты, рекламодатели будут за них платить. Так что мнения различных рекламодателей не стоит принимать совсем всерьез – цифры говорят сами за себя. «Разговоры с нашими рекламодателями подтверждают, что наша реклама работает, и что они продолжат работать с нами», – сказал пресс-секретарь Facebook ***(Стоит ли брендам платить за рекламу в Facebook // Marketing Media Review (http://mmr.ua/news/id/stoit-li-brendam-platit-za-reklamu-v-facebook-38846/). – 2014. – 19.03).***

***

Вы используете социальные сети для продвижения бизнеса? Обращаете внимания на тренды в SMM? Если да, то вы наверняка знаете, что правила и тенденции в SMM постоянно меняются, пишет Marketing Media Review (http://mmr.ua/news/id/4-issledovanija-socsetej-kotorye-povlijajut-na-vashu-smm-strategiju-38903/).

Ниже приведены результаты четырёх исследований, которые могут вас не только удивить, но и заставить сменить стратегию продвижения в социальных сетях.

Пользователи используют Facebook, чтобы логиниться на других сайтах

Когда дело доходит до регистрации на сайте с помощью социальных профилей, большинство пользователей (51 %) предпочитает логиниться, используя свои данные в Facebook, показывает исследование eMarketer. 63 % мобильных пользователей по всему миру также предпочитает Facebook, чтобы залогиниться на стороннем сайте.

Почему вам полезно это знать:

– Если у вас есть сайт и вы хотите, чтобы пользователи на нём регистрировались, забудьте об использовании паролей. 92 % покупателей покидают сайт, не пытаясь восстановить забытый или утерянный пароль. Но

если на вашем сайте есть возможность авторизоваться через социальные сети, 65 % покупателей скорее всего вернутся.

– Если у вас интернет-магазин, и ваши пользователи могут войти на сайт через Facebook, вам легко узнать их интересы и предпочтения. Используйте эту информацию для персонализации. Предложите им товары, которые их заинтересуют.

– Когда пользователи заходят на сайт через социальные профили, они одновременно входят и в социальные сети. Это значит, что они могут поделиться постом или прокомментировать понравившийся продукт. Предоставляйте интересный и полезный контент каждый раз, когда пользователи логинятся на вашем сайте.

Клиенты идут в Twitter за социальной поддержкой

Когда клиенты хотят пожаловаться или задать вопрос бренду, они идут в Twitter. Исследование Socialbakers показало, что 59,3 % вопросов брендам пользователи задают в Twitter (для сравнения, в Facebook – 40,7 %).

Почему вам полезно это знать:

Пользователи ждут от брендов в социальных сетях быстрой обратной связи. Неоправданные ожидания могут стоить компании клиентов или репутации.

Вот несколько советов, что вы можете сделать для поддержки клиентов в Twitter:

– Обучайте своих сотрудников и расширяйте их полномочия, чтобы они могли оперативно отвечать клиентам. Если вы боитесь, что они не смогут адекватно ответить от имени компании, то у вас либо неправильная команда, либо неправильная стратегия.

– Придерживайтесь правила: максимальное время ответа на жалобу или вопрос – один час. Если вы тянете слишком долго, клиент (потенциальный клиент) может уйти к другому продавцу.

– Если вы отвечаете от имени бренда, попытайтесь персонализировать каждый ответ, подписав твит своим именем или связав с Twitter-аккаунтом.

– Мониторьте упоминания бренда. Оценивайте тональность каждого упоминания. Твиты, которые включают слова «не работает», «ужасный», «неприятный опыт», должны быть обработаны немедленно до полного удовлетворения клиентов.

– Не влезайте в чужой разговор. Иногда клиенты просто говорят о вашем бренде и не нуждаются в помощи.

– Расставьте приоритеты. Кому вы будете отвечать в первую очередь: пользователям, у которых много подписчиков, или тем, у кого срочная проблема? А, может быть, вы будете использовать принцип «кто пришел первым, того первым и обслужат»?

Молодой аудитории нравится Facebook

Знаем, знаем. Было много обсуждений, что подростки не любят Facebook. Но это не совсем так.

Молодая аудитория действительно предпочитает более визуальные платформы, например, Instagram и Vine. Однако она не спешит выбрасывать и Facebook на помойку времени. Данная статистика eMarketer говорит сама за себя:

Почему вам полезно это знать:

Молодая аудитория (впрочем, как и все мы) пользуется сразу несколькими социальными сетями.

Например, подростки особенно активно любят делиться изображениями и видео. Они могут делать это в Facebook, но предпочитают Instagram, где не присутствуют родители и нет серьезных разговоров.

Если ваша целевая аудитория включает подростков, не паникуйте. Попробуйте следовать таким советам:

– Используйте больше социальных сетей. Если подростки важны для вашего бизнеса, следуйте за ними туда, где они обитают. Создавайте и распространяйте контент на разных платформах. Ваш контент будет лучше запоминаться, когда аудитория увидит его в Facebook, Instagram и т. д.

– Помните о релевантности. Подростки эгоцентричны, их интересуют мнения, которые схожи с их собственными и мнением их друзей. Вовлекайте их историями и визуальными элементами, которые показывают, как другие подростки вроде них взаимодействуют с вашим брендом.

– Убедитесь, что весь ваш контент удобно просматривать с мобильных устройств.

Instagram – самая быстрорастущая соцсеть в мире

Instagram – платформа, за которой нужно внимательно следить, согласно исследованию, опубликованному TechCrunch в январе.

За последние шесть месяцев 2013 г. число активных пользователей соцсети возросло на 26 %. В январе 2013 г. у Instagram было 90 млн активных пользователей. К январю 2014 г. это число удвоилось до 180 млн.

Почему вам полезно это знать:

Пользователи любят Instagram, потому что им интересны изображения и возможности редактирования фото с помощью фильтров. Кроме того, им нравится возможность мгновенно поделиться фотографией с сообществом единомышленников.

Вот несколько советов, как использовать Instagram для продвижения бренда:

– Сделайте ваших фолловеров известными, давая награды за фото и делясь изображениями с подписчиками. Например, Starbucks даже выкладывает фото своих фанов с Instagram в Facebook.

– Создавайте видео. Оно гораздо лучше передаст настроение и образ жизни вашего бренда. Чем статичное изображение. Например, если вы запускаете новый продукт, сделайте видео ваших сотрудников, которые готовятся к запуску или покажите сам запуск.

– Сотрудничайте с другими брендами в Instagram. Независимо от того, крупный вы бренд или мелкий, вы можете установить партнерство с другими

компаниями, размещая фото друг друга. Это сработает еще лучше, если ваши продукты дополняют друг друга.

– Задавайте вопросы. Например, если вы продаете обувь, спросите подписчиков, какую одежду и аксессуары они бы надели с новой коллекцией ***(4 исследования соцсетей, которые повлияют на вашу smm-стратегию // Marketing Media Review (http://mmr.ua/news/id/4-issledovanija-socsetej-kotorye-povlijajut-na-vashu-smm-strategiju-38903/). – 2014. – 21.03).***

***

Сбылась еще одна маленькая мечта SMM-щиков. Facebook пошел навстречу брендам и запустил новую функцию – возможность добавлять кнопку призыва к действию к объявлениям и постам.

Известно, что пользователи гораздо активнее взаимодействуют с брендом, когда их побуждают совершать конкретные действия. Поэтому возможность добавлять призывы к действию в рамках постов и рекламных объявлений Facebook все ждали давно. Наконец, дождались! Брендам стали доступны следующие виды CTA-кнопок:

Начать покупку (Shop Now)
Подробнее (Learn More)
Регистрация (Sign up)
Зарезервировать (Book Now)
Загрузить (Download)

Ниже представлена подробная инструкция, как создавать кнопки призыва к действию в Facebook для постов и объявлений.

Как создать CTA-кнопку для рекламного объявления

Чтобы создать кнопку с призывом к действию для объявления, вам придется использовать Power Editor. В настоящее время добавить кнопку можно только для ссылок при создании неопубликованной публикации (для фото, видео, статусов такая возможность пока недоступна).

Зайдите на страницу бренда в Power Editor, выберите пост, который хотите рекламировать. Задайте цель «Клики на веб-сайт». Ниже выберите «Создайте новую неразмещенную публикацию».

Появится окно, куда вам необходимо будет ввести ссылку на рекламируемый пост. Там же вы сможете выбрать подходящую для продвижения кнопку призыва к действию.

Миниатюру изображения, название и описание ссылки можно добавить самим. Если вы этого не сделаете, Facebook автоматически подтянет необходимые данные из поста.

Обратите внимание, что по умолчанию для всех ссылок при создании публикации стоит «Кнопка не выбрана». Также стоит иметь в виду, что кнопка призыва к действию будет появляться только в объявлениях, размещаемых в Ленте новостей, а не на боковой панели.

Как создать CTA-кнопку для органического поста

Добавлять кнопки призыва к действию можно не только к объявлениям. Используя Power Editor вы точно также можете сделать CTA-кнопку для органического поста.

Алгоритм действий таков. Для начала выберите в верхнем выпадающем меню «Управление Страницами». Затем выберите Страницу, для которой хотите создать пост с CTA-кнопкой. Далее нажмите кнопку «Создать публикацию».

Появится диалоговое окно идентичное тому, что вы видели, когда создавали рекламное объявление с CTA-кнопкой.

Когда закончите заполнять поля, кликните на «Создать публикацию». Щелкнув на строчке с неопубликованным постом, вам будет доступен предварительный просмотр.

Нажмите на кнопку «Разместить публикацию» в верхнем меню.

Теперь осталось только нажать на «Изменения загрузки» на верхней панели, чтобы пост с кнопкой призыва к действию появился на Странице.

Если даже после нашей подробной инструкции у вас остались вопросы, предлагаем посмотреть видео А. Зюзикова, где он наглядно показывает весь алгоритм действий при создании публикации с CTA-кнопкой ***(Как создать кнопку призыва к действию в Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kak_sozdat_knopku_prizyva_k_deystviyu_v_facebook2). – 2014. – 20.03).***

***

В LinkedIn намерены активнее заняться удержанием персонала и вопросами найма новых сотрудников для компаний. Д. Шаперо, глава группы LinkedIn’s Talent Solutions, наиболее прибыльного подразделения, говорит об удержании и найме сотрудников как наиболее прибыльной сфере деятельности социальной сети – за прошлый квартал выручка составила 245 млн дол.

Согласно недавнему исследованию LinkedIn, основной мотив перехода к другим работодателям соискателей – зарплата повыше и различные бонусы. А у тех, кто уже перешел и работает у нового работодателя, – невозможность профессионального роста на старом рабочем месте.

В США, к примеру, в результате исследования выяснилось, что нанятым новым сотрудникам платят существенно больше, ожидают меньше, и такие люди чаще увольняются, чем кандидаты, которые получили повышение на новую должность внутри компании.

Большим преимуществом для компаний станет использование огромной базы данных соискателей и собственных сотрудников с навыками и умениями, которая уже есть у LinkedIn. Так можно мобилизовать внутренние ресурсы компаний, продвигать на должности тех, кто уже работает в компании, и тем самым снижать риск потери кадров, привлеченных извне (равно как снизить затраты на новых, «внешних» сотрудников).

Именно в этом ключе намерена работать соцсеть в 2014 г. ***(LinkedIn заработала $245 млн на удержании и найме сотрудников компаний // «Цукерберг Позвонит» (http://www.siliconrus.com/2014/03/linkedin/). – 2014. – 20.03).***

***

Социальная сеть «Одноклассники» начала регулярное сотрудничество с компанией-правообладателем музыкального контента «Юнайтед Мьюзик Групп», сообщает пресс-служба Mail.Ru Group.

«Юнайтед Мьюзик Групп» объединяет компании «Квадро-Диск», «Никитин МДС», «Классик-Компани» и управляет правами таких популярных артистов как Л. Агутин, А. Варум, Г. Лепс и многих других.

Лицензионная музыка, в первую очередь, будет использовать в музыкальном сервисе соцсети – «Музыкальные подарки», который был запущен в конце прошлого года. Теперь любой пользователь социальной сети сможет прикрепить понравившуюся аудиозапись к подарку, который хочет отправить своему собеседнику.

По словам директора по маркетингу и развитию бизнеса социальной сети «Одноклассники» А. Исрапилова, музыкальные подарки – отличная возможность монетизации аудиоконтента для всех правообладателей, заинтересованных в сотрудничестве с соцсетью. Он также отметил, что в ближайшее время будет существенно расширен каталог музыкальных композиций, доступных пользователям для прослушивания, загрузки и дарения.

В декабре прошлого года социальная сеть «Одноклассники» подписала партнерское соглашение с музыкальным лейблом Warner Music. По условиям контракта Warner Music получает денежные отчисления от использования принадлежащих ей фонограмм в музыкальных подарках, которые отправляют друг другу пользователи соцсети ***(«Одноклассники» лицензировали музыкальный контент // Sostav.ru (http://www.sostav.ru/publication/odnoklassniki-litsenzirovali-muzykalnyj-kontent-8963.html). – 2014. – 19.03).***

***

Стикеры – крупный и красочный аналог смайликов – придут и в социальную сеть «ВКонтакте». Эти весёлые картинки, которыми можно разнообразить беседу, уже давно прижились в крупных заграничных социальных сервисах – Facebook, Path, Line, Viber и т. п. Во многих случаях они даже составляют львиную долю прибыли проекта.

В сентябре 2013 г. намёки на появление стикеров делал основатель сети П. Дуров – соответствующие изображения появились на анонсе обновлённого приложения для iOS.

Теперь это почти стало явью – несколько дней назад в сеть утек полный или почти полный набор стикеров «ВКонтакте».

Ими можно будет обмениваться в приватных и общих чатах. Для начала пользователи получат четыре набора по 24, 32 или 48 штук – бесплатные и платные (по 66 р.). Покупать их можно за рубли (через in-app в приложениях) или за голоса (через веб-версию). По информации источников РБК Daily во «ВКонтакте», новинка может прийтись по вкусу как минимум 10 % пользователей, соответственно, компания имеет возможность заработать на этом 3,2 млрд р.

Пресс-секретарь «ВКонтакте» Г. Лобушкин уточняет, что запуск нового сервиса состоится в ближайшее время, впоследствии его включат и в мобильные приложения (сперва для Android, затем – для iOS). Кроме того, для сторонних художников откроется специальная платформа, при помощи которой они смогут предлагать собственный дизайн стикеров. Потом специальное жюри будет отбирать лучшие варианты, а победители получат ценный приз.

Исполнительный директор «ВКонтакте» Д. Сергеев в комментарии для РБК уточняет, что аудитория пользователей стикеров может сравняться с аудиторией пользователей сервиса «Подарки», который в настоящее время составляет немалую долю прибыли компании. Он же заявил, что в 2014 г. соцсеть будет акцентировать внимание на мобильном трафике – сперва будет запущена мобильная игровая платформа, а затем мобильная реклама ***(«ВКонтакте» запустила платные стикеры в сообщениях и планирует заработать на них 3,2 млрд // «Цукерберг Позвонит» (http://www.siliconrus.com/2014/03/sticker/). – 2014. – 18.03).***

***

Глобальный рынок интернет-рекламы возрос по итогам 2013 г. на 105 %, до 17,96 млрд дол., стимулируемый успешными продажами в этом секторе со стороны компаний Google и Facebook, свидетельствуют данные аналитической компании eMarketer. Об этом сообщает digit.ru

По данным аналитиков, в 2012 г. объем рынка оценивался в 8,76 млрд дол., тогда как по итогам прошлого года более чем удвоился. В 2014 г. он может добиться 31,45 млрд дол. – на 75 % больше, чем годом ранее – и составить почти четверть всего рынка digital-рекламы, а к 2018 г. достичь отметки в 94,9 млрд дол., прогнозируют в eMarketer. Однако темпы роста рынка будут неизбежно снижаться — с почти 120 % в 2012 г. до 22 % в 2018 г.

По итогам прошлого года лидером мирового рынка мобильной рекламы остается Google, однако ее доля в совокупной выручке снизилась с 52,6 % до 49,3 %. Доля соцсети Facebook, напротив, возросла с 5,4 % в 2012 г. до 17,5 %. В совокупности компании контролируют более двух третей всего рынка мобильной рекламы.

В нынешнем году тенденция продолжится, говорят в eMarketer. Так, доля Google в совокупной выручке рынка может упасть до 46,8 %, а показатель Facebook – возрасти до 21,7 %. В собственной выручке Facebook

мобильная реклама сгенерирует 63,4 % в 2014 г., а в доходах Google — 33,8 %, оба показателя превысят значения прошлого года.

В тройку лидеров по итогам 2013 г. также вошел сервис микроблогов Twitter, на долю которого в 2013 г. пришлось 2,4 % доходов рынка. Как сообщал Digit.ru, по итогам IV квартала на долю мобильной рекламы пришлось 75 % выручки Twitter. Однако сервису, который в ноябре 2013 г. провел первичное публичное размещение акций на бирже, необходимо активнее наращивать выручку, чтобы поддерживать котировки ***(Рынок мобильной рекламы удвоился в 2013 году за счет Google и Facebook // Media бізнес (http://www.mediabusiness.com.ua/content/view/38730/126/lang,ru/). – 2014. – 20.03).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Американские исследователи изучали воздействие социальных сетей на психику в течение трех лет и обнаружили, что положительные «посты» очень быстро распространяются по всему Интернету. Они проанализировали более миллиарда обновлений статуса Facebook у более чем 100 млн пользователей. Результат однозначен: весёлые и лёгкие сообщения вызывают цепную реакцию и генерируют подобные сообщения у друзей, пишет menshealth.

Эксперты пришли к выводу, что сообщения позитивного характера распространяются по сети быстрее и чаще, чем негативные.

«Наше исследование показало, что твой статус в соцсети может иметь сильное влияние на настроение и эмоциональное состояние твоих друзей», – заявил глава исследовательской группы Д. Фаулер, профессор политологии в Университете Калифорнии ***(После кропотливого исследования ученые выяснили: веселые посты быстрее сделают вас популярным в соцсетях // IT Expert (http://itexpert.org.ua/rubrikator/item/34510-posle-kropotlivogo-issledovaniya-uchenye-vyyasnili-veselye-posty-bystree-sdelayut-vas-populyarnym-v-sotssetyakh.html). – 2014. – 17.03).***

Маніпулятивні технології

Война за Крым в сети: россияне нанимают антиукраинских троллей за деньги

Пока в Крыму наши военные стараются не реагировать на все провокации россиян, силы, заинтересованные в дестабилизации обстановки в Украине, ведут информационную войну в Интернете. «Сегодня» выяснила, кто эти провокаторы на форумах и сколько они получают за разжигание вражды (http://www.segodnya.ua/regions/odessa/voyna-za-krym-v-seti-rossiyane-nanimayut-antiukrainskih-trolley-za-dengi-501526.html).

Такая пропаганда углубляет уже существующий раскол в украинском обществе, полагает психолог А. Сагайдак. «Последствия этого мы будем ощущать еще не один год. В такие критические, переломные моменты на поверхность всплывает все то темное и черное, что есть в каждом народе, выплескиваются наружу все годами копившиеся злоба, обиды и зависть. Это – то коллективное сознание, которое движет толпой, и заставляет человека в ней не боятся пуль. Но особенно страшно, когда настроения нарочно подогреваются извне», – говорит А. Сагайдак.

В социальных сетях активно набирают рядовых бойцов в киберармии – вербовщики работают днем и ночью. В желающих поработать так называемым троллем, провоцируя конфликт едкими комментариями, отбоя нет. Но людей все равно не хватает – все оттого, что виртуальная «смертность» среди этого контингента большая. Редкий тролль «на вражеской» территории живет больше суток. Подавляющее большинство сразу вычисляют и банят, то есть запрещают доступ к сайту, рассказывает администратор ресурса. «К тому же в подарок обязательно вышлют вирус или троянскую программу, с помощью которой либо уничтожат его компьютер, либо присоединят его к ботнету. После этого компьютером будет дистанционно управлять другой человек», – говорит веб-инженер Е. Морозов.

На провокационных комментариях предлагают неплохо заработать. В социальных сетях города полно объявлений: хочешь помочь сопротивлению – обращайся по таким-то адресам. Мы обратились по одному из них. Номер оказался российским. Молодой человек представился Виталием. «Если умеешь писать так, чтобы с юмором и цепляло – напиши пару примеров на одобрение. Если нет – скажу, где можно взять шаблоны. Твоя задача – бить неприятеля на их же информационном поле. Перечень ресурсов в твоей зоне ответственности вышлю отдельно. С людьми из твоей команды, твоими “коллегами”, которые поддерживают общий настрой и создают необходимое общественное мнение, познакомишься сам. За сотню твоих опубликованных комментариев гарантированно получаешь 10 дол. Согласись, деньги хорошие», – обещает голос в трубке с характерным московским аканьем. Саму оплату этих услуг Виталий называет «благодарностью». Говорит, речь о ней может идти только после первой сотни комментариев.

По другую сторону информационного фронта тоже набирают в свои ряды троллей, но денег не предлагают. «Вам не стыдно о таком спрашивать? Речь идет о существовании на политической карте Украины, наших с вами

домов и городов. Здесь каждый помогает, как может», – говорит вербовщик Михаил.

Однако за идею работают далеко не все. Поругаться на форумах согласятся многие, а вот вычислять наиболее активных оппонентов и публиковать их личные данные в сетях, что само по себе является нарушением закона Украины, люди соглашаются только за определенную плату. «Большинство причастных к разжиганию межнациональной розни и призывающих к насилию людей пользуются так называемыми прокси-серверами. Это затрудняет определение их реального местонахождения. Люди, пишущие якобы от имени жителей Одессы или Крыма, на самом деле находятся на территории Московской и Ленинградской областей», – поясняет наш собеседник в правоохранительных органах.

Дезинформация. Тем временем на дезинформацию денег не жалеют: сотрудникам уважаемых изданий предлагают «сотрудничать» – мол, мы вам даем эксклюзив почти безвозмездно. В итоге «эксклюзив» оказывается выдумкой. Ставка – на то, что по соседству с правдивым материалом дезинформация будет дискредитировать весь информационный продукт, говорят правоохранители. За такое сотрудничество денег не жалеют.

Кроме того, особо востребованы хакеры, которые умеют взламывать чужие интернет-ресурсы и умеющие этому противостоять. С их помощью составляется база данных «потенциально опасных» людей. По словам А. Давидченко, такие списки составляют бандеровцы, «чтобы уничтожить патриотов России». В противоположном лагере уверяют в обратном: перечни делают люди А. Давидченко, туда вносят тех, «с кем нужно будет разобраться, когда появится поддержка российских военных» ***(Жуков А. Война за Крым в сети: россияне нанимают антиукраинских троллей за деньги // Сегодня (http://www.segodnya.ua/regions/odessa/voyna-za-krym-v-seti-rossiyane-nanimayut-antiukrainskih-trolley-za-dengi-501526.html). – 2014. – 11.03).***

***

Как победить Путина в информационной войне

Когда я в последнее время слышу слова на BBC или ITN «передают русские новости», я не могу не поморщиться.

За последние 10 дней российские новости сообщили о том, что около 675 тыс. украинских беженцев пересекли границу с Россией, что экстремисты и неонацисты незаконно захватили украинское правительство в Киеве, и что крымские «войска самообороны» или «пророссийские войска» спонтанно собрались перед крымским парламентом, чтобы защитить его от нацистов.

Каждое из этих утверждений – ложь. Российские войска не прибыли, чтобы защитить русскоязычное население, они здесь, чтобы создать истерию, чтобы дискредитировать правительство в Киеве, и убедить другие страны,

что оккупация Крыма является законной, и возможно и грядущая оккупация восточной Украины или других частей Украины.

В этом последнем старании, они, возможно, добились успеха. Ведь, традиция в этой стране – предоставить другой стороне возможность беспристрастного выбора, поэтому эта ложь в русских новостях используется для создания чувства равновесия среди британских программ, тоже. Иногда члены российских медиа приглашаются в студию. Их взгляды слегка противоречат взглядам британских репортеров, но они кажутся такими уверенными в том, что говорят, конечно, они должны быть зерном истины? Не должна ли реальная история находиться где-то посредине? Не высказывают ли они просто «российскую точку зрения»?

Конечно, целью российской информационной войны являются не британцы. Политические технологии, как их называют сейчас в Москве, заботятся о россиянах и тех, кто говорит на русском языке. Но хотя Кремль, возможно, не может диктовать то, как история преподносится на британском или европейском телевидении, он может помогать ее формировать.

Влияние ощутимо. Например, новости о «сепаратистах» заставили серьезных британских ученых подумать, не имеет ли Россия права выразить свое мнение в отношении Крыма. Россия, в конце концов, завоевала Крым в конце XVIII в., и там живет много русскоязычного населения. Ничто не мешает сказать с позиции той же логики, что у Британии есть право на Индию, страну, которую она завевала в XVIII в., и где есть много англоязычных жителей. О чем молчат российские медиа и ее представители на британском телевидении, это то, что законные права России на морскую базу в Севастополе не находятся под угрозой и никогда не были.

Я признаюсь, грубая и назойливая природа пропаганды, которая в настоящее время транслируется на российских медиа и особенно на Russia Today, международном новостном канале, владельцем которого является российское правительство, удивила меня. До этого времени тон скорее был фальшивым и циничным, а не агрессивным. Но теперь он открыто присоединился к информационной войне, которая проводится в невиданном размахе. Неприкрытая ложь стала повсеместной – RT недавно показал Крым как Россию на электронных картах.

К сожалению, единственным ответом на информационную войну является всеохватывающая информационная защита. У Запада это хорошо получалось: самому быть надежным источником правды. Языковые службы Radio Free Europe и BBC предоставляли эффективные инструменты в борьбе против коммунизма. Может, пришло время взять с них пример.

Но политики и дипломаты также должны стать креативнее. Несколько дней назад Министерство иностранных дел в США опубликовало заявление: «Фантазия президента Путина: 10 фальшивых заявлений об Украине». Через несколько часов российское министерство иностранных дел осудило список, назвав его «шокирующим, ни столько за его примитивное искажение реальности, как за его цинизм и неприкрытые двойные стандарты». Другими

словами, заявление достигло своей цели. Я надеюсь, их будет больше ***(Э. Аппельбаум, telegraph.co.uk: Как победить Путина в информационной войне // Marketing Media Review (http://mmr.ua/news/id/kak-pobedit-putina-v-informacionnoj-vojne-38708/). – 2014. – 11.03).***

***

Сервис YouTube заблокировал основной англоязычный аккаунт российского телеканала Russia Today. На странице телеканала сообщается, что она заблокирована «в связи с многочисленными и серьезными нарушениями правил YouTube (обман, распространения спама, недопустимое содержание и видео).

Русскоязычный аккаунт RT продолжает функционировать ***(YouTube за обман заблокировал Russia Today // UAINFO (http://uainfo.org/yandex/294278-youtube-za-obman-zablokiroval-russia-today.html). – 2014. – 18.03).***

***

Манипулирование общественным мнением, основанное на тезисах об ущемлении прав русских в Украине, обеспечило негативную мобилизацию большей части российского общества, реанимировав его спящие имперские комплексы. Об этом, как передаёт корреспондент РИА «Новый Регион», говорится в комментарии эксперта «Левада-Центра» Л. Гудкова к результатам опроса о ситуации в Украине и Крыму.

По данным социологов, эскалация напряженности в Украине, вызванная использованием российских военнослужащих в Крыму и экспансионистскими заявлениями российского руководства, заметно встревожила российское общество. Возможностью вооруженного конфликта между Россией и Украиной обеспокоены 83 % населения.

Между тем двухнедельная, беспрецедентная за все постсоветское время, кампания пропаганды и дезинформации дала мощный эффект и массовое одобрение политики президента России В. Путина в отношении Украины, считает эксперт. Он подчёркивает, что все альтернативные, отличающие от официоза или независимые источники информации и интерпретации событий были полностью отключены. Несмотря на то что 70 % опрошенных признаются в том, что не разбираются в сути процессов в Украине, большинство (63 %) считают, что «федеральные российские СМИ в целом или по большей части объективно освещают события, происходящие в Украине или в Крыму».

«Эта тактика манипулирования общественным мнением, построенная на нескольких простых тезисах и приемах: “ущемление прав русского и русскоязычного населения, угроза их благополучию и жизни”; дискредитация сторонников Евромайдана и интеграции Украины с Евросоюзом (навешивания на них ярлыков бандитов, нацистов, бандеровцев); “состояние хаоса и безвластия в Украине” после прихода к

власти противников В. Януковича и т. п., – обеспечила негативную мобилизацию большей части российского общества, реанимировав его спящие имперские комплексы», – подчёркивает эксперт ***(Лучистая А. «Левада-Центр»: Кремль реанимировал имперские комплексы // Новый Регион (http://www.nr2.ru/moskow/488872.html). – 2014. – 13.03).***

Зарубіжні спецслужби і технології «соціального контролю»

АНБ маскировалось под поддельный сервер Facebook, заражало компьютер своего объекта и получало данные с его жесткого диска, передает «Зеркало недели».

Агентство национальной безопасности США (АНБ) устанавливало вирусы на компьютеры пользователей с помощью социальной сети Facebook.

Разведывательное ведомство получало доступ к компьютерам, отправляя на них зараженные пакеты данных. Делалось это после того, как пользователь вводил на главной странице соцсети свой логин и пароль.

Судя по секретным материалам АНБ, опубликованным The Intercept, программа по слежке через Facebook называлась QUANTUMHAND и была запущена спецслужбой еще в 2010 г. Действует ли этот метод сбора данных до настоящего времени, не известно.

Представители Facebook заявили, что не знают о действиях спецслужб. «В любом случае, метод, который описывается в публикации The Intercept, больше не действует. Facebook теперь использует протокол HTTPS, который защищен от подобного перехвата информации», – заявили в Facebook ***(АНБ через Facebook заражало компьютеры пользователей // Новости Донбасса (http://novosti.dn.ua/details/220107/). – 2014. – 12.03).***

***

При помощи операции под названием Turbine, Агентство национальной безопасности США создавало автоматизированные системы для массового взлома «миллионов» компьютеров. Об этом 13 марта сообщило издание The Intercept со ссылкой на документы, полученные от Э. Сноудена. Напомним, что издание The Intercept было создано на деньги миллиардера и создателя Ebay П. Омидьяра. Главным редактором The Intercept является Г. Гринвальд, экс-журналист The Guardian, который первым опубликовал сведения о шпионских программах АНБ год назад.

Согласно сегодняшней публикации в The Intercept, операция Turbine имела своей целью создание «имплантов», которые открывали ведомству доступ к пользовательским компьютерам. Через специально созданное вредоносное ПО работники АНБ создавали поддельные страницы в соцсетях от лица пользователей, проводили атаки типа man-in-the-middle и выполняли другие действия. Также агенты АНБ занимались сбором информации с пользовательских компьютеров по всему миру, говорится в публикации.

Э. Сноуден сообщает, что рост использования защищенных каналов связи в последние пару лет стал создавать для ведомства проблемы с доступом к данным. Чтобы как-то решить ее, было принято решение о краже данных еще до того, как они будут зашифрованы – то есть еще на компьютере пользователя.

Один из таких «имплантов» – это программа CaptivatedAudience, которая использовалась для подключения к микрофону компьютера и записи данных с него. Другая – GymFish, использовалась для контроля за веб-камерой. Программа FoggyBottom записывала логи браузеров, собирала данные о логинах и паролях, чтобы впоследствии АНБ могло получать доступ к профилям пользователей. А программа SalvageRabbit применялась для получения данных со съемных носителей, в частности с USB-накопителей.

Хотя изначально эта система была создана для работы в крупных масштабах, так как была в значительной степени автоматизирована и не требовала постоянного контроля оператора, неясно, как далеко зашла американская разведка в получении данных граждан. Впрочем, уже очевидно то, что эта программа никак не вписывается в заявления главы АНБ К. Александра о «выборочном» и «целевом» наблюдении ***(Обнародована еще одна шпионская программа АНБ США – Turbine // InternetUA (http://internetua.com/obnarodovana-esxe-odna-shpionskaya-programma-anb-ssha---Turbine). – 2014. – 13.03).***

***

В Днепропетровске сотрудники Службы безопасности Украины задержали троих пользователей соцсетей, которые выступали за отделение юго-восточных областей от Украины, пишет Сегодня (http://www.segodnya.ua/regions/dnepr/v-dnepropetrovske-zaderzhali-gruppu-separatistov-503622.html).

Как сообщили Сегодня.ua в пресс-службе Управления СБУ в Днепропетровской области, начато досудебное расследование по признакам посягательства на территориальную целостность и неприкосновенность Украины.

«Группа лиц через социальные сети публично призывала к изменению территориального устройства Украины в нарушение порядка, установленного Конституцией Украины», – сказано в сообщении.

Трое активистов – жителей Днепропетровска, состоят в одной из радикальных организаций. Они позиционирует свою деятельность как «освободительное движение юго-восточных регионов Украины».

Сотрудники СБУ провели обыски. Правоохранители изъяли компьютерную технику и агитационно-пропагандистские материалы деструктивного характера. Открыто уголовное производство ***(Никитин А. В Днепропетровске задержали группу сепаратистов // Сегодня (http://www.segodnya.ua/regions/dnepr/v-dnepropetrovske-zaderzhali-gruppu-separatistov-503622.html). – 2014. – 19.03).***

***

У Саудівській Аравії двох чоловіків засудили до 10 і 8 років позбавлення волі за поширення у Twitter закликів до протестів та підривання авторитету чинної влади. Про це повідомляє CNN із посиланням на місцеве державне новинне агентство SPA.

Одного з чоловіків, який раніше вже відбував покарання за «політичною статтею», засудили до 10 років за розсилання запрошень до участі в акціях протесту проти монархії. Іншому винесли вирок про вісім років позбавлення волі за образу короля Саудівської Аравії Абдулли. Йому, крім цього, заборонили впродовж ще восьми років після відбуття покарання користуватися соціальними мережами та покидати країну.

Імена засуджених не розголошуються.

Саудівську Аравію останнім часом сильно критикують правозахисники за тиск щодо громадських активістів.

У лютневому звіті А. Кугла, експерта Human Rights Watch, ідеться про те, що нове антитерористичне законодавство Саудівської Аравії «створює видимість законності безперервних утисків прав людини з боку кримінального правосуддя».

За словами правозахисника, новий закон є «незрозумілим узагальнюючим документом, що може бути використаний для переслідування чи ув'язнення будь-кого, хто критикує саудівський уряд».

На початку лютого MediaSapiens повідомляв, що в Саудівській Аравії до 12 років засудили журналіста В. аль-Газзаві за «непокору правителю» та звинувачення країни в тероризмі ***(У Саудівській Аравії двох чоловіків засудили до позбавлення волі за пости у Twitter // «Телекритика» (http://osvita.mediasapiens.ua/material/28490). – 2014. – 11.03).***

***

29-летнему жителю Днепродзержинска, пользователю соцсети «ВКонтакте», грозит до 10 лет лишения свободы. На его странице в vk.com, местные правоохранители обнаружили несколько видеороликов с детской порнографией.

Об этом сообщил «Вестям» начальник сектора по борьбе с преступлениями, связанными с торговлей людьми, Днепродзержинской милиции Д. Воронин.

«У него на странице мы нашли несколько видеороликов с признаками детской порнографии. Он размещал их на протяжении нескольких лет. На одном из последних роликов согласно заключению судебно-медицинской экспертизы, девочка, присутствующая в сценах видеоролика, не достигла половой зрелости. На вид ей 12–13 лет. Пока подозреваемый не говорит, где взял эти видеоролики», – рассказывает Д. Воронин.

Подозреваемому сообщили о подозрении в совершении преступления, предусмотренного статьей «Ввоз, изготовление, сбыт и распространение

порнографических предметов». Санкция статьи предусматривает наказание в виде лишения свободы сроком от 5 до 10 лет ***(Днепродзержинскому пользователю «ВКонтакте» грозит до 10 лет тюрьмы // InternetUA (http://internetua.com/dneprodzerjinskomu-polzovatelua--vkontakte--grozit-do-10-let-tuarmi). – 2014. – 15.03).***

***

Компания mSpy приступила к продажам популярных моделей смартфонов, на которых изначально установлено и скрыто от владельца «шпионское» ПО. Целевая аудитория таких устройств – работодатели, которые хотят следить за своими сотрудниками, родители, которым нужно знать, где находится и с кем общается их ребенок, а также супружеские пары. Свой продукт разработчик рекламирует под слоганом «они не узнают».

«Шпионская» начинка mSpy способна отслеживать практически любую активность на смартфоне: историю звонков и посещенных сайтов в Интернете, переписку по электронной почте, в WhatsApp, iMessage, Viber, Skype и других мессенджерах, сделанные на камеру фото и видео. Также она узнает о событиях в календаре, записывает звук и нажатия клавиш, подслушивает окружающую обстановку через микрофон, определяет местоположение по GPS.

Вся эта информация отправляется на серверы вне ведома пользователя. Заказчик смартфона-шпиона может получить к ней доступ из личного кабинета на сайте mSpy. Там же он может дистанционно заблокировать устройство и удалить все его содержимое.

Основатель mSpy – 27-летний уроженец Белоруссии А. Шиманович, который недавно переехал в Нью-Йорк. Его компания предустанавливает «шпионское» ПО на современные модели, включая HTC One, Nexus 5, Samsung Galaxy S4 и iPhone 5S. К примеру, за Galaxy S4 покупателю придется заплатить 300 дол. за сам смартфон и еще 199 дол. за годовую подписку ***(mSpy начала продавать смартфоны-шпионы // InternetUA (http://internetua.com/mSpy-nacsala-prodavat-smartfoni-shpioni). – 2014. – 15.03).***

***

Корпорация IBM стала последним и одним из крупнейших ИТ-игроков, отрицающих свое сотрудничество с американским разведывательным ведомством АНБ в рамках его нашумевшей программы PRISM. В открытом письме клиентам и пользователям продуктов IBM генеральный юрисконсульт компании Р. Вебер заявил, что АНБ не запрашивало у IBM прямого доступа к данным клиентов и корпорация его не предоставляла.

Р. Вебер отметил, что IBM не предоставляла клиентских данных ни в АНБ, ни в какое-либо иное разведывательное ведомство в рамках программы PRISM. Также он заметил, что компания не предоставляла так называемых

метаданных и не разглашала данных клиентов за пределами США по распоряжениям FISA или так называемых National Security Letters.

В письме говорится, что в корпорацию также никто из правительства США не обращался на предмет встраивания шпионского софта или бэкдоров в оборудование и программное обеспечение. При этом в IBM признали, что в принципе разглашали данные о клиентах, но делали это адресно и по решению суда. Р. Вебер пишет, что большая часть крупных корпоративных клиентов компании так или иначе базируется в США, либо имеет представительство в этой стране, поэтому АНБ или другое ведомство могут обратиться непосредственно к клиенту.

Генеральный юрисконсульт отмечает, что по факту IBM сотрудничала с силовыми и разведывательными структурами, но делала это «через юридические каналы, признанные на мировом уровне».

Напомним, что ранее некоммерческая организация Information Technology & Innovation Foundation опубликовала отчет, в котором сказано, что американские хостинговые и ИТ-компании могут потерять от 22 до 35 млрд дол. в ближайшие три года на фоне скандала с прослушками АНБ. Кроме того, ряд стран, в частности Бразилия, некоторые страны Евросоюза, заявили, что могут принять законы, обязывающие хранить локальные данные только в пределах географических территорий страны.

Ранее с опровержениями информации о сотрудничестве с АНБ выступили и другие крупные западные ИТ-компании, в частности Google, Yahoo, Microsoft и Facebook ***(IBM отрицает информацию о сотрудничестве с АНБ // InternetUA (http://internetua.com/IBM-otricaet-informaciua-o-sotrudnicsestve-s-anb). – 2014. – 17.03).***

***

Агентство национальной безопасности (АНБ) США разработало техническую систему слежения, позволяющую записывать и потом при желании прослушивать абсолютно все телефонные разговоры отдельно взятой страны. Об этом сообщила 18 марта в своей электронной версии газета The Washington Post.

Ссылаясь на «людей, обладающих непосредственными знаниями» об этой программе АНБ, которое занимается радиоэлектронной разведкой, а также документы, полученные от бывшего сотрудника данного ведомства Э. Сноудена, издание уточнило, что означенная программа перехвата телефонных бесед целого государства впервые начала действовать в 2009 г.

Ее функция, позволяющая записывать и затем воспроизводить такие разговоры, работает с 2011 г. Весь колоссальный массив данных в виде аудиофайлов, который представляют собой перехваченные беседы по телефону абонентов какой-то конкретной страны, компьютеры АНБ способны хранить в течение месяца, подчеркнула газета. Соответственно, за это время спецслужбы США могут при желании получать доступ к любому такому перехваченному разговору в полном виде.

Против какой именно страны в 2009–2011 гг. США впервые стали применять эту программу, не поясняется. Цитируя документы Э. Сноудена, который предал гласности сведения о масштабных программах электронной слежки АНБ, TWP пишет только, что к 2013 г. США рассчитывали начать использовать систему перехвата телефонных разговоров и против других интересующих их государств. Бюджетные документы разведки США свидетельствуют о том, что программу перехвата телефонных бесед АНБ намеревалось распространить к октябрю минувшего года в общей сложности на шесть стран, отметила The Washington Post ***(АНБ США разработало систему для прослушки телефонов за пределами США // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/19/nsa-technique.html). – 2014. – 19.03).***

***

Международная неправительственная организация «Репортеры без границ» опубликовала очередную версию ежегодного отчета «Враги Интернета» по состоянию на 2014 г. Примечательным событием этого года стало то, что впервые в истории список пополнили сами родоначальники Всемирной сети, то есть Соединенные Штаты Америки. Как несложно догадаться, это произошло благодаря гиперактивности АНБ.

Особое внимание в отчете уделено Беларуси, где с недавних пор власти ужесточили контроль над Интернетом, в том числе обязали все белорусские компании размещать сайты обязательно только на белорусском хостинге, а также ввели в действие «черный список» оппозиционных сайтов, доступ к которым запрещен из государственных учреждений.

Кроме Беларуси и США, в список врагов Интернета традиционно включены Россия, Китай, Иран, Северная Корея и другие страны, которые осуществляют цензуру в Интернете, слежку за пользователями на уровне государственных агентств и владеют государственной монополией на телекоммуникационную инфраструктуру.

В России, как известно, действует система СОРМ для мониторинга трафика, в том числе на уровне интернет-провайдеров. Однако, в свете последних событий, становится понятно, что российские программы слежки по своему размаху и рядом не стояли с глобальной слежкой за трафиком и установкой вредоносных программ на компьютеры пользователей во многих странах мира, чем занимается АНБ. Да и до белорусских соседей России еще далеко ***(В список «врагов интернета» впервые добавлены США // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/19/usa-among-enemies-of-web.html). – 2014. – 19.03).***

***

Как сообщает издание The Guardian со ссылкой на одного из ведущих консультантов АНБ США Р. Де, крупнейшие технологические гиганты, в том числе Google, Apple, Microsoft, Facebook, Yahoo и AOL, были осведомлены о том, что разведывательное ведомство перехватывает данные их пользователей. При этом тот факт, что слежка велась в рамках программы PRISM, в этих компаниях могли не знать.

Выступая перед участниками правительственного заседания по вопросам защиты прав и свобод граждан США, Р. Де заявил, что сбор информации осуществлялся «с ведома и согласия» интернет-корпораций, однако они могли не знать, что данная программа наблюдения имеет название PRISM.

«Это термин, который использовался исключительно внутри АНБ, а широкой общественности стал известен лишь после утечек», – пояснил Р. Де.

Напомним, что ранее все без исключения крупные компании США, специализирующиеся на информационных технологиях, публично отрицали свою причастность к незаконному сбору информации граждан США и других стран ***(АНБ: Google, Apple, Microsoft, Facebook знали о слежке // InternetUA (http://internetua.com/anb--Google--Apple--Microsoft--Facebook-znali-o-slejke). – 2014. – 21.03).***

***

Власти Турции в ночь на 21 марта заблокировали доступ к популярному микроблогу Twitter. Всего за несколько часов до этого с заявлением о возможности блокировки сервиса выступил премьер-министр страны Р. Т. Эрдоган, пишет РИА «Новости» со ссылкой на газету Hurriyet.

Р. Т. Эрдоган на предвыборном митинге сторонников Партии справедливости и развития (ПСР) заявил, что в Турции будет искоренен Twitter. Он сослался на решение суда, позволяющее предпринять такие шаги, и отметил, что его правительство не волнует реакция международного сообщества.

Уже незадолго до полуночи турецкий телекоммуникационный регулятор BTK заблокировал доступ в Twitter. При попытке зайти в эту социальную сеть турецких пользователей перенаправляют к тексту регулятора, где цитируется судебные решения, позволяющие заблокировать сайт.

Канцелярия премьера пояснила, что на протяжении последних недель руководство компании игнорировало обращения турецких властей с требованием на основании судебных решений удалить некоторые ссылки в микроблогах. Таким образом, у Анкары «не осталось иного выбора, как закрыть доступ ко всему ресурсу».

Базирующаяся в Сан-Франциско компания уже посоветовала пользователям в Турции оставлять твиты через сервис смс в мобильных телефонах, что позволяет обходить введенный запрет.

Как сообщает агентство Reuters, некоторые пользователи Twitter выкладывали в сеть записи и документы, якобы свидетельствующие о

коррупции близкого окружения Р. Т. Эрдогана. Именно это послужило причиной резкой блокировки сервиса. Р. Т. Эрдоган назвал коррупционный скандал частью клеветнической кампании его политических врагов.

Политик ранее обращался в Twitter с просьбой открыть один из офисов компании на территории Турции, чтобы улучшить коммуникацию между властями страны и руководством ресурса. Однако Twitter на запрос так и не ответил.

На мартовском митинге политик даже обозвал микроблог, назвав его Twitter, mwitter.

Напомним, кроме Twitter, Р. Т. Эрдоган пригрозил заблокировать доступ к популярным ресурсам Facebook и YouTube. Поводом для заявления стала аудиозапись, на которой Р. Т. Эрдоган общается со своим сыном Билялем, обсуждая коррупционную схему. На записи речь идет о получении крупной взятки от местного бизнесмена С. Аяна, которому кабинет министров дал освобождение от налогов для строительства нового нефтепровода из Ирана ***(Власти Турции заблокировали доступ к Twitter, на очереди Facebook и YouTube // InternetUA (http://internetua.com/vlasti-turcii-zablokirovali-dostup-k-Twitter--na-ocseredi-Facebook-i-YouTube). – 2014. – 21.03).***

***

Команда Twitter отреагировала на блокировку своей работы в Турции, предложив всем поклонникам использовать для обмена короткими сообщениями SMS-службу, связанную с этим популярным сервисом микроблогов. Хотя данный «обходной маневр» не вполне удобен и чреват определенными ограничениями, другого пути к Twitter для турецких граждан, судя по всему, в ближайшее время уже не предвидится. Таким образом, Турция присоединилась к странам, где на официальной основе с подозрением относятся к соцсетям и Twitter в частности.

Напомним, что доступ к Twitter в той или иной степени ограничен в Иране, Египте, Китае и некоторых других странах, при этом в КНР, к примеру, создан даже свой национальный сервис микроблогов ***(Twitter предлагает использовать SMS в связи с турецкой блокадой // InternetUA (http://internetua.com/Twitter-predlagaet-ispolzovat-SMS-v-svyazi-s-tureckoi-blokadoi). – 2014. – 23.03).***

***

В Сеуле, Южная Корея, ученики школ отныне обязаны установить на свои смартфоны программу iSmartKeeper, которая предоставляет учителям дистанционный доступ к мобильному устройству и возможность блокировать работу смартфона.

Приложение позволяет закрывать доступ с мобильного устройства к любым играм, социальным сетям или SMS, оставив только то, что необходимо для учебы или ответа на срочные входящие звонки. Впрочем, смартфон можно «заглушить» и полностью.

В зависимости от настроек приложение автоматически начинает блокировать телефон в соответствии с расписанием уроков, открывая ученикам доступ к развлечениям только во время перемен. Помимо учителей, удалённый доступ к смартфонам могут получить и родители.

Такими методами власти Южной Кореи планируют бороться с засильем телефонов в школах – эта проблема стремительно превращается в настоящую эпидемию. Вместо того чтобы заниматься, дети всё время играют в игры, проверяют почту или общаются в социальных сетях.

Первые шаги в войне с телефонами в школе пока что не слишком впечатляют. Некоторые технически продвинутые школьники уже научились обходить действие программы-блокировщика и даже развернули целый подпольный рынок «разблокирования» смартфонов.

Кроме того, в настоящее время система работает только с Android-смартфонами – обладатели устройств, работающих под iOS или Windows Phone, могут продолжать развлекаться во время занятий.

Тем не менее, Министерство образования Южной Кореи полно решимости создать эффективно действующую систему, блокирующую телефоны учеников во время уроков ***(Учителя в Южной Корее удалённо блокируют смартфон ученика на время занятий // InternetUA (http://internetua.com/ucsitelya-v-uajnoi-koree-udal-nno-blokiruuat-smartfon-ucsenika-na-vremya-zanyatii). – 2014. – 23.03).***

Проблема захисту даних. DDOS та вірусні атаки

Специалисты говорят о новом суперсложном вредоносе Turla

Ранее неизвестное шпионское программное обеспечение уже смогло инфицировать сотни правительственных компьютеров в Европе и США. Специалисты говорят, что по своей логике вредонос является одним из сложнейших за всю историю. Несколько западных специалистов по ИТ-безопасности и разведывательных агентств полагают, что вредоносное программное обеспечение Turla работает в интересах официальных российских властей и связано с тем же программным обеспечением, которое уже поражало американские военные сети в 2008 г.

Подобные утверждения основаны на анализе тактики хакеров, а также на множестве технических индикаторов и жертвах, которые были атакованы Turla. «Это сложное программное обеспечение, похожее на другие эксплоиты российского производства. Оно использует шифрование и ориентировано на западные правительства», – говорит Д. Льюис, экс-служащий дипломатической службы США, в настоящее время старший научный сотрудник Центра стратегических и международных исследований в Вашингтоне.

Тем не менее, эксперты по безопасности предупреждают: связь с Россией – это лишь догадка, которую невозможно подтвердить до тех пор,

пока (и если) Москва не возьмет на себя ответственность за создание кода. В Turla разработчики используют много технологий для сокрытия собственной личности.

Отметим, что слухи о новом российском супер-вредоносе изначально были заявлены небольшой немецкой антивирусной компанией G Data, однако в терминологии этой компании код получил названием Uroburos. Здесь говорят, что российские проправительственные хакеры пишут достаточно качественный с точки зрения функционала софт и умело скрывают свою личность, кроме того, они очень эффективно поддерживают контроль над зараженными ресурсами и сетями. Здесь тактика атак выбирается очень избранно и подгоняется под конкретную жертву. Китайские проправительственные хакеры действуют совершенно иначе – они атакуют максимально широко, надеясь хотя бы единожды попасть в цель.

«Все они знают, что большинство людей не имеют технических знаний, чтобы победить. Кроме того, большинство людей не задумываются о хакерской угрозе и делают многие вещи в спящем состоянии», – говорит Д. Льюис.

В пятницу британский оборонный подрядчик BAE Systems Applied Intelligence также сообщил о выявлении нового вредоносного кода, атакующего британские правительственные учреждения. В терминологии BAE код именуется Snake. В BAE также говорят о чрезвычайно высокой сложности кода. В настоящее время невозможно установить, являются ли Turla, Uroburos и Snake одним и тем же кодом.

В антивирусной компании Symantec говорят, что на сегодняшний день жертвами Turla стали около 1000 сетей. Кроме того, здесь убеждены, что за Turla и ранее обнаруженным кодом Agent BTZ стоят одни и те же люди. В Symantec не называют жертв вирусов, но говорят, что подавляющее большинство – это правительственные агентства.

В финской F-Secure говорят, что они впервые с Turla столкнулись еще в прошлом году, когда расследовали комплексную атаку в интересах одного из заказчиков. «Turla похож на русский код, однако достоверно говорить об этом нельзя», – говорит технический специалист F-Secure М. Хиппонен. По его словам, Turla и Agent.BTZ – это коды одного семейства. Первые примеры этого семейства были использованы для атаки на Центральное командование США в 2008 г. При этом сам Вашингтон не признает факт данной атаки и по сей день.

В F-Secure говорят, что пророссийские коды использовались в том же 2008 г. для атаки сетей НАТО. В настоящее время неизвестны названия кодов, использованных тогда для атак. М. Хиппонен говорит, что в прошлом году похожий код был использован для нападения на Министерство иностранных дел Финляндии.

Э. Чен, технический директор Sysmantec Security Response, говорит, что Turla – это «дальнейшая эволюция» Agent.BTZ. «Очевидно, что группа, работающая над этими вредоносами активна и в наши дни», – полагает он.

Х. Бласко, директор AlienVault Labs, говорит, что им также известно о Turla. Здесь данный вредонос описывают как «фреймворк» для шпионажа, а не как единичное вредоносное ПО. Выявленный ими код создает клиентский руткит, который прячет свое присутствие посредством создания шифрованной виртуальной файловой системы, в которую уводятся краденные данные. Кроме того, архитектура вредоноса такова, что оператор атаки может добавлять во вредонос дополнительные модули с новым функционалом.

Э. Чен говорит, что кодами Turla пользуются и в данный момент, так как управляющие серверы, на которые стекаются данные, постоянно обновляются и при отключении одного сервера в сети тут же появляется новый ***(Специалисты говорят о новом супер-сложном вредоносе Turla // InternetUA (http://internetua.com/specialisti-govoryat-o-novom-super-slojnom-vredonose-Turla). – 2014. – 11.03).***

***

Защита данных в самом широком смысле этого слова становится лейтмотивом открывающейся в немецком Ганновере выставки CeBIT 2014. Здесь не так много новинок, как на январской CES 2014 или на февральской MWC 2014, однако философии и трендообразования тут не в пример больше.

Многие участники CeBIT 2014 вводят новое понятие Datability или Data Responsibility, то есть ответственность за данные. Понимать это следует в самом широком смысле: ответственность пользователей за генерируемые ими данные, ответственность провайдеров за клиентские данные, ответственность властей перед гражданами за доступ к их данным. «Цифровой мир изменился, его необходимо поместить в юридическую плоскость, не забывая о порядке и законности. Мы находимся в самом начале этого пути. Национальные законы отдельно взятой страны в цифровом мире уже не работают», – заявила на открытии CeBIT 2014 канцлер Германии А. Меркель.

Ограничение сбора данных – это уже неверный подход, полагает Д. Кемпф, президент немецкой ассоциации Bitkom. «Нам следует найти нужные границы сбора персональных данных для современного цифрового мира», – говорит он. – Конечно, можно запретить сбор данных в принципе, но это будет ударом по безопасности страны».

«Те, кто хочет использовать персональные данные, должны и защищать их. Сейчас сложилась ситуация, когда использование ИТ зачастую создает больше проблем, нежели преимуществ. Это в корне неверно», – говорит он. Одновременно с этим, Д. Кемпф заявил, что на фоне последних скандалом с прослушками данных со стороны разведки США в Европе, следует пересмотреть договоры о свободной торговле и обмене данными.

С. Вайль, президент-министр немецкой федеральной земли Нижняя Саксония, где расположен Ганновер, говорит, что защита данных с современном мире неразрывно связана с моральными аспектами частной

жизни. «Мы на уровне Европейского Союза должны установить стандартные правила о высоком уровне конфиденциальности данных. В ходе переговоров о свободной торговле с США наши европейские стандарты должны стать эталоном», – убежден он.

Даже М. Винтеркорн, генеральный директор Volkswagen, выразил обеспокоенность в связи с тем, что сегодняшние компьютерные технологии, связанные с автомобилями, могут стать угрозой для конфиденциальности своих владельцев. «Мы стремимся защитить наших клиентов от всех видов риска и опасности в дорожной ситуации. Однако сейчас мы должны быть в равной степени ответственны и за защиту наших клиентов от злоупотребления персональными данными клиентов», – говорит он.

Чтобы избежать «навязчивого мониторинга» водителей и избыточного государственного регулирования, он призвал всех автопроизводителей подумать над общими стандартами в области конфиденциальности данных.

Открывал выставку в том числе и европейский робот-гуманоид RoboThespian, который символизировал будущие тренды в развитии технологий. В рамках открытия CeBIT организаторы сообщили, что значительная часть приготовленных для журналистов инноваций так или иначе связана с инновациями в области защиты данных и облачного хранения.

Одними из первых свои новинки показали германские компании SecuSmart, Digittrade и Datev.

Продукты первой особенно актуальны на фоне недавнего скандала с прослушками. Разработка компании представляет собой программное обеспечение для смартфона, которое шифрует как голосовые звонки, так и передачу данных. Для хранения используется карта памяти microSD с 4 Гб памяти, а также специальный чип, выполняющий шифрование голоса. Кроме этого, компания поставляет защищенную систему телеконференций SecuBridge и телефонии SecuGate LV.

Показываются на CeBIT и европейские ответы мессенджеру WhatsApp, купленному Facebook за 19 млрд дол.

Компания Digittrade показывает собственные системы мобильной криптографии Chiffry. Эта компания подчеркивает, что она расположена в Европе, все ее разработчики – европейцы, а все данные находятся в ЕС. В свою очередь компания Datev показала старую технологию на новый лад: смарткарт-ридер для смартфонов. В компании говорят, что изначально смарткарты – это хорошая и надежная задумка, однако современные смартфоны для нее почему-то совершенно не предназначены. Продукт компании работает по технологии Bluetooth ***(CeBIT 2014: Курс на приватность данных // InternetUA (http://internetua.com/CeBIT-2014--kurs-na-privatnost-dannih). – 2014. – 11.03).***

***

В последнее время злоумышленники все чаще прибегают к DDoS-атакам, при этом весьма масштабным. В частности, эксперты из Sucuri говорят о том, что в одном из недавних инцидентов безопасности были задействованы более 162 тыс. сайтов на базе WordPress. Известно, что все ресурсы работали с активным по умолчанию протоколом вызова удаленных процедур XML-RPC.

Как утверждают эксперты, атака осуществляется посредством генерации HTTP-запросов. При этом все сайты могут отправлять сотни тысяч запросов в секунду.

Судя по всему, большинство запросов содержат случайное значение (?4137049=643182), необходимое для очистки кэша и полной перезагрузки страницы. По данным Sucuri, подобные атаки весьма успешны, поскольку они способны быстро нарушить работу сервера.

Эксперты компании также уверены, что DDoS-атаки с задействованием сайтов с уязвимостью XML-RPC могут быть более масштабными. Узнать, не является ли сайт частью атаки, можно посредством проверки файла регистрации на наличие POST-запросов к файлу XML-RPC. Также существует база, созданная Sucuri, в которой содержится список задействованных в инцидентах безопасности ресурсов.

По данным компании, избежать использования ресурса на базе WordPress можно посредством прописывания в шаблоне специального кода:

```
add_filter( ‘xmlrpc_methods’, function( $methods ) {
unset( $methods[‘pingback.ping’] );
return $methods;
} );
```

(Более 162 тысяч сайтов на WordPress были использованы для DDoS-атаки // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/12/WordPress-sites-used-for-DDoS.html). – 2014. – 12.03).

***

Разработчики социальной сети утверждают, что решение проблемы, заключающееся в использовании HTTPS, является не практичным.

В Facebook реализован целый ряд мер безопасности, предназначенных для защиты учетных записей пользователей от взлома. К примеру, многие приложения социальной сети используют специальный маркер доступа (access token), который должен быть подтвержден пользователем, чтобы программа могла получить временный и безопасный доступ к различным API-интерфейсам Facebook.

Таким образом, путем подтверждения соответствующего запроса от того или иного приложения, пользователь разрешает ему получить доступ к строго определенной информации своей учетной записи. При этом упомянутый маркер доступа хранит информацию о собственном сроке

действия, предоставленных программе правах доступа, а также о том, каким приложением он был сгенерирован.

Исследователь безопасности из Египта А. Эльсобки опубликовал пример проведения MITM-атаки на пользователей Facebook, позволяющей получить доступ к этому маркеру. По словам эксперта, проведение подобной атаки возможно из-за того, что приложения социальной сети не используют HTTPS.

Отметим, что приложения, получившие соответствующие привилегии от пользователя, могут публиковать и удалять контент Facebook от имени этого пользователя. При этом для доступа используется access token, а не пароль владельца учетной записи. Таким образом, любой, кто завладел маркером, может также получить доступ к конфиденциальным данным, а также может выполнять любые действия (на которые ранее было выдано разрешение) от имени пользователя до тех пор, пока маркер является валидным.

В Facebook заверяют, что им известно о слабых местах данной технологии, и команда уже работает над усовершенствованием официальных приложений социальной сети, поскольку им «заранее выдаются необходимые привилегии». В то же время разработчики социальной сети отмечают, что в настоящее время они не могут заняться той же проблемой в отношении программ независимых разработчиков.

«К сожалению, для сторонних приложений наши методы решения проблемы будут означать необходимость использовать HTTPS любым сайтом, интегрированным с Facebook, что в настоящее время просто не практично», – поясняют представители социальной сети ***(Facebook не может защитить пользователей от MITM-атак // InternetUA (http://internetua.com/Facebook-ne-mojet-zasxitit-polzovatelei-ot-MITM-atak). – 2014. – 13.03).***

***

Эксперт по информационной безопасности Д. Данчев сообщил, что киберпреступники постоянно совершенствуют инструменты для осуществления вредоносной деятельности (вирусы, ботнеты и т. д.) с целью их продажи на черном рынке. По его словам, недавно специалисты обратили внимание на новый инструмент киберпреступников – DNS амплификацию, включающую DDoS-бота.

Этот DDoS-бот использует публично доступные открытые DNS распознаватели, созданные для исследовательских целей. ПО написано на языке C, а код бот-агента имеет небольшой размер и полагается на собственную обфускацию и алгоритм упаковки. Все соединения с C&C-серверами зашифрованы, что делает ботнет более устойчивым.

Сервис включает в себя встроенный DNS сканер, обнаруживающий DNS-серверы неправильной конфигурации, которые можно задействовать в атаках. Стоимость инструмента составляет 2,5 тыс. дол. Сюда входит

«пуленепробиваемый» хостинг для сервера управления, а также опция размещения на выбранном заказчиком сервере зашифрованного архива.

Кроме того, покупатель получит доступ к VPN серверу для эксклюзивного использования при доступе к интерфейсу бота. Особый интерес у Д. Данчева вызвали видеоролики, наглядно демонстрирующие распознаватель DNS ***(Ботнет с технологией DNS амплификации доступен на черном рынке // InternetUA (http://internetua.com/botnet-s-tehnologiei-DNS-amplifikacii-dostupen-na-csernom-rinke). – 2014. – 13.03).***

***

Специалист по информационной безопасности опубликовал инструкцию по взлому базы данных WhatsApp с историей переписки. «Я должен сделать вывод, что любое приложение может читать вашу переписку в WhatsApp», – резюмировал он.

Уязвимость в мобильном приложении WhatsApp позволяет получать полный доступ к переписке пользователя злоумышленникам из сторонних приложений, установленных на мобильное устройство. Инструкцию по взлому написал и опубликовал в своем блоге независимый специалист по информационной безопасности и главный технический директор DoubleThink Б. Босхерт.

Проблема касается только устройств на базе Android, в которых WhatsApp сохраняет резервную копию истории на карте памяти. Большинство приложений, устанавливаемых на устройство, имеют доступ к карте памяти. Таким образом, они могут легко получить доступ к файлу базы данных WhatsApp.

Для того чтобы расшифровать файл, Б. Босхерт написал несложный скрипт на языке Python, текст которого опубликовал в своем блоге. Ключ шифрования автор взял из приложения WhatsApp Xtract, которое позволяет просматривать и хранить историю переписки из WhatsApp на персональном компьютере. WhatsApp использует один и тот же ключ для шифрования сообщений всех пользователей, отметил эксперт.

После расшифровки Б. Босхерт воспользовался простым приемом для преобразования файла базы данных в легко читаемый на любом компьютере файл в формате Excel.

По словам Б. Босхерта, извлечение данных из файла WhatsApp может происходить в фоновом режиме незаметно для пользователя. Это может быть сделано в любом приложении, безобидном на первый взгляд. Данные затем могут быть отправлены на сервер злоумышленников. Эксперт отметил, что в последнем обновлении WhatsApp, которое вышло 11 марта, эта уязвимость не была устранена.

В iPhone воспользоваться указанной уязвимостью мешают алгоритмы защиты, встроенные непосредственно в платформу iOS. Они изолируют каждое запущенное приложение, запрещая доступ ко всем его файлам извне, поясняет TechCrunch.

Низкий уровень безопасности в WhatsApp является объектом критики с прошлого года, из-за чего власти Германии, например, рекомендуют воздержаться от его использования. «Приложение WhatsApp понравилось бы АНБ», – передает слова исследователя из консалтингового агентства Praetorian П. Хауреги издание Ars Technica. Специалист имеет в виду, что разработчики сами облегчают спецслужбам прослушку. Причем WhatsApp пользуются свыше 450 млн человек во всем мире.

«Я должен сделать вывод, что любое приложение может читать вашу переписку в WhatsApp. Кроме того, возможно читать переписку в зашифрованной базе данных. Facebook вовсе не требовалось покупать WhatsApp, чтобы читать ваши чаты», – написал Б. Босхерт ***(Опубликована инструкция по взлому переписки WhatsApp // InternetUA (http://internetua.com/opublikovana-instrukciya-po-vzlomu-perepiski-WhatsApp). – 2014. – 13.03).***

***

16 березня здійснюється потужна DDOoS-атака на сайт «Укрінформ».

Про це «Телекритику» повідомив гендиректор інформагенції О. Децик. Нагадаємо, 16 березня редакція сайту «Сегодня» заявила про DDoS-атаки ***(Здійснюється потужна DDoS-атака на сайт «Укрінформ» // «Телекритика» (http://www.telekritika.ua/kontent/2014-03-16/91587). – 2014. – 16.03).***

***

Сайт президента Росії www.kremlin.ru працює з перебоями через DDoS-атаки, фахівці вживають заходів для відновлення роботи ресурсу

Про це повідомили в прес-службі Кремля, пише Еспресо.TV з посиланням на «РИА Новости».

«Іде потужна атака на сайт. У зв’язку з тим, що атака продовжується, можливі перебої в його роботі. Вживаються всі заходи для організації нормальної роботи ресурсу, для того, щоб сайт був доступний», – розповіли в прес-службі, зазначивши, що хакерській атаці 14 березня піддався і ряд інших ресурсів.

Зокрема, сайт ЦБ РФ не працював з 10 ранку протягом приблизно однієї години, фахівці служби безпеки вживають усіх необхідних заходів для усунення проблеми ***(Хакери атакують сайт Кремля // Espreso.tv (http://espreso.tv/new/2014/03/14/khakery_atakuyut_sayt_kremlya). – 2014. – 14.03).***

***

Мифы о компьютерной безопасности, которые могут вам навредить

Игнорирование простых правил цифровой безопасности сулит вам потерю конфиденциальных данных, денег, и поход к психотерапевту. Подкованные юзеры знают большинство методов защиты личной

информации и не питают лишних иллюзий о компьютерной безопасности. Данный пост, в первую очередь, ориентирован на пользователей ПК, только начинающих приобщаться к компьютерной грамотности. Мы развеем некоторые распространенные мифы о сетевой безопасности, дабы уберечь вас от потенциального вреда.

Вирус не попадет в компьютер, если ничего не скачивать

Некоторые пользователи ПК полагают, что вирус – это злокачественный файл с вредоносным кодом, загруженный из недобросовестного закоулка Интернета. Данное суждение не актуально для веба уже с десяток лет. Спектр угроз не ограничен лишь запуском непонятного файла с расширением bat или exe.

Компьютерные черви, самостоятельно распространяющиеся вредоносные программы, находят уязвимости в программном обеспечении операционной системы и заражают компьютер-жертву без участия и ведома пользователя. В большинстве случаев уязвимости содержатся в софте, но иногда лазейки могут быть найдены в прошивке оборудования. Например, некоторые маршрутизаторы могут быть подвержены удаленному заражению.

Но и это не все. Даже доверенный сайт с большой аудиторией может быть взломан хакерами. Инфицированная веб-страница может не оказывать никакого вреда в течение многих лет до той поры, пока злоумышленники не отправят команду нападения.

Вывод прост. Используйте антивирусное решение для компьютера, даже если вы ничего не скачиваете и пользуетесь только заслуживающими доверия сайтами.

Компьютер работает хорошо. Зачем его загружать антивирусом?

Наивно воспринимать стабильную работу компьютера за отсутствие проблем с безопасностью. А дело в том, что Голливуд укоренил в головах любителей американского кино веру в показушную деструктивность вирусов. При заражении обязательно должна выскочить страшная картинка, а диспетчер задач тут же отобразит повышенную нагрузку на процессор.

На самом деле, все немного не так. Хотя некоторые вирусы действительно устраивают настоящий перфоманс, большинство все же действуют скрытно и максимально заметают следы. Наиболее изощренными из них являются вирусы и троянские программы, пытающиеся завладеть личной информацией пользователя.

Действительно, антивирус будет потреблять некоторые ресурсы вашего персонального компьютера. Обычно это пара сотен мегабайт оперативной памяти и небольшая часть мощности процессора. Для более или менее современной машины данные ресурсы абсолютно незначительны.

Итак, установив антивирусное ПО, вы можете быть уверенными в том, что никакой зловред не пытается выдать уверенную работу компьютера за отсутствие проблем с безопасностью.

Все антивирусы одинаковы

Рынок антивирусных решений богат, а поэтому – насыщен предложениями. Многим пользователям сложно сориентироваться в широком выборе, поэтому они устанавливают любой попавшийся под руку антивирус, утешая себя мыслью об идентичности всех решений.

Так на чем остановить свой выбор? Холивар на эту тему не закончится никогда. Кто-то оперирует собственным опытом, кто-то ориентируется на своих знакомых, но лучше положиться на результаты тестов независимых профессионалов. Хотя и их методики сравнения обязательно будут подвергнуты критике, но это все же лучшем, чем просто слова.

Не претендуя на абсолютную правду, приведем статистику независимой организации Av-test, занимающейся тестированием возможностей большого числа антивирусных пакетов.

Как правило, платные пакеты справляются с выявлением и удалением угроз лучше, чем их бесплатные братья. Результаты тестов могут варьироваться от года к году и различаться в различных операционных системах. Поэтому стоит регулярно ознакамливаться с мнением профессионалов.

Я не такой как все. У меня нет Windows. Мне нечего опасаться

Не беря в учет операционные системы для планшетов и смартфонов, Windows по-прежнему доминирует на рынке компьютерных рабочих систем. Неудивительно, что именно семейство Windows остается главной мишенью для вредоносных программ. Но это абсолютно не означает, что другие операционные системы безопасны. За последние годы увеличившаяся доля Mac OS привела к возрастанию количества инфицированных компьютеров под этой ОС. Mac OS не неуязвимы, просто до поры до времени написание ПО для них не имело экономической выгоды для злоумышленников. Да что говорить о продукции Apple, если вирусы пишутся даже под Linux.

Мне 15 и я живу с мамой. Кому я нужен?

Некоторые пользователи придумывают массу причин, по которым они просто не могут попасть под прицел злых программ. Я ничего не покупаю онлайн. Я не плачу за коммунальные услуги через Интернет. Я вообще редко сижу за компьютером.

Дело в том, что все вирусы – это лишь программы. Как и все программы, вирус делает то, на что он запрограммирован. Ни больше, ни меньше. Если зловред крадет вводимые логины и пароли, он будет делать свою работу каждый раз и на всех сайтах. Будет ли это вечером во «ВКонтакте» или с утра в интернет-банке. Ему все равно.

В общем, антивирус – необходимая штука, как ни крути. Не стоит ждать того момента, когда вы заподозрите или точно узнаете о наличии вируса на компьютере. Лучше предупредить ситуацию и установить защитное ПО до наступления проблем ***(Мифы о компьютерной безопасности, которые могут вам навредить // InternetUA (http://internetua.com/mifi-o-kompuaternoi-bezopasnosti--kotorie-mogut-vam-navredit). – 2014. – 15.03).***

***

У переддень референдуму в Криму хакери вчинили напад на кібермережі НАТО, повідомила у Twitter речниця Організації Північноатлантичного договору О. Лунджеску. Відповідальність за атаки взяв на себе сайт cyber-berkut.org.

«Декілька сайтів НАТО стали мішенню значної DDoS-атаки, – написала вона у Twitter. – Однак це не вплинуло на здійснення ними операцій. Наші експерти працюють над тим, щоб відновити їхнє нормальне функціонування».

Інший офіційний представник НАТО заявив: «Це не перешкоджає нашим спроможностям здійснювати командування і контроль над збройними силами. Жодного ризику нашим засекреченим джерелам ніколи не виникало», повідомила Reuters.

CNN повідомила, що впродовж декількох годин після оприлюднення заяви телемережа не могла отримати доступ до щонайменше трьох сайтів НАТО.

Головний громадський сайт НАТО nato.int, на якому розміщено заяву Генерального секретаря А. Расмуссена із засудженням кримського референдуму як нелегітимного, функціонував безперебійно.

Натомість DDoS-атака вразила також пов'язаний з НАТО Центр кібербезпеки в Естонії. Постраждала також мережа електронної пошти НАТО, що поширює незасекречену інформацію, повідомила Reuters.

Організація Північноатлантичного договору не інформувала, хто вчинив атаку. Натомість відповідальність взяв на себе сайт під назвою Cyber Berkut. Він проголосив російською мовою: «Ми заявляємо, що сьогодні, (в суботу), о 18:00 розпочали кібератаку на ресурси НАТО». Далі в заяві стверджувалося, що НАТО нема чого шукати на українській території.

Хто саме здійснив атаку через сайт cyber-berkut.org визначити не вдалося.

Перші ознаки серйозно вказують на те, що насправді це – справа проросійських сил, вважає головний експерт з технологій дослідного інституту U.S. Cyber Consequences Unit Д. Бамгарнер. Він порівняв їхні кібератаки проти НАТО зі «жбурлянням піску в обличчя».

Експерт з кібервійни Д. Карр вважає Cyber Berkut групою затятих прихильників усуненого від влади президента В. Януковича і «проросійських хакерів-активістів, які борються проти незалежності України».

Reuters характеризує їхню акцію як «останній прояв ескалації у кіберпросторі у зв'язку з напруженістю довкола Криму».

Кібератаки на комп'ютерні системи НАТО, відзначає Reuters, – звичне явище. Однак офіційний представник на умовах анонімності сказав у неділю інформаційній агенції, що остання з них була серйозною.

Останнім часом, після усунення від влади В. Януковича, у зв'язку з втручанням Росії у внутрішні справи України та виникненням кризи в її

стосунках із Заходом, кібернападів зазнавали українські та російські сайти. Та відтоді це – «перша велика атака на західний сайт», наголошує Reuters.

Spiegelonline так само вважає, що «за нападниками стоять проросійські сили».

Директор оборонного центру реагування НАТО на кібератаки (NATO's cyber defense nerve centre) Я. Вест заявив, що торік його системи стеження фіксували щодня близько 147 млн «підозрілих інцидентів» і близько 2500 з них виявлялися серйозними атаками ***(Сайти НАТО стали мішенню «КіберБеркута» // «Телекритика» (http://osvita.mediasapiens.ua/material/28678). – 2014. – 17.03).***

***

Антиправительственная организация «КиберБеркут» за последние несколько дней осуществила ряд успешных атак на украинские веб-ресурсы. Хакеры временно заблокировали работу информагентств Liga.net и Unian.net, веб-сайта А. Парубия Parubiy.org, западного портала zik.com.ua и ряда других онлайн-ресурсов. На днях те же злоумышленники взломали почтовые ящики региональных отделений партий УДАР и «Батькивщина» и произвели ряд атак на телефоны украинских политиков и вербовщиков Национальной Гвардии, пишет AIN.UA (http://ain.ua/2014/03/19/516603).

«КиберБеркут» позиционирует себя как хакерская группировка, которая «помогает Украине сохранить независимость от военной агрессии Запада, готового защитить правительство неофашистов». Участники группы создали свою страницу в Facebook, где преимущественно общаются российские пользователи, и сайт Cyber-berkut.org.

19 марта на телефонную хакерскую атаку пожаловался член партии «Свобода» И. Мирошниченко. По его словам, о подобной проблеме заявили несколько его однопартийцев, в том числе, лидер партии О. Тягнибок.

До этого о подобных атаках писали на своей странице в Facebook народные депутаты А. Бригинец и Л. Оробец. По их словам, каждые несколько десятков секунд поступает входящий вызов, но как только абонент поднимает трубку, связь обрывается.

Пророссийские хакеры «КиберБеркут» уже вторую неделю атакуют украинские сайты и телефоны политиков. По информации издания «Дело», звонки совершаются через транзитные номера с телефонов российских операторов. При этом сами операторы пока толком не знают, как бороться с такими атаками. «К сожалению, бороться с этим явлением на сегодняшний день очень трудно. У мобильных операторов нет способа автоматической блокировки подобных атак, – рассказывает начальник департамента безопасности "МТС Украина" Д. Винцевич. – Единственное, что может сделать оператор, – это с разрешения атакуемого абонента временно заблокировать международный трафик, весь или с определенных направлений. Но блокировка не решает задачи, потому что определить по транзитным номерам происхождение звонков невозможно, так как

используются коды разных стран и даже локальных мобильных операторов для того, чтобы сделать это невозможным».

Также в МТС поясняют, что существует возможность подставить любой телефонный номер в качестве входящего, чем и пользуются «телефонные террористы». То есть жертва «телефонного терроризма» будет видеть входящий звонок, например, от абонента МТС или «Укртелекома», а на самом деле звонок осуществляется с «модуля», установленного за границей. При этом каждая иностранная компания в этой цепочке держит в тайне имена своих партнеров.

В пресс-службе «Киевстара» AIN.UA рассказали, что какой-то перенагрузки или аномальной активности в сетях оператора нет. При этом уточнили, что такие вещи лучше проверять по конкретным абонентским номерам.

Участники «КиберБеркута» пишут, что будут продолжать атаки до тех пор, пока «политические предатели Яценюк, Кличко, Тягнибок и Ярош не явятся с повинной в органы прокуратуры Республики Украины в Харькове или Симферополе» (про Симферополь «КиберБеркут» писал еще до референдума). В этом случае они обещают учесть «чистосердечное раскаяние политиков и применить к ним минимальное наказание» ***(Пророссийские хакеры «КиберБеркут» уже вторую неделю атакуют украинские сайты и телефоны политиков // AIN.UA (http://ain.ua/2014/03/19/516603). – 2014. – 19.03).***

***

Эксперты компании Dr. Web провели исследование трояна Rbrute, используемого для взлома Wi-Fi маршрутизаторов и распространения вредоносного ПО одного из старейших семейств Sality. Ему удалось продержаться столько времени благодаря способу распространения и коммуникационным возможностям.

Вирус способен отключать антивирусное ПО и межсетевые экраны, похищать информацию с зараженного компьютера и использовать его для рассылки спама, скачивать дополнительные вредоносные программы и т. д. Кроме того, он может использоваться в качестве руткита и распространяется через съемные накопители и сетевые ресурсы. Вредонос также работает в сочетании с вышеупомянутым трояном.

«После загрузки на Windows троян Rbrute устанавливает соединение с удаленным сервером и ждет дальнейших инструкций. Одна из них обеспечивает троян определенным количеством IP-адресов для сканирования», – поясняют эксперты. Помимо этого, ПО используется для осуществления атак по словарю. В случае их успешного проведения, троян отсылает соответствующий отчет на сервер, который затем дает команду маршрутизатору изменить настройки DNS-адресов.

Таким образом при попытке зайти на какой-либо сайт, пользователь перенаправляется на созданный злоумышленниками ресурс. По словам

исследователей, данная схема применяется киберпреступниками для расширения ботнета, созданного при помощи вируса Win32.Sector, который также относится к семейству Sality.

Rbrute способен взламывать пароли к маршрутизаторам D-Link DSL-2520U, DSL-2600U, TP-Link TD-W8901G, TD-W8901G 3.0, TD-W8901GB, TD-W8951ND, TD-W8961ND, TD-8840T, TD-8840T 2.0, TD-W8961ND, TD-8816, TD-8817 2.0, TD-8817, TD-W8151N, TD-W8101G, ZTE ZXV10 W300, ZXDSL 831CII ***(Троян Rbrute взламывает маршрутизаторы с целью распространения Sality // InternetUA (http://internetua.com/troyan-Rbrute-vzlamivaet-marshrutizatori-s-celua-rasprostraneniya-Sality). – 2014. – 15.03).***

***

Сайт известного информационного агентства Lenta.ru 17 марта перестал работать в результате хакерской атаки, пишут Новости ИТ.

Все произошло «как обычно» – в определенный момент времени сайт стал выдавать ошибку о недоступности содержимого, с соответствующим сообщением от владельцев хостинга, на котором размещен ресурс. В первый раз сайт Lenta.ru был непрерывно недоступен на протяжении целого часа.

Основной версией по поводу виновников нарушения работы сайта является участие группы Anonymous, ее русского представительства, которая уже успела заявить о своей причастности к данному акту. Они объясняют свои действием несогласием с редакционной политикой ресурса. Как известно, 12 марта был уволен главный редактор ресурса Г. Тимченко, а следом ушли еще 39 сотрудников компании. Anonymous опасаются, что вместо более-менее свободных и объективных материалов на Lenta.ru появится цензура и пропаганда ***(Anonymous атаковали сайт Lenta.ru // ProstoWeb (http://novostiit.net/anonymous-atakovali-sayt-lenta-ru-0005753). – 2014. – 18.03).***

***

В субботу, 15 марта, злоумышленники провели успешную атаку и сумели перенаправить DNS-запросы к публичному DNS серверу Google на сервер в Венесуэле. Атака была направлена на бразильских пользователей и длилась 22 мин.

По информации компании BGPmon, злоумышленники провели успешную атаку на маршрутизаторы вышестоящего провайдера и сумели осуществить подмену BPG таблиц. Затем маршрутизаторы оператора BT Latin America анонсировали некорректные маршруты, что привело к перенаправлению трафика. Причины, по которым маршрутизатор провайдера согласился анонсировать некорректные маршруты, неизвестны. Предполагается, что злоумышленники использовали одну из уязвимостей в реализации BGP.

Это далеко не первый случай перенаправления DNS трафика Google. В 2010 г. вследствие похожей атаки злоумышленники сумели перехватить весь

DNS-трафик пользователей Румынии и Австралии ***(Злоумышленники атаковали публичный DNS сервер Google // InternetUA (http://internetua.com/zloumishlenniki-atakovali-publicsnii-DNS-server-Google). – 2014. – 17.03).***

***

Как следует из сообщения ESET, команде исследователей компании при содействии CERT-Bund и шведских национальных ведомств удалось раскрыть вредоносную кампанию, в ходе которой хакерам удалось скомпрометировать более 25 тыс. Unix-серверов по всему миру.

В ходе инцидента, получившего название Operation Windigo, злоумышленники использовали троян, обладающий функционалом бэкдора, для образования ботнета. После заражения системы эта программа похищала учетные данные пользователей с целью перенаправления трафика жертв на вредоносные веб-сайты, а также для рассылки спама.

«Windigo разрастался в течение более чем двух лет, оставаясь абсолютно незамеченным исследователями безопасности. В настоящее время в распоряжении злоумышленников находится 10 тыс. серверов, – поясняет эксперт ESET П.-М. Бюро. – Это число становится еще более значимым, если подсчитать, какие вычислительные мощности, пропускные способности и объемы памяти находятся в руках хакеров».

По предварительным данным, хакеры рассылали не менее 35 млн нежелательных писем в день. При этом наибольшая часть инфицированных машин расположена на территории США, Германии, Франции и Великобритании.

Исследователи также предполагают, что в течение суток количество пользователей, перенаправленных злоумышленниками на вредоносные ресурсы, может достигать полумиллиона человек.

Следует отметить, что ставшие жертвой Windigo веб-сайты пытаются заразить пользователей систем на базе ОС Windows. Поклонники Mac в свою очередь просто перенаправлялись на рекламируемый злоумышленниками сайт знакомств, а владельцы iPhone – на порталы с порнографическими материалами ***(ESET обнаружила ботнет из 25 тысяч Unix-серверов // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/03/19/operation-windigo-malware-used-to-attack-over-500000-computers-daily.html). – 2014. – 19.03).***

***

Согласно данным экспертов из FireEye, им удалось обнаружить активность нового RAT WinSpy, способного инфицировать системы как на базе Windows, так и под управлением Android. В компании говорят, что вредоносную кампанию зафиксировали во время расследования атаки на ряд финансовых организаций США.

«Недавно FireEye наблюдал за целенаправленной атакой на американскую финансовую компанию, осуществляемую посредством рассылки фишинговых писем. В процессе исследования Windows-модулей для WinSpy мы также обнаружили различные Android-компоненты, которые можно применить для слежки за жертвой», – следует из сообщения, опубликованного в блоге компании.

В частности, эксперты по вопросам безопасности утверждают, что они заметили по крайней мере три разных приложения, которые содействуют в осуществлении слежки.

Старший исследователь угроз безопасности Н. Вилленев заявил, что комбинации Android и Windows компонентов могут быть использованы злоумышленниками для ряда целей: «У злоумышленника есть возможность установить и запустить дополнительную полезную нагрузку, перехватывать важные данные, такие как учетные данные и интеллектуальную собственность, передвигаться по сети, а также следить за жертвой посредством активации различных подключенных периферийных устройств, таких как web-камеры и микрофоны».

Стоит отметить, что RAT с компонентами, которые можно применять как в отношении Android-устройств, так и Windows-девайсов, являются весьма большой редкостью. «Мы сталкиваемся с RAT для Android и RAT для Windows, но не с комбинациями для них обоих», – подчеркнул Н. Вилленев ***(В сети зафиксирован RAT с компонентами для Windows и Android // InternetUA (http://internetua.com/v-seti-zafiksirovan-RAT-s-komponentami-dlya-Windows-i-Android). – 2014. – 20.03).***

***

Немецкоязычный веб-сайт интернет-магазина французской компании Citroën недавно был скомпрометирован неизвестными хакерами при помощи уязвимости в ColdFusion от Adobe. По данным издания The Guardian, речь идет о портале shop.citroen.de.

Ресурс специализируется на торговле различными товарами и тематическими подарками с символикой автопроизводителя. При этом его администрированием занималась сторонняя организация anyMotion, специализирующаяся на оказании услуг по веб-дизайну.

В Citroën подтвердили, что хакерам удалось взломать сайт и установить бэкдор, однако не стали уточнять, имела ли место кража личных данных клиентов компании или какая информация пользователей ресурса могла оказаться в руках злоумышленников.

Вместе с тем в компании настоятельно рекомендуют своим клиентам проявить бдительность и убедиться в сохранности своих сбережений на банковских счетах. Кроме того, администрация ресурса осуществила сброс паролей пользователей.

По данным независимого исследователя Б. Кребса, предыдущими жертвами хакеров, стоящих за данной атакой, являются пищевая компания

Smucker’s и организация Securepay, специализирующаяся на обработке операций с кредитными картами, брокерский новостной сервис PR Newswire и даже Adobe ***(Хакеры взломали электронный магазин Citroën с помощью эксплоитов для ColdFusion // InternetUA (http://internetua.com/hakeri-vzlomali-elektronnii-magazin-Citro-n-s-pomosxua-eksploitov-dlya-ColdFusion). – 2014. – 21.03).***

***

Веб-серверы, работающие под управлением устаревших версий ядра Linux, были атакованы с феноменальной скоростью, сообщили в Cisco. Согласно сообщению компании, все затронутые серверы работают под управлением Linux Kernel 2.6, выпущенного в декабре 2003 г. Однако большинство поддерживаемых на сегодня Linux-дистрибутивов работают на базе ядер, выпущенных после 2010 г.

М. Ли, технический директор Cisco Threat Intelligence, говорит, что атака затронула старые серверы, работающие на базе Linux-ядер, выпущенных в 2003–2007 гг. «Подобные системы уже давно не поддерживаются и патчей для них нет. Когда атакующие нацелены на подобные системы, они могут не волноваться за то, что их эксплоит вскоре окажется не работающим», – говорит он.

После того как на атакованный сервер попадал эксплоит, через него организаторы атак размещали JavaScript на обслуживаемых сайтах. Размещенный JavaScript ссылался на другой файл, который подгружал клиентский вредоносный код на ПК клиентов. «Подобный двухступенчатный подход позволяет атакующим работать с разнообразным вредоносным контентом», – говорит М. Ли.

Согласно данным мониторинга Cisco Cloud Web Security, атаке на устаревшие Linux-ядра подверглись около 2700 хостов, на которых были размещены легитимные сайты. Значительная часть атакованных хостов размещена в США и Германии. Также компания отметила, что взрывной рост количества заражений выявлен 17–18 марта этого года, когда за несколько часов жертвами стали около 500 серверов ***(В сети зафиксирована масштабная атака на устаревшие Linux-серверы // InternetUA (http://internetua.com/v-seti-zafiksirovana-masshtabnaya-ataka-na-ustarevshie-Linux-serveri). – 2014. – 22.03).***

***

Компания Microsoft внесла изменения в условия использования почтовой службы Hotmail и сервиса Outlook.com. Теперь для получения доступа к переписке пользователя достаточно лишь подозрений, что он занимается противоправными действиями.

Изменения связаны с инцидентом, который произошел в сентябре 2012 г., когда С. Синофски, работавший главой подразделения Microsoft, получил по почте код сервиса активации Windows 8 с просьбой подтвердить

его подлинность. Как выяснилось, этот код отправитель получил от человека, который пользовался почтой Hotmail. Для того, чтобы заглянуть в ящик электронной почты злоумышленника, распространяющего украденный код, компании пришлось обратиться в правоохранительные органы. Теперь такого не потребуется – Microsoft сможет читать письма любого, кто по ее мнению, замешан в чем-то нелегальном.

В общем, причинять ущерб Microsoft и вести об этом переписку в ее сервисах теперь – очень плохая идея.

Примечательно, что несколько месяцев назад Microsoft упрекала Google в куда меньшем нарушении тайны переписки. Редмондцы запустили кампанию Scroogle, в которой пытались убедить людей, что мониторить письма для того, чтобы показывать более релевантную рекламу, как это делает Google, – аморально.

Удивительным образом Google выступила с обратной инициативой, нежели Microsoft. Отныне все сессии пользователей в Gmail будут осуществлять только через защищенное соединение HTTPS, отключить эту опцию нельзя. Более того, все передаваемые между серверами Google письма будут шифроваться. Письма Gmail и раньше шифровались, но информация между внутренними серверами перемещалась в незашифрованном виде. Нововведения направлены на что, чтобы пользователи были спокойны: их письма не смогут прочитать ни хакеры, ни спецслужбы, ни сотрудники Google.

Впервые поддержка HTTPS появилась в Gmail в 2004 г., а с 2008 г. этот тип соединения в настройках почты стало можно установить основным.

Как видим, подход Microsoft и Google к защите переписки совершенно разный. Пользователи Gmail могут бесстрашно отправлять письма хоть через открытый Wi-Fi, а любое из писем в Hotmail может быть прочитано кем угодно – без судебного решения и прочих формальностей. Просто потому, что сотрудник Microsoft сливал кому-то скриншоты операционной системы. Microsoft не может уследить на собственными работниками, поэтому будет следить за пользователям. Молодцы, так держать ***(Приватность для Microsoft – пустой звук // InternetUA (http://internetua.com/privatnost-dlya-Microsoft---pustoi-zvuk). – 2014. – 23.03).***

***

После 8 апреля, когда будет прекращена поддержка операционной системы Windows XP, прекратится выпуск обновлений безопасности для неё, и Microsoft не устаёт повторять о том, что система станет намного более уязвимой перед лицом сетевых атак. В том же духе высказывается и компания Avast, производитель одного из наиболее популярных бесплатных антивирусных приложений.

«Уязвимая операционная система станет лёгкой мишенью для хакеров и вратами для поражения связанных компьютеров на более современных версиях Windows», гласит запись в блоге Avast. «Данные нашей телеметрии

показывают, что пользователи XP подвергаются атакам в 6 раз чаще обладателей Windows 7, и после 8 апреля этот разрыв только возрастёт».

Почти четверть от 211 млн пользователей антивируса Avast работают как раз на Windows XP, так что компании есть, где собирать свои данные. По показаниям различных источников, от пятой части до 30 % подключенных к Интернету компьютеров по всему миру до сих пор управляются Windows XP.

Естественно, сама Avast видит главным способом избежать сетевых угроз для пользователей Windows XP в переходе на более современную версию системы и в использовании своего антивирусного программного обеспечения ***(Атаки на Windows XP уже происходят в 6 раз чаще, чем на Windows 7 // InternetUA (http://internetua.com/ataki-na-Windows-XP-uje-proishodyat-v-6-raz-csasxe--csem-na-Windows-7). – 2014. – 23.03).***

***

Эксперты безопасности, внимательно следящие за подпольными форумами, на которых продается вредоносное ПО, недавно обнаружили несколько интересных предложений, в том числе пакет программного обеспечения BlackOS.

Его не следует путать с BlackPOS, поскольку BlackOS представляет собой набор инструментов, направленных на упрощение работы киберпреступников. ПО централизует управление перенаправлением трафика с вредоносных или скомпрометированных сайтов через веб-интерфейс.

Согласно инструкции, пакет программного обеспечения обладает следующим функционалом:

· Реализация оптимальной модели преобразования трафика. Распространяется и устанавливается на User Agent.

· Уникальная возможность отказывать в продаже iframe-трафика.

· Автоматическое обнаружение PR доменов и ссылок, а также эффективное влияние на выдачу поисковых систем.

· Получение быстрых, стабильных списков socks5 для любого ПО, требующего использования прокси.

· Быстрая сортировка списка учетных записей.

· Загрузка любого скрипта с верификацией.

· Сканирование серверов на предмет наличия уязвимостей.

· Анализ баз данных удаленных систем управления контентом.

Стоимость BlackOS составляет 3,8 тыс. дол. в год и может быть уплачена в криптовалюте ***(Исследователи обнаружили пакет ПО BlackOS, централизующий управление перенаправлением трафика // InternetUA (http://internetua.com/issledovateli-obnarujili-paket-po-BlackOS--centralizuuasxii-upravlenie-perenapravleniem-trafika). – 2014. – 22.03).***

***

Інтегральна частина сучасного протистояння не лише військова техніка та економічний тиск, а й кібервійни та хакерські атаки. Вони помітно проявилися під час кримської кризи.

Солдати цієї війни не носять однострої та не дають присяги на вірність. Утім, їхня диверсійна діяльність може мати руйнівний ефект у сучасному високотехнологічному світі. Головна зброя в цій війні – DDos-атаки, які виводять з ладу функціональність веб-сайтів.

Подібних атак зазнають не лише сторінки ЗМІ, а й офіційні представництва владних органів та організацій. Наприклад, останніми днями через хакерські атаки з ладу на кілька годин був виведений офіційний сайт НАТО. Відповідальність за це взяла на себе невідома досі група «КіберБеркут». Відтак атаки зазнав створений сепаратистами в Криму сайт, присвячений так званому референдуму. Кримська влада звинуватила в цьому хакерів з американського університету в Урбана-Шампейн, штат Іллінойс.

Труднощі ідентифікації

Цьому передували хакерські атаки на сайти Кремля, Банку Росії та інформагенції РІА-Новості. Водночас, як зазначає інформагенція AFP, уряди країн світу та міжнародні організації традиційно не коментують використання хакерських атак проти опонентів. «Ідентифікувати нападників дуже важко. Відповідальність на себе може взяти будь-хто», – пояснює естонський експерт з питань інтернет-технологій А. Анспер.

За даними британської фірми BAE Systems, що працює у сфері оборонних технологій, DDos-атаки стали вже звичною частиною протистояння в українському інтернет-просторі. За її оцінками, починаючи з 2013 р., принаймні 22 рази проти українських веб-сайтів використовували особливо небезпечний вірус Snake.

«Фішинг» чи кібер-зброя?

Його розробили ще 2006 р., але відтоді він зазнав низки модифікацій, ставши ще агресивнішим, а головною мішенню залишається Україна. За оцінками BAE Systems, за його розробленням та використанням стоїть «добре організована і технічно потужна група».

Офіційно аналітики не беруться стверджувати, яка країна може за нею стояти. Водночас за оцінками голови російської «Лабораторії Касперського» Є. Касперського, Росія б діяла більш дискретно, а вірус Snake, на його думку, швидше нагадує не кіберзброю, а фішинг-вірус, який використовують онлайн-шахраї для викрадення банківських і персональних даних необережних користувачів ***(Кібервійни як частина конфлікту в Україні // InternetUA (http://internetua.com/k-berv-ini-yak-csastina-konfl-ktu-v-ukra-n). – 2014. – 23.03).***

***

Согласно последнему отчету ИБ-компании PandaLabs, в прошлом году было создано рекордное число совершенного нового вредоносного ПО. Так,

новые вирусы, появившиеся в 2013 г., составляют 20 % от их общего количества (30 млн образцов).

Наиболее распространенным вредоносным ПО являются трояны (78,97 % от всех существующих вредоносов). Более того, им принадлежит лидерство среди вредоносных программ, созданных в прошлом году (77,11 %). Отметим, что в 2011 г. на долю троянов припадало 66 %.

По данным исследователей, в 2013 г. вредоносным ПО были заражены 31,53 % компьютеров по всему миру. Этот показатель очень близок к показателю 2012 г. Также зафиксирован рост количества вирусов (с 9,67 % в 2012 г. до 13,3 % в 2013 г.), на которые приходится 5,83 % от всего вредоносного ПО. В основном рост коснулся представителей семейств Sality и Xpiro.

Кроме итогов за прошлый год в отчете также содержится прогноз по угрозам безопасности на 2014 г. По версии PandaLabs в нынешнем году особое внимание злоумышленники уделят Интернету вещей и Android-устройствам, компрометируя данные для похищения денег. Что касается мобильной платформы от Google, то эксперты прогнозируют появление сотен тысяч новых образцов вредоносного ПО, ориентированных на нее.

В прошлом году исследователи обнаружили огромное количество легитимных приложений для Android, содержащих вредоносную рекламу. По их данным, в 2013 г. для этой платформы было создано более 2 млн образцов нового вредоносного ПО ***(В 2013 году было создано рекордное число нового вредоносного ПО // InternetUA (http://internetua.com/v-2013-godu-bilo-sozdano-rekordnoe-csislo-novogo-vredonosnogo-po). – 2014. – 23.03).***

***

Многие эксперты по компьютерной безопасности не рекомендуют создавать открытых сетей WiFi, применяя вместо этого шифрование. Вместе с тем не рекомендуется применять стандарт шифрования WEP (Wired Equivalent Privacy), так как он предлагает достаточно слабый вариант шифрования данных и легко поддается взлому. До сих пор эффективным считался стандарт WPA2 (Wireless Protected Access 2), однако в настоящее время и его научились обходить.

В рамках совместного исследования Университета Бруннеля в Лондоне и Университета Македонии и Греции было установлено, что стандарт защиты WiFi-сетей WPA2 является на сегодняшний день сравнительно простым для взлома и содержит в себе уязвимости. По словам авторов исследования, WPA2 может быть взломан сравнительно легко за счет вредоносной атаки на беспроводную сеть. При этом авторы исследования говорят, что техническую базу WPA2 можно улучшить, однако для этого нужно работать с представителями стандартизирующих органов.

«Удобство подключения к беспроводной сети многочисленных устройств связи, таких как смартфоны, планшетные ПК, ноутбуки и телевизоры, компенсируется уязвимостями, присущими безопасности.

Потенциал третьей стороны, перехватывающей вещательный сигнал, существует всегда», – отмечают авторы исследования.

По их словам, проводные сети по своему определению более безопасны в сравнении с беспроводными, так как ареал распространения сигнала в них ограничен проводом. В то же время у беспроводных сетей ареал сигнала ограничен его мощностью и зачастую может простираться на сотни метров от компьютера или смартфона. Однако удобство работы с WiFi зачастую заставляет жертвовать безопасностью.

Авторы исследования говорят, что если пользователи будут использовать ключи шифрования WPA2 Pre-Shared Keys (PSK), то сами ключи шифрования могут быть в безопасности. В зависимости от версии системы, присутствующей в беспроводном устройстве, пользователи также могут использовать временные ключи TKIP (temporal key integrity protocol) или более безопасный CCMP (cipher block chaining message authentication code protocol), где длина пароля может быть увеличена до 63 символов и ключи длиной до 256 бит.

В рамках исследования специалисты на практике доказали, что атака по словарю на WPA2-пароли возможна не только в теории, но и на практике, хотя иногда время атаки может быть довольно продолжительным. Ускорить его можно, если хакер будет прослушивать сеть во время процесса де-аутентификации, когда клиенты обмениваются последними криптопоследовательностями. В отчете говорится, что сейчас технологии управления ключами WPA2 не меняются, тогда как мощности вычислительных устройств, способных на перебор ключей, постоянно растут.

В отчете специалистов говорится, что во время анализа WiFi-трафика существуют так называемые «точки входа», когда прослушать незакрытый трафик просто. Кроме того, исследователи рекомендуют отказаться от шифрования с привязкой к MAC-адресу, так как MAC-адреса сравнительно легко подделываются на программном уровне ***(WPA2 уже не такой надежный, как кажется // InternetUA (http://internetua.com/WPA2-uje-ne-takoi-nadejnii--kak-kajetsya). – 2014. – 23.03).***