СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(29.12.14–14.01.15)

2015 № 1

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(29.12.14–14.01.15)
№ 1

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 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Чим запам’ятався 2014 рік у соцмережах?

Поява нових соціальних мереж в Україні та світі, скандальний експеримент Facebook з емоціями користувачів, Twitter-шторми в час Євромайдану, блокування Twitter та YouTube в Туреччині – таким був 2014 р. у соціальних медіа.

Нові соціальні мережі

Патріотичне піднесення в Україні привело до появи протягом року низки нових соціальних мереж. Станом на липень було відомо про щонайменше п’ять українських соціальних медіа – druzi.org.ua, Socialface, Zine, «Українці» та weua.info. Остання досить довго анонсувала свою появу, а в день запланованого запуску через масовані DDoS-атаки була недоступною. Довгоочікувана презентація ресурсу відбулася лише через тиждень.

На цьому пригоди weua.info, що позиціонує як українська соцмережа, створена з метою бойкоту «ВКонтакте» та «Одноклассники», не завершилися. У вересні стало відомо про її конфлікт із ресурсом, що взяв собі аналогічну назву. Засновник weua.info Б. Оліярчук стверджував, що мережу-близнючку створили росіяни, а домен we.ua вони зайняли, випередивши його в подачі заявки лише на годину.

Виявили активність і українські нішеві проекти. Приміром, було створено ресурс для любителів футболу Footplayer та мережу корисних контактів Cardsaround.

Із новинок світового масштабу запам’яталася соцмережа Ello, яка із самого початку позиціонувала себе як конкурент Facebook. «Проста, красива і вільна від реклами», як твердить гасло, соціальна мережа була створена в березні, а вже у жовтні заявляла про кількість користувачів у понад мільйон та про доходи на суму 5,5 млн дол.

Скандальне звільнення

Оскільки «ВКонтакте» залишається найпопулярнішою соцмережею серед українців, перипетії зі зміною її гендиректора не могли залишитися для нас непоміченими. Чутки про можливу відставку П. Дурова з’явилися після зміни акціонерів компанії у 2013 р., вони час від часу виринали, та їх періодично спростовували.

Відомим фактом є те, що засновник та багаторічний керівник російської мережі П. Дуров має звичку публікувати провокативні повідомлення. Тому першоквітневий допис про рішення піти з посади гендиректора «ВКонтакте» було сприйнято як жарт. І через кілька днів він справді відкликав свою заяву. Проте 22 квітня П. Дурова таки звільнили акціонери компанії, стверджуючи, що формально заяви про звільнення він не відкликав. Зрештою, засновник «ВКонтакте» зізнався, що державні органи

чинили на нього тиск, та покинув Росію, заявивши, що не має наміру повертатися. Через деякий час стало відомо про отримання ним громадянства держави Сент-Кітс і Невіс, розташованої в Карибському морі.

Цензура

У країнах, де соціальні медіа залишаються одним з небагатьох незалежних джерел інформації, влада робила спробу заблокувати їх. Наприклад, прем'єр-міністр Туреччини, який згодом стане президентом, Р. Ердоган погрожував заборонити соціальні мережі, а згодом це таки трапилося з YouTube і Twitter, щоправда тривало недовго. Блокування соцмереж, як і нещодавні арешти журналістів опозиційних видань, експерти пов'язували з корупційними скандалами, що розгорнулися в Туреччині наприкінці минулого року, серед фігурантів яких був і Р. Ердоган.

Загроза блокування Facebook і Twitter була і в Росії. Прес-секретар тамтешнього органу контролю (Роскомнагляд) В. Ампелонський заявляв, що керівництво західних інтернет-компаній не йде на контакт із держорганами РФ, тож відомство може повністю їх заблокувати. І не вбачатиме в цьому, за словами чиновника, жодних ризиків. Ішлося тоді, зокрема, про можливе блокування Twitter, однак через деякий час сервіс мікроблогів таки поступився Роскомнагляду і почав блокувати на території Росії акаунти деяких користувачів, зокрема «Правого сектора».

Блокування соцмереж відбувалося і в авторитарному Казахстані, а також під час гонконзьких протестів.

Флешмоби

Цього року соціальні медіа були для українців майданчиком для вияву своєї громадянської позиції. Неодноразово організовувалися акції з метою поінформувати про ситуацію в Україні. Приміром, у січні, після загострення протистояння та перших убивств на вулиці Грушевського, відбувся Twitter-шторм із хештегом #digitalmaidan, що мав на меті привернути увагу західних журналістів, знаменитостей та політиків до подій у Києві. І хештегу #digitalmaidan таки вдалося вийти на перше місце у світі.

Звертался інтернет-користувачі і до окремих політиків. Приміром, у липні Facebook-сторінку німецького канцлера А. Меркель буквально «заспамили» коментарями «Дякую, пані Ріббентроп» (Danke Frau Ribbentrop) нібито за заклик вести переговори з терористами. А. Меркель тоді пояснила, що її заяву неправильно витлумачили і насправді вона висловлювала ідею щодо консультацій Тристоронньої контактної групи.

Тролили українці також французького президента Ф. Олланда за рішення продати Росії авіаносці «Містраль». Інтернет-користувачі масово залишали на його Facebook-сторінці повідомлення такого змісту: «Merci pour le «Mistral» à la Russie, Monsieur Président! Vous aiderez les Ukrainiens à mourir!» («Дякую за «Містраль» для Росії, пане Президенте! Ви допомагаєте українцям померти!»).

Скандальне «емоційне дослідження»

Попри позитиви соціальних мереж, користувачі констатували й несподівано неприємні події. Влітку команда науковців Facebook та вчених з Університету Корнелла (Cornell Universit), Університету Каліфорнії та Сан-Франциско презентувала результати дослідження про те, як емоції, виражені в статусах, можуть «поширюватися» на друзів користувача соціальної мережі. Під час експерименту дослідницька група випадково обрала 689 003 із 1,3 млрд користувачів Facebook та маніпулювала з їхньою новинною стрічкою. У частини людей була відчутно менша кількість позитивних новин, у частини – негативних.

Такі дії науковців викликали шквал критики, скарги до органів контролю з боку правозахисників і навіть спонукали британського регулятора розпочати розслідування. Через кілька місяців від початку скандалу Facebook відповіла на критику, заявивши про внесення змін до правил проведення досліджень та до освітньої програми для інженерів.

Корисні нововведення

Окрім скандалів, найпопулярніша соцмережа світу, яка в цьому році відзначила своє 10-річчя, запам'яталася корисними нововведеннями. Зокрема, було створено Facebook Media – новий ресурс, який допоможе організаціям засобів масової інформації та громадським діячам більш ефективно взаємодіяти із соцмережею. Запрацював також новинний агрегатор FB Newswire, що шукає, збирає та обробляє інформацію, яку публікують користувачі Facebook, і таким чином допомагає журналістам та редакторам швидше знаходити й поширювати цікавий новинний контент.

Чемпіонат світу з футболу – медіаподія року

2014 р. запам'ятався двома великими спортивними подіями – Олімпійськими іграми в Сочі та чемпіонатом світу з футболу у Бразилії. У світі медіа вони запам'яталися не стільки телевізійними рекордами чи цікавими онлайн-проектами, як дуже активним використанням соцмереж.

Олімпіада в Сочі була цікавою не лише спортивними подіями. Напередодні змагань соцмережі заполонили дописи журналістів про умови в тамтешніх готелях. Беззаперечним хітом соціальних мереж стали зображення туалетів із двома унітазами без перегородки.

Чемпіонат світу з футболу натомість запам'ятався рекордами, зокрема в соціальних медіа. CNN навіть назвала цьогорічний чемпіонат «найважливішою подією всіх часів» у соцмережах.

І Facebook, і Twitter фіксували рекорди за кількістю повідомлень. Навіть у Сполучених Штатах Америки, де прийнято вважати більш популярним американський футбол, Мундіаль бив рекорди і перевершив результати фінального матчу Super Bowl ***(Будівська Г. Чим запам'ятався 2014 рік у соцмережах? // MediaSapiens (http://osvita.mediasapiens.ua/web/social/chim_zapamyatavsya_2014_rik_u_sotsmerezhakh/). – 2015. – 2.01).***

***

Названы пять основных трендов в развитии соцсетей в 2015 г. по версии Gigaom, Inc:

Первый состоит в том, что обмен сообщениями перестанет быть просто функцией и перерастет в самостоятельную платформу.

Второй – появятся ветки обсуждений, привязанные к месту их проведения.

Третий – Foursquare умрет как самостоятельная платформа.

Четвертый – появятся приложения, выстроенные вокруг сетей.

Пятый – Instagram, Pinterest и Snapchat начнут устаревать ***(Названы 5 основных трендов в развитии соцсетей в 2015 году // InternetUA (http://internetua.com/nazvani-5-osnovnih-trendov-v-razvitii-socsetei-v-2015-godu). – 2015. – 6.01).***

***

Сервис микроблогов Twitter в скором времени запустит собственный аналог YouTube, сообщает IT Expert со ссылкой на Новое время.

Новый сервис получит название Twitter Video Player, и в нем будет реализована поддержка самых популярных видеоформатов. Однако продолжительность каждого видео не должна превышать 10 мин.

По данным TechCrurch, на Twitter Video нельзя будет размещать пользователям рекламу и редактировать загруженные видео ***(Twitter планирует запустить свой аналог YouTube // IT Expert (http://itexpert.org.ua/rubrikator/item/40369-twitter-planiruet-zapustit-svoj-analog-youtube.html). – 2015. – 7.01).***

***

Социальная сеть Facebook собирается продолжить запуск автономных приложений, по типу Messenger, в следующем году. Об этом сообщил директор по вопросам вертикальной стратегии Д. Бэнкс, рассказывая о планах компании по развитию мобильных приложений в 2015 г.

«Мы отходим от концепции единственного приложения, в котором заключены все функции. В 2014 г. компания выпустила 9 разных приложений и, я предполагаю, что в 2015 г. их выпуск продолжится – по просьбам наших пользователей», – сказал руководитель.

«Пользователям нужно приложение, которое будет отлично выполнять одну функцию. Это – одна из причин того, почему мы отделили Messenger от приложения Facebook и сделали его автономным приложением. Мы сделали то, о чём нам говорили пользователи. Они не хотят кликать два или три раза, чтобы попасть в Messenger… Поэтому, эта тенденция будет ведущей в следующем году, а пользователи увидят ещё больше автономных приложений Facebook», – добавил он.

Ранее аналогичные причины внедрения стратегии запуска отдельных приложений Facebook озвучил CEO компании М. Цукерберг.

«Основное назначение приложения Facebook – новостная лента. Объём сообщений стремительно увеличивался (до 10 млрд в день). Для того, чтобы получить сообщение, пользователю нужно было ждать, пока приложение загрузится, а затем перейти на отдельную вкладку, – сказал руководитель вскоре после запуска приложения Messenger. – Мы видели, что ведущие мессенджеры были отдельными продуктами. Они работали быстро и были сосредоточенными только на обмене сообщениями. Например, пользователь отправляет 15 сообщений в день. Необходимость каждый раз проходить несколько шагов для их отправки вызывает напряжение».

Несмотря на заявления Facebook, ориентация компании на разработку и запуск автономных приложений раздражает пользователей. Вместо ощущения того, что теперь у них есть два приложения, каждое из которых отлично выполняет одну функцию, многие пользователи чувствуют, что теперь они должны иметь два приложения вместо одного, где хорошо работают обе функции.

Теперь пользователям придётся привыкать к нескольким приложениям Facebook на своих мобильных устройствах в том случае, если они хотят получить полный опыт взаимодействия с социальной сетью ***(Facebook продолжит запуск автономных приложений в 2015 году // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_prodolzhit_zapusk_avtonomnyh_prilozheniy_v_2015_godu). – 2015. – 6.01).***

***

Twitter запустил функцию «Пока вас не было» в приложении для iPhone и iPad

Пользователи Twitter часто жалуются на то, что пропускают интересные твиты, находясь в оффлайне. Чтобы вернуться к моменту, когда человек ушел из сети и просмотреть новостную ленту, нужно пролистать десятки твитов, что не слишком удобно. Новая функция Twitter решает эту проблему.

Сервис микроблогов запустил в iOS-приложении функцию «Пока вас не было» (While you were away), которая выделяет актуальные твиты, пропущенные пользователем. Для людей, которые не успевают следить за своей лентой, система автоматически собирает все популярные твиты в специальный раздел. Сервис основывается на данных о пользователях, на которых подписан человек и на информации, которой он обычно интересуется.

Функция «Пока вас не было» является одним из шести нововведений, которые запланировал Twitter. В ближайшее время компания намерена улучшить систему личных переписок, оптимизировать технологию привлечения новых пользователей, расширить возможности геолокационных функций. В 2015 г. Twitter планирует увеличить темп, с которым появляются новые возможности.

На сегодняшний день функция «Пока вас не было» работает в тестовом режиме и пока доступна не для всех пользователей. Ее полномасштабный релиз состоится в ближайшие недели ***(Twitter запустил функцию «Пока вас не было» в приложении для iPhone и iPad // InternetUA (http://internetua.com/Twitter-zapustil-funkciua--poka-vas-ne-bilo--v-prilojenii-dlya-iPhone-i-iPad). – 2015. – 3.01).***

***

Facebook запустит собственный видеосервис до конца января

Новый сервис появится в социальной сети до конца января. По сообщению израильского телеканала 9TV, в Facebook можно будет размещать и просматривать видеоматериалы.

По формату плейлисты видеосервиса будут похожи на плейлисты YouTube. Модераторы групп и сообществ на соответствующих бизнес-страницах получат доступ к видеоконтенту.Пользователи смогут видеть все видео по теме, доступные для онлайн-просмотра, и один ролик в увеличенном размере с возможностью комментирования в режиме реального времени ***(Facebook запустит собственный видеосервис до конца января // InternetUA (http://internetua.com/Facebook-zapustit-sobstvennii-videoservis-do-konca-yanvarya). – 2015. – 9.01).***

***

2014 – год окончания эры социальных сетей?

Венчурный финансист Ф. Уилсон убежден, что в 2014 г. «завершилась социальная стадия Интернета». Конечно, социальными сетями пользуются и еще долго будут пользоваться, однако в ушедшем году произошла одна важная вещь: по количеству пользователей социальные сети почти сравнялись с программами для обмена сообщениями, они же мессенджеры.

Последние три года рост четырех крупнейших социальных сетей замедляется. Если же взять четыре крупнейших мессенджера, то их рост, напротив, ускоряется, и в 2014 г. они почти сравнялись на отметке в 2 млрд пользователей. В следующем году, если не произойдет ничего экстраординарного, мессенджеры обгонят социальные сети и уйдут в большой отрыв. Это серьезная веха, которая знаменует смену правил игры в сфере социального взаимодействия пользователей Интернета.

В чем здесь дело? Все больше людей предпочитают общаться с друзьями и родственниками не в социальных сетях, как раньше, а с помощью мессенджеров. Другая причина упадка социальных сетей – опасения из-за проблем с безопасностью и сбора данных. Так, крупнейшую социальную сеть Facebook подавляющее большинство пользователей, а именно 91 %, считают небезопасной и незаслуживающей доверия. Кто-то просто находит мессенджеры более удобными в использовании, особенно на мобильных

устройствах. Наконец, многие молодые пользователи считают Facebook и Twitter скучными.

Впрочем, для Facebook здесь есть и хорошие новости, ведь, помимо одноименной сети, она владеет также популярнейшей фотосетью Instagram и двумя самыми популярными мессенджерами: Facebook Messenger и WhatsApp. Возможно, залогом выживания социальных сетей в наступившем году (и последующих) станет умение диверсифицировать бизнес ***(2014 – год окончания эры социальных сетей? // InternetUA (http://internetua.com/2014---god-okoncsaniya-eri-socialnih-setei). – 2015. – 3.01).***

***

LinkedIn совершенствует площадку для профессионалов

По официальному заявлению руководства социальной сети для профессионалов LinkedIn, на ее страницах в настоящее время уже разместилось более 1 млн заметок, которые были опубликованы на основе ее издательской платформы.

Издательское отделение, открытое год назад на английском языке, стало доступно для всех жителей США, являющихся пользователями соцсети. Статистика показывает, что еженедельно на страницах этой платформы появляется около 40 тыс. постов.

Данные сервиса WordPress, опубликованные в начале недели, свидетельствуют, что его издательская платформа стала базой для публикации 556 млрд заметок в блогах, что в среднем составляет более полутора миллионов постов ежедневно. Никто не мог подумать, что издательская платформа сети LinkedIn покажет столь значительные результаты на первом году своей деятельности, однако разрыв с сервисом WordPress на данном этапе развития более, чем очевиден.

В плане доступности рынков сеть LinkedIn имеет более ограниченные возможности, но она работает над изменением ситуации. В настоящее время ведутся работы над открытием платформы для всех пользователей сети во всех странах мира, где в список официальных языков общения входит английский. Таким образом доступ к издательской платформе получают 230 из 330 млн участников. Жители других стран смогут присоединиться к сообществу в ближайшие несколько месяцев, что значительно увеличит продуктивность ресурса в 2015 г.

По словам одного из представителей ресурса А. Котари, публикация заметок на страницах LinkedIn – отличный способ продемонстрировать свою компетентность в области современной научной мысли, обменяться опытом с единомышленниками и получить ряд ценной информации от ведущих профессионалов в своей области.

Функционал платформы позволяет публиковать посты, делиться полученными знаниями с группой людей с помощью иконок популярных соцсетей, вести диалог с заинтересованными лицами и даже иллюстрировать свои заметки изображениями, графиками, видеосюжетами.

Летом 2014 г. сервис приобрел службу Newsle, которая поддерживает подключение к LinkedIn аккаунтов из Facebook и адресную книгу Gmail с целью отслеживания постов, которые упоминаются на просторах социальных площадок ***(LinkedIn совершенствует площадку для профессионалов // Бизнес онлайн (http://b-online.ru/socnetwork/2097-linkedin-sovershenstvuet-ploschadku-dlya-professionalov.html). – 2015. – 9.01).***

***

Популярная социальная сеть «Одноклассники» запустила удобный безостановочный режим просмотра видеороликов «НОН-СТОП».

Как отмечают администраторы соцсети, такое нововведение является новогодним подарком всем пользователям «Одноклассников», которые сталкивались с неудобством просмотра видеороликов на сайте, в частности, с необходимостью постоянно переключаться между видео, что довольно неудобно.

Особенностью режима «НОН-СТОП» на «Одноклассниках» является факт того, что видеоролики при просмотре теперь будут идти один за другим.

По сути, у пользователя нет необходимости каждый раз нажимать на кнопку просмотра, дабы включить просмотр следующего видеоролика канала либо эпизода сериала.

Включить или выключить новый режим автовоспроизведения можно будет при помощи специальной кнопки-стрелочки, расположенной в правом верхнем углу страницы ***(«Одноклассники» обзавелись новым режимом просмотра видео «НОН-СТОП» // Дэлайт новости (http://delate.info/39453-odnoklassniki-obzavelis-novym-rezhimom-prosmotra-video-non-stop.html). – 2015. – 4.01).***

***

В России появилась новая социальная сеть для обмена мнениями

Социальная сеть FactCloud полностью разработана российскими программистами. Инновационный проект работает в режиме бета-теста и в дальнейшем планирует составить конкуренцию «ВКонтакте», Twitter и Facebook.

FactCloud кардинально отличается от других социальных сетей. На сайте отсутствует система личных сообщений и комментариев. Разработчики намеренно ограничили функционал портала, сделав ставку на сервисы, недоступные в других социальных сетях.

Основным способом общения в FactCloud является полилог. Пользователи новой социальной сети могут обмениваться короткими фактами в общем информационном облаке. Структуризация данных происходит с помощью рубрик, тем, меток и рейтинга.

FactCloud работает под слоганом «Стань лидером мнений». В социальной сети каждый пользователь может высказать свое мнение, которое, возможно, поддержат миллионы других людей.

Каждая тема, созданная в облаке, получит множество отзывов, среди которых найдутся популярные мнения, достоверная информация, а также интересные факты. Разработчики говорят о том, что на сайте можно ставить «дислайки». Система оценивания позволит отсеять непопулярные мнения и оставить только полезную информацию.

В FactCloud нет настроек приватности, социальная сеть работает в открытом режиме. Основатель сети, полностью разработанной в России, считает, что продукт будет популярен не только в России, но и по всему миру. По словам С. Мельникова, успех проекта будет напрямую связан с тем, что в Росси ценятся не деньги, а человеческие убеждения.

Присоединиться к новому проекту можно на factcloud.com ***(В России появилась новая социальная сеть для обмена мнениями // Newsland (http://newsland.com/news/detail/id/1478954/). – 2015. – 29.12).***

***

ComScore скорректировала ранее объявленные цифры посещаемости соцсетей: по уточненным данным, «Одноклассникам» не удалось опередить «ВКонтакте» по числу уникальных пользователей сайта.

По сведениям comScore, у «ВКонтакте» в ноябре было 57,6 млн уникальных пользователей веб-версии, у «Одноклассников» – 52,1 млн (по первоначальным данным – 61,1 млн). В эти данные не включены посещения с мобильных устройств.

«Любой аналитик понимает, что скачок посещаемости одного сайта за месяц на 9 млн человек невозможен ни при каких условиях. Мы рады, что коллеги из comScore оперативно исправили очевидную ошибку», – прокомментировал результаты представитель «ВКонтакте» Г. Лобушкин.

В comScore пояснили «Известиям», что эта служба стремится максимально точно измерять в Интернете поведение людей, а не машин. Когда человек просматривает одну страницу сайта, совершается много вызовов от браузера к серверам просматриваемого сайта и многим другим серверам, что и создает риски для точности измерений. Чтобы правильно учитывать поведение именно человека, а не машины, нужно среди всего набора вызовов выделить один валидный. «В данном случае часть невалидного трафика была засчитана как валидный, что впоследствии было проанализировано, и вы получили уточненные данные», – сообщили в comScore.

Согласно данным другого статистического сервиса – TNS, количество уникальных пользователей «ВКонтакте» в ноябре составило 54,6 млн, у «Одноклассников» – 40,1 млн. По статистике LiveInternet, в ноябре количество уникальных пользователей «ВКонтакте» (суммарно – с обычных

компьютеров и мобильных устройств) составило 65,3 млн человек, у «Одноклассников» – 44,9 млн.

По словам главы сайта знакомств «Теамо.ру» А. Бурина, интернет-компании простят неточность крупнейшему аналитическому порталу. comScore является почти монополистом в своем сегменте. На данные этой службы ссылаются многие публичные компании.

До 2008 г. социальная сеть «Одноклассники» была самой популярной в России. Но затем новое руководство компании активно занялось монетизацией различных сервисов. В частности, регистрация нового пользователя в «Одноклассниках» стала платной. Тогда компания объяснила это возросшим количеством аккаунтов, распространяющих спам. После этого приток новых пользователей в соцсеть сильно уменьшился. Осенью 2008 г. «ВКонтакте» по посещаемости опередила «Одноклассников» – и с тех пор сохраняла первенство ***(«ВКонтакте» снова популярнее «Одноклассников» // InternetUA (http://internetua.com/vkontakte--snova-populyarnee--odnoklassnikov). – 2015. – 1.01).***

***

Аудитория крупнейшей в мире социальной сети Facebook постепенно взрослеет, в то время как молодежь переключается на другие сервисы, пишет IT Expert со ссылкой на Газету.ру.

Facebook предсказуемо оказался самым популярным социальным интернет-сервисом среди американцев солидного возраста. Согласно опросу, проведенному исследовательской компанией Pew Research среди 2 тыс. жителей США старше 18 лет, активные аккаунты Facebook есть у 56 % американских интернет-пользователей старше 65 лет или у 31 % американцев этого возраста.

Facebook – это «базовая» социальная сеть, которая остается самой популярной среди владельцев страниц только в одном из таких сервисов, и при этом ее аудитория существенно пересекается с другими платформами, отмечают аналитики.

За последний год доля жителей США, пользующихся Facebook, практически не изменилась, как не изменились и показатели по отдельным демографическим группам. Популярность Facebook заметно увеличилась только среди самых старших пользователей Интернета.

У конкурентов Facebook дела обстоят иначе.

«Все другие социальные медиа, которые мы исследовали, продемонстрировали значительный рост с 2013 по 2014 г. Instagram не только увеличил число пользователей на 9 %, но и продемонстрировал рост практически в каждой демографической группе», – отмечается в исследовании.

Социальная сеть для обмена профессиональными контактами LinkedIn продолжает становиться все популярнее в тех демографических группах, которые изначально составляли большую часть ее пользователей, то есть

высококвалифицированных специалистов и людей с высшим образованием. В то же время популярность Twitter и Pinterest растет сразу у многих групп американцев.

Несмотря на повзрослевшую аудиторию, Facebook явно не страдает от недостатка трафика. Его роль в жизни уже существующих пользователей становится все важнее: по данным Pew, 70 % американцев заходят в эту соцсеть ежедневно, а 45 % – несколько раз в день.

Facebook теряет популярность только среди самой молодой части пользователей Интернета – подростков. Согласно исследованию, проведенному аналитической компанией Frank N. Magid Associates, в 2014 г. доля американских тинейджеров от 13 до 17 лет, которые активно пользуются Facebook, составила 88 %. Еще годом ранее эта доля составляла 94 %, а в 2012 г. – 95 %.

«Подросткам нравится Twitter, потому что в нем меньше взрослых, меньше родителей и меньше сложностей. Конечно, дети не удаляют свой аккаунт в Facebook, однако они проводят там значительно меньше времени, чем в Twitter, Instagram или Tumblr», – рассуждает исследователь Pew Research А. Ленхарт.

При этом руководство Facebook отрицает снижение популярности соцсети среди молодежи. В ноябре 2013 г. СОО Facebook Ш. Сэндберг заявила, что «подавляющее большинство подростков в США пользуются Facebook, и большинство подростков в США используют Facebook почти каждый день» ***(Типичный пользователь Facebook – уже давно не подросток и не студент // IT Expert (http://itexpert.org.ua/rubrikator/item/40433-tipichnyj-polzovatel-facebook--uzhe-davno-ne-podrostok-i-ne-student.html). – 2015. – 12.01).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

5 січня в Інтернеті стартувала міжнародна інтернет-акція на підтримку української льотчиці, народного депутата від партії «Батьківщина» Н. Савченко, яку в Росії звинувачують у загибелі журналістів каналу «Россия 1». Про це повідомляє «Радіо Свобода».

Активісти створюють і поширюють у мережах Twitter і Facebook фото- та відеоматеріали з інформацією про Н. Савченко різними мовами і поширюють її з хештегом.

Twitter-шторм активно підтримують адвокати української військовополоненої М. Фейгін і М. Полозов.

До Twitter-шторму долучаються також посольства України в різних країнах світу. Зокрема, повідомлення з інформацією про військовополонену Н. Савченко розмістили на своїх сторінках посольства України у Великобританії, Македонії, Японії, Вірменії, Кувейті та Посольство України при Святому Престолі (Ватикан).

Також до акції приєднався Посол США в Україні Д. Пайєтт.

Нагадаємо, 25 грудня Верховна Рада звернулася до міжнародних організацій та міжпарламентських асамблей щодо звільнення українського пілота Н. Савченко та включила її до складу постійної делегації України в Парламентській асамблеї ради Європи (ПАРЄ).

Раніше адвокат льотчиці М. Фейгін повідомив, що Н. Савченко має намір голодувати до 26 січня 2015 р. – дати, коли розпочинається сесія Парламентської ради Європи (ПАРЄ) у Страсбурзі (Франція). Якщо вона вступить у повноваження делегата ПАРЄ від України і набере дипломатичній імунітет, російська влада повинна її відпустити з-під варти, каже адвокат.

Н. Савченко заявила, що визнає себе виключно військовополоненою і політв'язнем. Її продовжують звинувачувати в загибелі журналістів телеканалу «Россия 1», хоча адвокати доводять алібі льотчиці та її непричетність до загибелі кореспондентів.

З набуттям Н. Савченко дипломатичного імунітету як делегата ПАРЄ, РФ не матиме права утримувати українську громадянку у СІЗО і переслідувати її у кримінальній справі ***(У світі почався Twitter-шторм за звільнення Надії Савченко #FreeSavchenko // UAINFO (http://uainfo.org/blognews/471412-u-svt-pochavsya-twitter-shtorm-za-zvlnennya-nadyi-savchenko-freesavchenko.html). – 2015. – 5.01).***

***

У соціальній мережі Facebook з'явилася спільнота «Защита Кировоградского Лесопарка». Активісти та журналісти створили її з метою координації дій на захист кіровоградської лісопаркової зони та протидії її забудові і вирубці дерев ***(У Facebook з'явилася спільнота на захист кіровоградського лісопарку // Весь Кіровоград (http://www.kirovograd.net/shortly/2015/1/8/u_facebook_zjavilasja_spilnota_na_zahist_kirovogradskogo_lisoparku.htm). – 2015. – 8.01).***

***

#JeSuisCharlie стал одним из самых популярных хэштегов в истории Twitter, сообщили представители сервиса.

Хэштег был проявлением солидарности пользователей с сотрудниками французского сатирического журнала Charlie Hebdo.

На своем пике 8 января вечером создавалось около 6 тыс. твитов в минуту с этим хэштегом. По данным сервиса, всего пользователи отправили более 5 млн твитов с упоминанием #JeSuisCharlie ***(Один из самых популярных хэштегов в истории Twitter // InternetUA***

(http://internetua.com/odin-iz-samih-populyarnih-heshtegov-v-istorii-Twitter). – 2015. – 11.01).

***

LiveJornal опубликовал рейтинги за 2014 г.: по тегам, сообществам, блогерам, записям. И самым популярным словом в LiveJornal оказалась… «Украина»! Именно «Украина» интересовала пользователей сервиса больше всего – это ключевое слово использовалось свыше 250 тыс. раз. На втором почетном месте «фото» и только на третьем – «Россия», 177 и 154 тыс. соответственно. Популярными тегами стали: «музыка», «история», «Крым», «видео», «война», «юмор» и «политика».

Наиболее «почитаемые» блогеры – А. Лебедев, Л. Миро и И. Варламов. В топ среди сообществ вошли «Пора валить? Эмиграция из России», «Чрезвычайное происшествие» и «Сами себе психологи».

Записью года, которая определялась по количеству просмотров, стала – «Как не надо снимать свадьбу». Подборка фотографий из самых «удачных» свадебных снимков привлекла внимание 2 млн человек. Отдельное спасибо фотографам, проявившим недюжинную «креативность» и молодоженам, уверенным в своих способностях шикарно позировать. «Что в действительности произошло в Одессе вчера» – больше миллиона просмотров и второе место. Запись рассказывает о трагических весенних событиях, забравших жизни 40 человек в Украине. На третьем месте – славное достояние В. Януковича, пост, получивший название «Межигорье, музей коррупции» и собравший 600 тыс. визитов ***(«Живой журнал»: рейтинги 2014 года // Uinny (http://uinny.ru/index.php?id=1566). – 2015. – 30.12).***

***

Після трагедії 13 січня під Волновахою, де бойовики розстріляли з «Градів» пасажирський автобус, у соцмережах розгорнулася акція «Я – Волноваха».

Акція проводиться за аналогією з акцією «Я – Шарлі», що почалася після трагедії в Парижі, де терористи розстріляли редакцію сатиричного видання «Шарлі Едбо».

Ініціатором української акції став Д. Корчинський, який першим розмістив своє фото з написом «Я – Волноваха».

Нагадаємо, 13 січня відбувся артилерійський обстріл пасажирського автобусу під Волновахою, у результаті якого загинуло 12 мирних жителів і 18 було поранено.

Також нагадаємо, держдепартамент США поклав на Росію провину за обстріл автобуса поблизу Донецька. Про це заявила офіційний представник відомства М. Харф ***(У соцмережах почалася акція «Я – Волноваха» // Вісник Кременчука (http://vestnik.in.ua/news/20832-u-socmerezhah-pochalasya-akcya-ya-volnovaha.html). – 2015. – 14.01).***

***

У соцмережі шириться флеш-моб «Мій Симоненко»

До 80-річчя черкаського поета в соцмережі Facebook оголосили поетичний флешмоб «Мій Симоненко». Його мета: вустами простих людей прочитати усі вірші В. Симоненка.

Учасники флеш-мобу передають один одному естафету, так як це було в кампанії Ice Bucket Challenge. Потрібно зняти на відео і викласти в мережу декламацію вірша, який сподобався. Треба передати естафету трьом друзям, а відповісти на поетичний виклик потрібно не пізніше 3 діб.

«Ніяких покарань. Бо саме у віршах він "воскрес, щоб знову з нами жити"», – зазначають організатори акції ***(У соцмережі шириться флеш-моб "Мій Симоненко" // ДЗВІН (http://dzvin.org/u-sotsmerezhi-shyrytsya-flesh-mob-mij-symonenko/). – 2015. – 13.01).***

***

Крупнейшая в мире соцсеть Facebook начала демонстрировать пользователям в США сообщения о детях, пропавших в районе их проживания. Об этом сообщается в корпоративном блоге Facebook.

Инициатива запущена в рамках партнерства Facebook с организацией National Center for Missing and Exploited Children, которая занимается в США поиском пропавших детей или детей, подвергшихся насилию.

Сначала полиция определяет, можно ли включить тот или иной случай пропажи ребенка в систему оповещения AMBER Alert. Далее центр выпускает оповещение о пропаже ребенка, которое попадает в систему Facebook.

Facebook покажет сообщение в ленте новостей тех пользователей, которые живут в зонах, где ведется поиск. Оповещения на Facebook будут содержать фотографию и подробную информацию о пропавшем ребенке, а отображаться будут как в десктопной версии соцсети, так и в мобильных приложениях.

Количество сообщений, которые видит тот или иной пользователь, будет зависеть от числа оповещений AMBER Alert в месте его проживания. Звуковые сигналы на мобильных не будут срабатывать на эти оповещения.

«Годами люди использовали Facebook, чтобы публиковать новости о пропавших детях и оповещения AMBER. В некоторых случаях кто-то видел запись или фото в ленте новостей и предпринимал действия, в результате которых ребенок был найден», – говорится в блоге.

Система AMBER Alert – система оповещения о пропаже детей в США и Канаде, подразумевающая распространение информации самыми разными способами: через радиостанции, телеканалы, электронную почту, смс, информационные табло. В Facebook отметили, что благодаря системе AMBER Alert с 1996 г. были найдены 728 пропавших детей, и что механизм распространения информации в соцсети потенциально позволит повысить

число успешных поисковых операций ***(Facebook покажет в ленте новостей сообщения о пропавших детях // InternetUA (http://internetua.com/Facebook-pokajet-v-lente-novostei-soobsxeniya-o-propavshih-detyah). – 2015. – 14.01).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Почти каждый год новые тренды появляются для социальных медиа. Пришло время посмотреть на самые ожидаемые тренды в социальных медиа для 2015 г.

Социальных медиа будут адаптированы для мобильных девайсов

Этот тренд начался несколько лет назад и продолжится в 2015 г. Все больше пользователей заходят в социальные медиа через мобильные девайсы. Поэтому социальные платформы будут адаптировать свои сервисы под мобильные деваайсы.

Появятся новые приложения для платформ, чтобы облегчить доступ потребителей к социальным медиа.

Возрастет популярность фото

Использование фото в социальных медиа значительно возрастет. Известный факт, что визуальный контент легче запомнить. В 2015 г. компании будут использовать больше фото для того, чтобы рассказать о своем бизнесе.

Возрастет популярность маркетинга с помощью коротких видео

Видеомаркетинг будет одним из самых важных форм маркетинга на платформах социальных медиа в 2015 г.

Компании будут создавать короткие, но информационные видео о своих продуктах и услугах. И это станет лучшим способом связаться со своей целевой аудиторией за короткое время. Интерактивные видео будут задавать тон. Такие сайты как Instagram станут более популярными в следующем году.

Вирусный маркетинг станет более желанным

Онлайн-мир уже испытал силу вирусного маркетинга. Это лучший способ получить массу шейров, которые помогают донести сведения о компании большому количеству пользователей.

В 2015 г. больше компаний будут создавать контент, который станет вирусным.

Компании будут использовать маркетинг в реальном времени, чтобы обслужить своих потребителей

Социальные медиа – это прекрасная платформа для компании напрямую связаться со своим потребителями. Большинство компаний будут

использовать эту возможность на полную. Концепция маркетинга в реальном времени станет все более популярной.

Поэтому бренды должны быть в своих активностях. Кроме того, они должны реагировать как можно быстрее на комментарии и вопросы, которые их потребители размешают в социальных медиа.

LinkedIn и Instagram станут самыми популярными платформами

LinkedIn и Instagram станут наиболее популярными среди других платформ. В то время как LinkedIn должна стать наиболее важной платформой для B2B аудитории, много пользователей будут использовать Instagram для B2C коммуникаций. Instagram станет одной из самых важных платформ для распространения видео. Кроме того, компании будут относиться к LinkedIn более серьезно в будущем.

Креативность станет ключом к успеху

Независимо от того, сколько времени вы проводите в социальных медиа, вы не получите результата, если вы не будете креативными. Вы не можете ожидать от аудитории, что они будут отвечать на ваши сообщения, если они шаблонные и старые. Вместо этого, подумайте о чем-то нестандартном. Когда контент креативный, он достаточно уникальный, чтобы привлечь многочисленных пользователей.

Другие социальные платформы, такие как Twitter и другие, останутся релевантными в 2015 г. Но компаниям придется потратить больше денег, чтобы их реклама появилась на таких платформах как Facebook. Поэтому компаниям нужно значительно увеличить свой бюджет на маркетинг в социальных медиа на 2015 г. Кроме того, они также будут использовать социальные медиа как идеальную платформу для стимулирования бизнес-доходов ***(Топ-7 трендов социальных медиа в 2015 году // Marketing Media Review (http://mmr.ua/news/id/top-7-trendov-socialnyh-media-v-2015-godu-42462/). – 2015. – 6.01).***

***

Специалисты Facebook по мере приближения нового года предлагают задуматься о том, как тенденции уходящего года повлияют на маркетологов в наступающем году. Специалистам маркетинга 2015 г. принесет более персонализированное взаимодействие с клиентами, использование более точных инструментов измерения и полный охват быстрой мобильной экспансии во всем мире.

В 2015 г. мобильные устройства будут продолжать привлекать большую долю внимания потребителя. Этот сдвиг создал новое пространство в обыденной жизни людей, которое изменяет способ потребления СМИ. У пользователей появился более широкий выбор – больше изображений, новостей и видео, а также новый способ осуществления покупок с множеством новых вариантов открытия новых продуктов.

Реклама должна быть сосредоточена на вовлечении людей в это новое пространство разнообразными способами, не ограничиваясь одним местом

или опытом. Цифровая реклама станет из измеримой по-настоящему объяснимой. Основные формы измерения, основанные на кликах, дают слишком мало информации. С более масштабными, точными новыми средствами измерений маркетологи смогут понять, что сработало, и сосредоточиться на том, что важно для их бизнеса: на показателях бренда и продажах.

Выиграют организации, которые применяют более индивидуальный подход. Маркетологи имеют больше информации и инструментов для создания соответствующих кампаний, чем когда-либо прежде, и люди все чаще ожидают увидеть релевантные объявления по всем каналам. По данным eMarketer, только 5 % маркетологов на стороне клиента по всему миру сообщили, что они широко внедряют персонализацию.

Сообщения станут ключевой частью непосредственного взаимодействия предприятия с клиентами. Диалог в режиме реального времени важен для быстрого удовлетворения текущих потребностей клиентов. Поскольку все больше людей продолжают стремиться к связи с помощью сообщений, организации откроют этот новый канал коммуникации для поддержания конструктивного диалога с сотрудниками и клиентами.

Рост мирового населения обеспечивается за счет развитых стран, и процесс продолжится в течение следующих 10 лет, причем большая часть этого роста будет происходить в странах за пределами США. По данным eMarketer, в ближайшие 3 года уровень проникновения сотовой связи возрастет с 61,1 % до 69,4 % от общей численности населения. Поскольку все больше людей впервые становятся обладателями мобильных устройств, организации и маркетологи будут следовать за ними ***(Facebook опубликовал цифровой маркетинговый прогноз на 2015 год // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_opublikoval_tsifrovoy_marketingovyy_prognoz_na_2015_god). – 2014. – 31.12).***

***

Социальная сеть Pinterest объявила о том, что 1 января 2015 г. программа «Продвигаемые пины» будет расширена на рекламодателей во всём мире.

Бета-версия рекламных пинов была запущена восемь месяцев назад. Функционал был доступен лишь ограниченному числу брендов в США. По информации компании, во время тестового периода продвигаемые пины работали так же эффективно, а иногда даже лучше, чем органические.

Бренды, принявшие участие в программе, увидели 30 % увеличение «заработанных» медиаканалов – количества пользователей, сохранивших продвигаемый пин на одной из своих досок. В среднем, на один продвигаемый пин приходилось 11 перепостов, аналогично органическому пину. Более того, пользователи продолжали сохранять платные пины на

своих досках через месяц после окончания кампании. Показатель роста «заработанных» медиаканалов в этот период составлял 5 %.

По словам представителей сервиса, как только программа «Продвигаемые пины» будет запущена, рекламодатели получат доступ к бóльшему количеству рекламных форматов, а также к продвинутому функционалу таргетинга. Кроме того, компания также запускает Pinstitute – обучающую программу, которая научит рекламодателей использовать преимущества продвигаемых пинов посредством воркшопов и вебинаров.

Запуск Pinsitute последовал за внедрением панели управления «Аналитика» в августе этого года, которая позволяет рекламодателям отслеживать производительность своих пинов и то, какая часть контента их сайтов была сохранена пользователями посредством кнопки «Pin It».

Пилотная программа «Продвигаемые пины» была запущена в сентябре 2013 г. В мае 2014 г. Pinterest приступил к тестированию рекламных пинов небольшой группой рекламодателей в США.

В сентябре компания сообщила о том, что она работает над повышением релевантности продвигаемых пинов для пользователей, а также над разработкой инструментов, которые помогут рекламодателям увидеть, как реклама в сервисе влияет на их бизнес ***(Pinterest запускает продвигаемые пины для всех рекламодателей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_zapuskaet_prodvigaemye_piny_dlya_vseh_reklamodateley). – 2015. – 6.01).***

***

Facebook объявил о том, что его видеоплатформа возросла на 75 % глобально. Социальная сеть отметила, что видеоплатформа растет и количество видео, производимого брендами и размещаемого в лентах, увеличилось в 3,6 раз по сравнению с прошлым годом, сообщает Marketing Media Review (http://mmr.ua/news/id/kolichestvo-video-v-facebook-vyroslo-na-75-42782/).

В декабре социальная сеть показала, что количество просмотров на ее платформе рекламной кампании John Lewis превысило просмотры на YouTube.

Глобальное digital-агентство Metia выпустило статистику, в которой показало, что 75 % владельцев смартфонов смотрят видео на своих дейвасах 2–3 раза в день.

К 2017 г. Metia прогнозирует, что онлайн-видео составит почти 70 % потребительского интернет-трафика. С такими прогнозами не удивительно, что социальные платформы пустились в путешествие, чтобы взять на вооружение преимущества успеха от видео ***(Количество видео в Facebook выросло на 75 % // Marketing Media Review (http://mmr.ua/news/id/kolichestvo-video-v-facebook-vyroslo-na-75-42782/). – 2015. – 12.01).***

***

Американский стартап SpotItBuyIt из Филадельфии планирует помочь своим бизнес-клиентам использовать их аккаунты в популярном сервисе Instagram в качестве платформы мобильной электронной коммерции, сообщает itexpert.org.ua со ссылкой на Payspacemagazine и Philadelphia Daily News.

Основатели стартапа всегда сотрудничали с небольшими розничными торговцами и пришли к выводу, что сервис Instagram становится все более популярным во всем мире. Поэтому они решили помочь торговцам конвертировать мобильный трафик в Instagram в реальных клиентов.

«Мы достигнем этого путем создания мультиканального, оптимизированного к мобильным устройствам продукта, который подключается к веб-сайту компании», – сообщила генеральный директор SpotItBuyIt Э. Берлинер.

SpotItBuyIt начал тестировать свой сервис в ноябре 2014 г., а уже в декабре 50 предприятий подключили бета-версию решения. После завершения этапа тестирования компания планирует взимать 20 дол. за использование сервиса и дополнительный процент с каждой транзакции (предположительно 3 %) ***(В Instagram займутся электронной коммерцией // Media бізнес (http://www.mediabusiness.com.ua/content/view/42031/118/lang,ru/). – 2015. – 13.01).***

***

Twitter планирует существенно расширить рекламный охват и намерен показывать объявления пользователям, которые не посещают сервис. На конференции CES в Лас-Вегасе представители Twitter анонсировали скорый запуск обновленной страницы выхода, где пользователям будет предлагаться партнёрская реклама продуктов и услуг с учётом интересов людей.

Также на конференции CES были озвучены и другие планы Twitter, связанные с продажей рекламы. В частности, разработчики Twitter представили издателям новую возможность Instant timeline. Издатели могут встраивать тематические ленты твитов к себе на сайты и транслировать публикации по релевантным темам пользователям в режиме реального времени. Реклама из твитов также будет показываться в ленте.

По заявлению руководства сервиса, каждый месяц контент Twitter потребляют до 500 млн интернет-пользователей, в то время как месячная аудитория активных пользователей сервиса составляет 284 млн человек. Таким образом, сегодня для Twitter важно показывать рекламу не только тем, кто зарегистрирован на сервисе и посещает его, но и сторонним пользователям. Именно к этому и будут сводиться дальнейшие рекламные инициативы компании.

«Компания планирует продавать рекламу в потоках сообщений, которые транслируются в лентах, встраиваемых на сторонние сайты и в

приложения. Представители Twitter уже выступили с этой инициативой перед ключевыми медиабаерами на Consumer Electronics Show», – сообщает The Wall Street Journal ***(Twitter начнёт показывать рекламу на сторонних площадках незарегистрированным пользователям // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/42038/118/lang,ru/). – 2015. – 13.01).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Австралійські фахівці провели унікальне соціологічне дослідження, підсумки якого показали, що людина в сучасних умовах може легко прожити без живого спілкування.

Провідні фахівці зазначили, що на сьогодні безліч людей не потребує дружньої розмови. Завдяки нинішнім технологіям, жінки і чоловіки із задоволенням спілкуються в спеціальних соціальних мережах, використовуючи при цьому мобільні телефони, комп'ютери або планшети. Такого висновку група дослідників дійшла після того, як їм став відомий результат проведеного експерименту. Згідно з підсумками опитування, людині достатньо мати лише пару знайомих, які час від часу будуть вносити різноманітності в його життя.

Повідомляється, що дослідження вчених з Австралії тривало більше 20 років. За цей час науковці детально вивчили поведінку юних дівчат і хлопців. При цьому у випробуваннях була задіяна аудиторія, що складається з 400 тис. представників молодого покоління.

Таким чином, група вчених дійшла висновку, що брак живого спілкування заповнюється за допомогою звичайних засобів телекомунікації, тобто Інтернету ***(Вчені: Сучасні технології можуть замінити друзів // Перші Інтелектуальні Новини України (http://pinu.com.ua/novyny/it/11-01-15/vcheni-suchasni-tehnologiyi-mozhut-zaminiti-druziv). – 2015. – 11.01).***

***

Около двух третей пользователей социальных сетей признают, что зависимы от них. По крайней мере такие данные следуют из опроса, проведенного по заказу сайта Pencourage.

Все эти пользователи делают фотографии, главным образом, для того, чтобы разместить их в Facebook или в Instagram. Они также признают, что

посты в соцсетях могут заставить их чувствовать себя обиженными, униженными и завистливыми. Что поделать, паранойя – частый спутник Facebook-наркоманов.

Вот еще парочка фактов о том, что происходит с людьми, которые не ограничивают время, которое тратят на социальные сети.

Цифровая амнезия

Доктор философии и клинический психолог Р. Шерри говорит, что люди, которые чрезмерно увлекаются социальными сетями, зачастую в состоянии запомнить только те события из своей жизни, о которых написали в постах. Более того, в памяти остаются только те сообщения, которые собрали больше всех лайков.

Так что когда Facebook предлагал всем нам в конце года посмотреть, чем он нам должен был запомниться, большинство из нас поймало себя на мысли, что кроме того, что отражено в ленте, и вспомнить-то нечего.

Мы идентифицируем себя в соответствии со своими аккаунтами в соцсетях. Хотя часто об этом даже не подозреваем. То, что не отображено в вашей ленте, не существует. По этой причине когда возникает ситуация, при которой нам на несколько дней приходится отказываться от Интернета, у нас наблюдаются приступы паники, тревоги и печали.

«Когда люди отключены от Интернета, то фактически не способны выразить себя», – заключает профессор. И добавляет: хуже всего в таких ситуациях чувствуют себя те, кто играет в соцсетях в игры.

Мы охотимся за негативными новостями

Исследование университета Мичигана доказало, что люди в Twitter чаще ретвитят негативные новости. Это приводит к тому, что другие пользователи постят чаще негативные новости. Вследствие этого у людей, которых можно назвать Twitter-маньяками, развивается неадекватное восприятие действительности: мир начинает казаться им черно-белым.

Мы стали очень одиноки...

Еще одно исследование – на этот раз немецкое – доказало, что почти все пользователи Facebook грешат тем, что рассматривают фотографии других пользователей. Результат: разочарование в собственной жизни, зависть, усиленное ощущение одиночества.

Разумеется, все пользователи соцсетей выкладывают только самые классные свои фотографии. Поэтому стороннему наблюдателю кажется, что их жизнь лучше, чем есть на самом деле.

Facebook вытесняет личную жизнь

Недавний опрос, проведенный в Германии учеными Школы бизнеса им. Бута Чикагского университета, показал, что общение в Facebook и Twitter оказалось более непреодолимым искушением, чем сигареты и секс, желание потратить деньги и заняться спортом. В ходе исследования на протяжении семи дней 250 участникам опроса несколько раз в день рассылали сообщения, на которые они должны были ответить – испытывают ли они

какое-либо желание в данный момент, насколько сильное и подчинились ли они импульсу. Социальные сети оказались самыми большим искушением.

Что же делать? Очевидно, придется сократить время пользования социальными сетями. Например, до часа в день. Это будет отличное начало. А вы как считаете? ***(Шиян К. Как Facebook и Twitter делают нас психопатами // Lifter (http://lifter.com.ua/post/526). – 2015. – 9.01).***

***

Социальные сети вызывают зависимость

Чувствуете, что не можете и пяти минут прожить без того, чтобы не заглянуть во «ВКонтакте»? Испытываете раздражение, если Facebook вдруг оказывается недоступен? Возможно вам «повезло» оказаться среди тех, кто подвержен зависимости от социальных сетей.

Мы часто говорим о зависимости от соцсетей, не подозревая, насколько близки к истине. Психологи из Университета в Олбани (США) опубликовали в журнале Addiction статью, в которой утверждают, что от Facebook можно быть зависимым точно так же, как от каких-нибудь химических веществ.

В исследовании участвовали около 300 студентов в возрасте от 18 лет. Подавляющее большинство (90 %) пользовались социальной сетью, проводя в ней примерно треть всего времени, потраченного на Интернет. Все они должны были ответить на вопросы, которые представляли собой тест на алкогольную зависимость, только приспособленный к социальной сети – например, один из вопросов мог звучать как «Насколько хорошо вам бывает от посещения Facebook?»

В результате психологи пришли к выводу, что у 10 % пользователей социальной сети возникают психологические симптомы, сходные с теми, которые возникают при алкогольной зависимости. Разумеется, они часто заходили на страницу Facebook – но, кроме того, если они по какой-то причине не могли этого сделать, у них росло раздражение, и росло тем сильнее, чем дольше человек оставался без любимой социальной сети. У «фейсбукозависимых» развивалась эмоциональная неустойчивость, импульсивность поведения, они хуже контролировали собственные эмоциональные порывы. Кстати говоря, у тех, кто испытывал зависимость от социальной сети, часто бывали ещё и проблемы со спиртным. То есть, как полагают авторы исследования, пристрастие к Facebook облегчает развитие других видов зависимостей.

Всякая зависимость возникает из непомерного чувства удовлетворения, награды, которое наш мозг стремится испытывать ещё и ещё. В социальной сети такие «награды» представлены, что называется, в ассортименте, от «лайков» до уведомлений об обновлении контента. И при том мы не знаем, когда и как произойдёт такое обновление, кто и когда поставит «лайк», а такая неопределённость в ожидании и получении награды сильнейшим образом формирует привычку к повторению каких-то действий, от которой к тому же очень трудно потом избавиться. В случае с социальными сетями

свой вклад вносят мобильные приложения, благодаря которым можно вообще не вылезать из обновлений страницы и новых новостей.

Впрочем, признают ли за «зависимостью от Facebook» право на существование, будет ясно после дальнейших исследований; не исключено, что этот феномен станет частью какой-нибудь более общей, глобально медиазависимости, когда человек уже не мыслит своё существование без новостей, картинок, телевизора, социальной сети и тому подобных вещей ***(Стасевич К. Социальные сети вызывают зависимость // Newsland (http://newsland.com/news/detail/id/1481444/). – 2015. – 5.01).***

Маніпулятивні технології

На одной из популярных фриланс-бирж появилось объявление о поиске пользователей, которые будут оставлять антиукраинские комментарии и разжигать вражду на сайтах в Интернете. Одна из главных задач «работы» – вступать в споры на новостных сайтах, провоцировать других пользователей, навязывать свое мнение и троллить, пишет Watcher.

Согласно описанию «вакансии», главные темы, которыми предстоит овладеть проплаченным троллям, – «ухудшение уровня жизни в Украине, возможный Майдан-3, угнетение русскоязычных жителей, обнищание, карательные операция на Юго-Востоке». Все эти сообщения должны подаваться на фоне того, что в России и Крыму якобы прекрасно живется.

Платить таким «сотрудникам» заказчик обещает от 5 до 15 р. за пост. По его словам, в день авторы «легко получают» 500–700 р. (около 135 грн) ***(Троллей для антиукраинской травли ищут через фриланс-биржу // InternetUA (http://internetua.com/trollei-dlya-antiukrainskoi-travli-isxut-cserez-frilans-birju). – 2015. – 7.01).***

***

Із початку року мережею Facebook знову почали ширитися повідомлення про авторські права і копірайт користувачів на дані, які вони розміщують на власних сторінках, пише видання «ВВС Україна» (http://www.bbc.co.uk/ukrainian/science/2015/01/150109_copyright_in_facebook_sa).

Два роки тому користувачі соцмережі вже піймалися на схожу містифікацію. Чому вони наступають на ті самі граблі вдруге, розмірковує Г. Рубін.

«У відповідь на нову політику Facebook я оголошую, що всі мої персональні дані, фотографії, малюнки, переписка (листування, в т. ч. електронне) і так далі, є об’єктами мого авторського права (згідно Бернської конвенції)», – чи бачили ви такий чи схожий допис на сторінці у котрогось із ваших друзів у Facebook?

Якщо так, то знайте – це обман, що шириться з 2012 р. і ніяк не зникає, як би його не розвінчували.

Деякі варіанти цього допису апелюють до Римської конвенції, деякі – до «Бернерської конвенції», якої взагалі не існує.

Повідомлення припускає, що соцмережа планує привласнювати та продавати опубліковані фото та відео. Але це нонсенс. Facebook не має авторського права на контент своїх користувачів, а може лише поширювати його – у цьому і є суть цього сайту.

За словами речника соціальної мережі Е. Ноєса, за умовами користування, Facebook має право ділитися вашим контентом та поширювати його, проте за бажання ви можете змінити власні налаштування приватності.

«Ми б хотіли скористатися моментом, аби нагадати: коли ви публікуєте фото на Facebook, ми не отримуємо на нього права», – наголошує Е. Ноєс.

«Не звертайте уваги уваги на такі дописи, вони ні на що не впливають, – каже головний редактор видання PC Advisor М. Бревіс. – Не важливо, що ви напишете на своїй сторінці, – ви вже підписалися під умовами Facebook, і якщо він захоче змінити їх, він про це скаже».

Проте користувачі продовжують звертати увагу.

«Це одна з тих речей, які притаманні соцмережам: люди бачать, що їхні друзі говорять про це, і думають, що, напевне, це правда, – каже М. Бревіс. – І, звісно, кожен хоче бути в курсі справи і поширити щось перед тим, як це зроблять інші».

«Люди думають, що Facebook та Google витягують їхні персональні дані, тож навіть ті, кому немає чого приховувати, починають непокоїтися», – продовжує вона.

За її словами, в умовах користування сайтом буває складно розібратися, тож багато хто з нас не читає їх при реєстрації, просто натискаючи на кнопку «Погоджуюся».

Утім, забрати свою згоду вже після того, як ви погодилися з умовами користування соцмережею, неможливо. Єдиний спосіб, у який ви можете заборонити компанії поширювати свої дані, – видалити власний профіль.

Із М. Бревіс погоджується і доктор М. Майкаліс із Центру досліджень соціальних медіа університету Вестмінстера: «Це річ, притаманна соцмережам – коли ви бачите допис від друга, ви схильні йому вірити. Дописи поширюються як вірус, і їх не зупинити. Саме тому ми роками бачимо цю містифікацію».

Чи не єдиний позитив у цих дописах, каже дехто з користувачів Twitter та Facebook, – вони показують, хто із друзів настільки довірливий, щоб попадатися на таку стару «качку» ***(Авторські права у Facebook: правда і вигадки // BBC Україна (http://www.bbc.co.uk/ukrainian/science/2015/01/150109_copyright_in_facebook_sa). – 2015. – 9.01).***

***

Скрытая война Кремля распространяется теперь не только на Восток Украины. Его кибервоины взялись за инфраструктуру западных стран – а именно за федеральное правительство Германии.

Об этом пишет У. Клаус в статье под названием «Путин переносит свою войну с Украиной в Берлин», опубликованной на сайте немецкой газеты Die Welt, передает Цензор.НЕТ.

Дело гораздо более серьезное, чем многие думают. Кибератака пророссийской группы хакеров на инфраструктуру парламента и правительственных учреждений в Берлине – это продолжение скрытой войны, которая как очевидно согласованная акция сопровождает российскую агрессию в Украине уже в течение нескольких месяцев.

Насчет этой атаки не нужно строить никаких иллюзий. Определение «хакер» для группы «КиберБеркут», которая несет ответственность за атаку, возможно, звучит довольно безобидно.

Но за этим стоят комбатанты Кремля, которые активно участвовали в военных действиях в процессе оккупации Россией Крыма, и, среди прочего, уже совершали атаки на штаб-квартиру НАТО в Брюсселе, а также на Министерство обороны Украины. Что дальше? Немецкая электростанция? Больница?

Характер и масштабы атак указывают на высокопрофессиональное ведение войны с привлечением российских командных структур. К тому же, как подтверждают немецкие спецслужбы, в последние месяцы ощутимо увеличилось количество пропагандистских прокремлевских кампаний в социальных сетях. Также форумы почти всех немецких газет и телеканалов постоянно засыпают комментариями с враждебной пропагандой против США и НАТО. В шутку, стоящих за этим активистов называют «троллями».

Кибервойна является одной из разновидностей войны нашего времени. Россия Путина ведет ее и на немецкой территории. Можно и дальше вести философские дебаты о «сторонниках Путина», в салонах и пабах. Но наши политики в сфере безопасности должны, наконец, осознать, что нападение на внутреннюю инфраструктуру положило конец таким дебатам и стало вопросом национальной обороны.

Кто ждет, пока В. Путин официально объявит свои захваты территорий и кибератаки на другие государства, как войну, к сожалению, только после окончания [этой войны] поймет, что проиграл ее ***(«Путин переносит свою войну с Украиной в Берлин», – Die Welt // Цензор.НЕТ (http://censor.net.ua/news/319270/putin_perenosit_svoyu_voyinu_s_ukrainoyi_v_berlin_die_welt). – 2015. – 8.01).***

***

Социальные сети помогают распространению исламофобии

Популярные площадки Twitter и Facebook способствуют расцвету исламофобии, помогая распространять антимусульманские настроения. К

такому выводу пришли представители британских СМИ. Несмотря на жалобы пользователей и собственные правила, социальные сети отказываются удалять сотни разжигающих межрелигиозную ненависть сообщений на своих сайтах.

Количество записей в социальных сетях, обвиняющих мусульман в изнасилованиях, педофилии или сравнивающих ислам с раковой болезнью, за последний год существенно возросло. Однако Twitter и Facebook не спешат принимать меры, и призывы к насилию и оскорбления верующих продолжают оставаться доступными для миллионов людей по всему миру, пишет издание The Independent.

Некоторые из таких записей содержат прямые призывы отстреливать мусульман в Великобритании, но в большинстве случаев руководство социальных сетей закрывает на это глаза и даже не выносит пользователям предупреждения, отмечает издание.

За последние четыре месяца мусульманские сообщества пытались собрать данные об оскорблениях и передать их администрациям Twitter и Facebook. Они указали на десятки аккаунтов и сотни сообщений, но большинство из них всё ещё доступны на страницах этих социальных сетей.

Один из таких пользователей написал: «Нам следовало проиграть во Второй мировой войне. Твоя дочь бы забеременела от красивого немецкого блондина, а не от какого-нибудь пакистанского пастуха».

Следующая запись, которая появилась после казни западных граждан террористами в Сирии, тоже по-прежнему доступна, несмотря на то что на неё пожаловались ещё несколько недель назад: «За каждого человека, обезглавленного этими больными дикарями, мы должны выловить на улице десять человек, отрезать им головы, снять это на видео и выложить в Интернет. За каждого ребёнка, которого они зарезали, мы должны зарезать одного их ребёнка. Око за око».

В Facebook заявили, что эти сообщения не нарушают правил организации. «Мы серьёзно рассматриваем сообщения, вызывающие ненависть, и удаляем любой контент, который оскорбляет расу, этническую принадлежность, национальность, религию, пол, сексуальную ориентацию, ограниченные возможности или состояние здоровья», – сказал представитель компании. В Twitter также заверили, что проверяют весь контент, на который жалуются пользователи, а их правила запрещают угрозы применения насилия.

«Это неприемлемо, что такие платформы, как Facebook и Twitter, которые имеют огромные доходы, решают, что можно и что нельзя говорить, раз они поощряют социальное расслоение и фанатичные взгляды в обществе», – сказал Ф. Мугал, директор межконфессиональной организации Faith Matters, которая помогает и жертвам исламофобии.– Эти социальные платформы превратили себя в фабрики по зарабатыванию денег, но они не могут сидеть сложа руки и формировать наше будущее на основе «условий и требований», которые не соответствуют своему назначению».

По мнению Ф. Мугала, социальные сети должны более строго управлять своим контентом. «Когда люди выражают такие неприемлемые мнения, как отстрел чернокожих британцев, или сравнивают евреев с раковой опухолью, это должно стать незаконным», – сказал он.

Рост оскорблений в Интернете стал отражением роста реальных нападений на почве ненависти. По данным полиции Лондона, за последний год количество преступлений против мусульман в британской столице увеличились на 65 % ***(Социальные сети помогают распространению исламофобии // Newsland (http://newsland.com/news/detail/id/1480769/). – 2015. – 3.01).***

***

АР проаналізувала реакцію ісламістів у мережі на теракт у Charlie Hebdo

«Войовничий гелгіт поширювався як лісова пожежа...», – так Associated Press описала перший відгук ісламістів у мережі на збройний напад у редакції сатиричного тижневика Charlie Hebdo.

За кілька хвилин після появи гарячої новини про смертельну терористичну атаку на паризький часопис прихильники екстремістських ісламських угруповань почали возвеличувати підозрюваних у вбивстві як «левів Халіфату», зазначає американське інформаційне агентство. Скоєні ними злочини вихвалялися в соціальних медіа.

Групи, лояльні «Аль-Кайді» та «Ісламській державі в Іраку і Леванті» (ISIS), в унісон характеризували напад на редакцію Charlie Hebdo та убивство 12 осіб як «помсту» за глум з ісламу та пророка Мухаммеда і за військове втручання Франції у мусульманських країнах.

Б. Шеріф і С. Куаші стали «іконами тероризму».

Чимало їхніх войовничих прихильників активізувалися в хаштегах арабською мовою #Parisattack і #Parisisburning. Декотрі з них називали напад «священним».

Користувачі Twitter, які ідентифікували себе з угрупованням «Ісламської держави» чи з «Аль-Кайдою» постійно, розміщували знімки та відео одягненого в чорне бойовика. Імовірно, на них ньому був зображений один з братів-нападників, який стріляв у голову охоронцю порядку, коли той лежав на паризькій бруківці.

«Подивіться, як наш брат убиває французького поліцейського!», – раділи декотрі. Інші описували убивства у редакції Charlie Hebdo як «героїчну» й «радісну» подію.

«Ставлення до нападу “у військовому стилі”, вчиненого братами Куаші, та до їхньої “мученицької” смерті під градом куль у будівлі, де вони переховувалися після втечі перегукується з неодноразовими закликами екстремістів чинити атаки проти Франції, – зазначає АР. – Це – відлуння кадрів пропагандистських відео ісламістів, мета яких – відлякувати».

Associated Press торкається важливої проблеми впливу паризької драми на подальші виклики ісламських терористів західному правопорядку.

«Відчутно виміряти, як збройний напад на Charlie Hebdo вплине на вербування, яке здійснюють екстремістські групи, неможливо, – вважає інформагенція. – Поки що немає жодних доказів того, що число потенційних джихадистів внаслідок цього набагато зросте. Однак експерти вважають, що дії братів Куаші під час атаки, які подаються як професійні, та подальша розбірка з поліцією може зібрати в їхні войовничі ряди нових прихильників».

АР посилається на британського експерта з дослідження діяльності ісламських екстремістів у Сирії та Іраку А. Таміні.

«Вербуванню, – заявив він, – сприяє якість проведення таких операцій». За його словами, вочевидь добре спланована атака в центрі Парижа служить «прикладом для потенційних оперативників».

Після того як братів Куаші було вбито, член єменської філії «Аль-Кайди» на Аравійському півострові підтвердив АР, що він координував напад на Charlie Hebdo. На умовах анонімності він розповів інформагенції, що провідники угруповання «ретельно визначали мету операції та керували нею».

Потенційно від паризького кровопролиття виграють «Аль-Кайда» та ISIS, робить висновок АР.

«Ісламська держава в Іраку і Сирії» привітала його як «успіх» у глобальній «священній війні». Вона служить імпульсом боротьбі проти США, які завдають авіаудари по її позиціях на захоплених торік цим угрупованням великих частках територій обох цих держав.

Атака «Аль-Кайди» демонструє, що це угруповання не зійшло з арени і більш як через 10 років після вересневих терактів проти Сполучених Штатів ще спроможне завдавати удари в саме серце західної цивілізації.

Джихадисти скомпонували з відео паризької драми колаж тривалістю 2 хв і подають його як «помсту Аллаха та його пророка», рекламуючи «священну війну».

АР відзначає: обидва угруповання, щоб підвищити довіру до себе молодих, схоплених ними на гачок мусульман, покладаються «на кліпи у голлівудському стилі» ***(АР проаналізувала реакцію ісламістів у мережі на теракт у Charlie Hebdo // Телекритика (http://www.telekritika.ua/kontekst/2015-01-11/102375). – 2015. – 11.01).***

***

У соціальних мережех діє група під назвою «РНР» – «Ровенская Народная Республика.»

Навряд, що переважна більшість її членів мають хоча б якесь відношення до Рівного. Члени спільноти «РНР», яких майже 400 осіб – ті, хто живуть у Росії, або заходять під виглядом «сторінок-фейків», аби поширювати сепаратистські настрої в Західній Україні.

У соціальних мережах рівняни вже відреагували на створення цієї спільноти, і в коментарях звертаються до органів СБУ «розібратись із цим питанням» ***(У Рівному створили Рівненську народну республіку? // Інтернет-портал «ЧаРівне.інфо» (http://charivne.info/rivne-news/U-Rivnomu-stvorili-Rivnensku-narodnu-respubliku). – 2015. – 12.01).***

***

Чотири країни – Литва, Великобританія, Данія та Естонія – звернулися до Єврокомісії із закликом розробити план дій щодо боротьби з російською пропагандою.

Про це повідомляє delfi.lt.

Міністри закордонних справ чотирьох країн попередили, що РФ швидко розширює свою «кампанію дезінформації та пропаганди», метою якої є підтримка політичних та військових завдань російського уряду.

Очільники зовнішньополітичних відомств надіслали листа Верховному представнику із закордонних справ ЄС Ф. Могеріні. У ньому закликали «забезпечити надійну та конкурентоздатну інформаційну альтернативу російськомовним жителям і тим, хто користується ЗМІ, контрольованими Російською державою».

Ф. Могеріні запропонували обговорити тему російської пропаганди під час зустрічі міністрів країн-членів ЄС. Вони також закликали зовнішньополітичне представництво ЄС розробити план дій на 2015–2016 рр.

Автором ініціативи став міністр закордонних справ Литви Л. Лінкявічюс. За його словами, ідеться не про цензуру чи заборону, а про створення рівних умов для вільних джерел інформації. Міністр також додав, що Росія виділяє мільярдні суми на державні ЗМІ, тому потрібно «зміцнити стійкість суспільства до маніпуляцій». «Хотілося б, щоб ми приділяли більше уваги створенню не лише на словах, але й конкретними діями умов для того, щоби люди отримували альтернативну, вільну, об'єктивну інформацію. В жодному разі вона не повинна контролюватися іншою «справедливою» владою, тому що це також невільна інформація», – сказав Л. Лінкявічюс.

Крім нього лист підписали міністри закордонних справ Великобританії, Данії та Естонії – Ф. Хеммонд, М. Лідергаард та К. Пентус-Росіманнус.

У зверненні міністри запропонували створити інтернет-платформу для представлення інформації про брехню та маніпуляції, надавати підтримку ініціативам зі створення нових телеканалів, сайтів, радіостанцій чи газет російською мовою, заохочувати обмін інформаційною продукцією всередині ЄС, а також з надання її російським ЗМІ.

Підписанти листа також переконані, що ЄС має приділяти більшу увагу об'єктивному інформуванню та запобіганню розпалювання ворожнечі чи пропаганді війни. Для цього пропонується більш тісно співпрацювати медійним регуляторам різних країн ЄС ***(ЄС закликають розробити план боротьби з російською пропагандою // Телекритика***

(http://osvita.mediasapiens.ua/media_law/government/es_zaklikayut_rozrobiti_plan_borotbi_z_rosiyskoyu_propagandoyu/). – 2015. – 10.01).

Зарубіжні спецслужби і технології «соціального контролю»

Российские соцсети становятся очень опасными для украинцев

Чтобы не получилось так, что где-то в аэропорту Европейского Союза на паспортном контроле вы, или ваши друзья узнали, что РФ подала на вас (и/или на ваших друзей) в международный розыск, полезно знать, информируют «Экономические известия» (http://news.eizvestia.com/news_technology/full/232-rossijskie-socseti-stanovyatsya-ochen-opasnymi-dlya-ukraincev).

Для этого нужно сделать некоторые действия самому, проинформировать и попросить сделать эти же действия своих родственников, друзей, знакомых, коллег.

Минимальный набор шагов:

1. Срочный уход с российских электронных почтовых ящиков. До сих пор многие украинские чиновники используют эти ресурсы для ОФИЦИАЛЬНОЙ переписки и работы. Естественно для личных целей тоже не используем!

2. Российские социальные сети. Украинским организациям и бизнесу там делать нечего. Для личных целей, формат может быть такой: присутствие, но режим полного эфирного молчания. На этих сетях, ни в коем случае не использовать встроенные приватные чаты и сообщения!

3. Российские продукты и ПО, такие как Антивирус Касперского, должны быть удалены с заменой, компьютеры переформатированы. Всегда подробно выясняйте происхождение и держателя софта!

4. С российскими мобильными приложениями необходимо поступить так же, как и в пункте 3.

5. Максимально ограничить использование российских онлайн ресурсов (например поисковиков).

Глава Службы безопасности Украины В. Наливайченко советует соотечественникам быть более сдержанными в социальных сетях – из-за того, что в России от 1 августа 2014 г. вступил в силу так называемый закон о блогерах.

«На территории Российской Федерации в их ресурсах действительно очень серьезно развернута дискредитационная кампания, фальсификации, пропаганда с использованием серверов и ресурсов соцсетей, которые используют граждане нашей страны. Наша первая рекомендация, если вы нам доверяете: меньше пользоваться и не давать доступ к вашей личной переписке, к данным, которые вы выкладываете в соцсети», – заявил В. Наливайченко на брифинге в Киеве.

СБУ также принимает меры для защиты пользователей мобильных операторов Украины «от несанкционированного вторжения спецслужб Российской Федерации в ваши смс-сообщения, в ваши передвижения и ваши частные разговоры», – отметил В. Наливайченко.

В СБУ предупреждают всех граждан, которые обеспокоены безопасностью личной информации и рекомендуют воздержаться от использования интернет-ресурсов российской доменной зоны, в первую очередь это касается соцсетей и почтовых ящиков ***(Российские соцсети становятся очень опасными для украинцев // Экономические известия (http://news.eizvestia.com/news_technology/full/232-rossijskie-socseti-stanovyatsya-ochen-opasnymi-dlya-ukraincev). – 2015. – 11.01).***

***

Служба безпеки України порушила кримінальну справу з приводу поширення в соціальних мережах неправдивої інформації про українських військовослужбовців.

Про це на своїй сторінці у Facebook повідомив радник голови Служби безпеки України М. Лубківський.

Зокрема, кримінальне провадження зареєстровано проти громадянки України, яка, як повідомляють, «запустила» в соцмережах інформацію про те, що українським військовим, які перебувають у полоні, відрізали геніталії і один із них після цього вчинив самогубство.

Мова, за словами М. Лубківського, ішла про бійців, яких звільнили з полону 26 грудня.

«Кримінальне провадження зареєстровано за ознаками правопорушення, передбаченого частиною 1 статті 259 Кримінального кодексу України (свідомо неправдиве повідомлення про підготовку вибуху, підпалу або інших дій, які загрожують загибеллю людей чи іншими тяжкими наслідками. – Ред.)», – повідомив радник голови СБУ.

Карається це правопорушення позбавленням волі на термін від двох до шести років.

Нині проводиться досудове розслідування.

Нагадаємо, 26 грудня з полону бойовиків вдалося звільнити 150 українських військовослужбовців. Днями бойовики анонсували ще один обмін, за результатами якого мусили звільнити ще 30 осіб. Скільки військових утримують у заручниках у терористів, достеменно невідомо ***(СБУ порушила справу за неправдиву інформацію про українських військових // LB.ua (http://ukr.lb.ua/news/2015/01/05/291386_sbu_porushila_spravu_nepravdivu.html). – 2015. – 5.01).***

***

Общеизвестно, что наши смартфоны и браузеры следят за нами.

При этом, как пишет Lifter, это уже даже никого не удивляет, после всех шпионских скандалов, которые произошли в 2014 г.

Наряду с этим сообщается, какую именно информацию о вас собирает Google.

1. Google решает, какую рекламу вам показывать.

Каждый пользователь при регистрации в Google указывает свой возраст, пол, интересы. Это базовая информация, на которую ориентируется Google, показывая вам те или иные данные.

2. Google знает о том, где вы бываете.

Если вы используете Android, ваше мобильное устройство может отправлять на сервера Google информацию не только о вашем текущем местоположении, но и формирует карту ваших передвижений.

3. Google знает, что вы ищете в Интернете.

Каждый раз, когда вы формируете поисковый запрос и отправляете его в Google, сервера компании сохраняют эту информацию. А еще они сохраняют ссылки, на которые вы в результате кликнули.

4. Google знает, какими устройствами вы пользуетесь.

Google запоминает, какие гаджеты вы используете для работы с аккаунтом на нем. Более того, он хранит сведения о том, где вы примерно находились каждый раз с каждым новым гаджетом. Он даже хранит IP-адрес устройства.

5. Google знает, что о вас знают другие.

Другие – это авторы тех приложений и расширений для браузера Chrome, которыми вы пользуетесь ***(Что знает о вас Google? // Власти.нет (http://vlasti.net/news/209403). – 2015. – 11.01).***

***

Трояны для слежки за пользователями iOS и Android

Управление общественной безопасности города Вэньчжоу закупило троянские программы для слежения за пользователями смартфонов, сообщает Epochtimes. Отдел пропаганды ЦК КПК распорядился удалять всю информацию об этом в подконтрольном Пекину сегменте Интернета.

15 декабря 2014 г. на официальном сайте экономического и технологического развития района г. Вэньчжоу провинции Чжэцзян появилась информация о том, что районное управление безопасности купило два троянских приложения – за 49 тыс. юаней (7,9 тыс. дол.) и 100 тыс. юаней (16 тыс. дол.). Эти шпионские программы позволяют отслеживать телефонные разговоры, смс-сообщения, фотографии и другую информацию, находящуюся в смартфонах с операционными системами на Android и iOS. iPhone и iPad предварительно должны пройти процедуру джейлбрейка.

Вредоносное ПО разработала компания Wuhan Hongxin Telecommunication Technologies Co., работающая при Комитете по контролю и управлению государственным имуществом КНР.

Информацию на сайте районной администрации обнаружили китайские блогеры и начали активно распространять её в соцсетях. Вскоре сообщение с сайта исчезло, но к тому времени оно широко разлетелось по Интернету и вызвало волну недовольства и критики в адрес властей.

«Власти уже не скрывают того, что следят за нами с помощью троянов, и это самое страшное», – возмущается китайский пользователь.

«Это законно? Мы тут активно критиковали США после откровений Э. Сноудена, а у нас ситуация не лучше», – пишет другой блогер.

«Вот так у нас преступники и превратились в блюстителей закона», – замечает еще один пользователь.

В последнее время всё чаще появляется информация о том, что китайские смартфоны продаются с уже встроенными бэкдорами. В конце декабря американская компания Palo Alto Networks сообщила, что в китайских смартфонах Coolpad (шестой по величине производитель этих гаджетов в мире) обнаружено приложение, предоставляющее удалённый доступ ко всем функциям телефона.

В июне 2014 г. немецкая фирма G Data обнаружила шпионское приложение в китайских телефонах Star N9500. Бэкдор был установлен на стадии производства и от него невозможно избавиться обычными способами.

Даже в смартфонах Sony, в частности в моделях Xperia Z3 и Xperia Z3 Compact, которые производятся в Китае, также была обнаружена шпионская программа, отправляющая информацию на китайские серверы. Для обычного пользователя удалить ее не представляется возможным.

Аналогичная программа была обнаружена компанией F-Secure в смартфонах Xiaomi. Телефоны отправляли имя владельца, номер его телефона, идентификатор устройства, данные адресной книги и текстовые сообщения на серверы в Пекине ***(Трояны для слежки за пользователями iOS и Android // InternetUA (http://internetua.com/troyani-dlya-slejki-za-polzovatelyami-iOS-i-Android). – 2015. – 11.01).***

***

Российское военно-историческое общество предложило создать «патриотический интернет», «патриотическое радио» и вступить в «идеологическое контрнаступление по всему фронту», сказано на официальном сайте организации, пишет «Обозреватель» (http://tech.obozrevatel.com/news/50914-v-rossii-sozdadut-patrioticheskij-internet-chtobyi-ne-prospat-molodezh.htm).

«Нам нельзя “проспать” молодежь. Нам необходима консолидация государства и общества на основе ценностей, привитых нашей историей. Нам необходим патриотический тренд в общественном сознании. Нужны фильмы, книги, выставки, современные видеоигры, нужен патриотический Интернет, патриотическое радио и ТВ», – сказано в обращении.

Россия должна вступить, как отмечается в обращении, в «идеологическое контрнаступление по всему фронту».

Также в тексте обращения упоминается, что скандирование лозунгов в поддержку жертв теракта в Париже 7 января «заглушает грохот артиллерийских залпов украинской армии по мирным городам Донбасса».

Под обращением подписались 15 человек, среди которых вице-премьер Д. Рогозин, министр культуры В. Мединский, режиссер Н. Михалков и артист М. Пореченков ***(В России создадут «патриотический интернет», чтобы не «проспать» молодежь // Обозреватель (http://tech.obozrevatel.com/news/50914-v-rossii-sozdadut-patrioticheskij-internet-chtobyi-ne-prospat-molodezh.htm). – 2015. – 13.01).***

Проблема захисту даних. DDOS та вірусні атаки

В федеральном суде США началось разбирательство по делу против социальной сети Facebook. Групповой иск против ресурса был подан еще в 2013 г. Компания уже пыталась отклонить иск, но в результате были сняты только часть обвинений, передает IT Expert со ссылой на Piratemedia.

Социальную сеть обвиняют в сканировании постов, подсчете «лайков», а также просмотре ссылок, на которые переходит пользователь. По мнению истцов, это является нарушением приватности пользовательской информации. Кроме того, Facebook не просто изучает личные сообщения, но и перепродает третьим лицам информацию, которую извлекает из частной переписки.

Истцы требуют от Facebook сумму в 10 тыс. дол. за каждого пользователя, сообщения которого подвергались сканированию ***(В США начался суд над Facebook // IT Expert (http://itexpert.org.ua/rubrikator/item/40353-v-ssha-nachalsya-sud-nad-facebook.html). – 2015. – 7.01).***

***

На своей странице в социальной сети хакер Е. Докукин сообщает, что СБУ получила данные о тысяче террористов Донбасса от украинских хакеров, передает «В Кулаке».

Сообщается, что данные включают себя полноценное досье на каждого террориста.

Так, стали известны ФИО, адреса, и воинские части боевиков, которые прибыли из РФ.

Результаты работы хакеров Е. Докунин опубликовал на своей странице в социальной сети ***(Украинские хакеры передали СБУ информацию о террористах Донбасса // InternetUA (http://internetua.com/ukrainskie-hakeri-peredali-sbu-informaciua-o-terroristah-donbassa). – 2015. – 5.01).***

***

Исследователь безопасности, известный под псевдонимом SecBit, обнаружил XSS-уязвимость на сайте Apple Store. Об этом сообщается на сайте XSSPosed.

Брешь была обнаружена 27 декабря 2014 г. По данным XSSPosed, на момент написания статьи она не была исправлена. Это означает, что злоумышленники могут ее проэксплуатировать и с помощью специально сформированной ссылки похитить данные пользователей. Киберпреступники могут похитить cookie-файлы с целью дальнейшего осуществления спуфинг-атаки, а также получить доступ к логину и паролю пользователей.

Это не первый случай, когда на сайте online-магазина Apple обнаруживались XSS-бреши. В базе данных XSSPosed упоминается о еще как минимум шести уязвимостях, в разное время обнаруженных на данной веб-странице ***(На сайте Apple Store обнаружена XSS-уязвимость // InternetUA (http://internetua.com/na-saite-Apple-Store-obnarujena-XSS-uyazvimost). – 2014. – 29.12).***

***

Уязвимость в нативном браузере Android ставит под угрозу учетные записи в Facebook. Все устройства, работающие под управлением ОС Android ниже KitKat, подвержены уязвимости, позволяющей обойти политику единства происхождения.

В браузере по умолчанию, который встроен в версии ОС Android ниже 4.4, существует серьезная уязвимость, которая позволяет злоумышленнику обойти политику единства происхождения (Same Origin Policy, SOP).

Первым об этой уязвимости в начале сентября 2014 г. сообщил независимый исследователь безопасности Р. Балох. Исследователи из Trend Micro и Facebook зафиксировали множественные инциденты, в которых жертвами кибератак с эксплуатацией именно этой уязвимости становились пользователи Facebook. Большое количество инцидентов объясняется тем, что экплоит для этой уязвимости опубликован в открытом доступе.

Кроме того, для обхода системы безопасности SOP браузеров более ранних версий ОС Android предпринимались XSS-атаки, с помощью которых в устройство жертвы из облачного хранилища внедрялся вредоносный файл на JavaScript. Речь идет об атаке с использованием ссылки, которая перенаправляет пользователей Facebook на вредоносный сайт.

Как сообщил эксперт из Trend Micro С. Хуанг, сайт содержит обфусцированный JavaScript-код, который предусматривает загрузку URL страницы Facebook во внутренний фрейм. Вследствие использования тега <div> HTML-настройки страницы изменяются таким образом, что на экране изображение отсутствует, а размер внутреннего фрейма составляет 1 пиксель.

JavaScript-код позволяет злоумышленнику выполнять различные задачи от имени владельца учетной записи в Facebook. В частности,

зафиксированы инциденты с применением официального приложения для BlackBerry для похищения маркеров доступа и последующего взлома учетных записей в Facebook.

Все устройства, работающие под управлением ОС Android ниже KitKat, подвержены этой уязвимости. Компанией Google еще в сентябре 2014 г. было выпущено исправление, однако миллионы устройств остаются под угрозой атаки: либо производители смартфонов прекратили выпуск обновлений, либо устройства не поддерживают более поздние версии операционной системы.

Уязвимость SOP существует в браузере Android-устройств, который невозможно деинсталлировать. В целях защиты следует отключить этот бразуер в настройках: зайти в меню «Приложения», выбрать пункт «Все», найти браузер и нажать кнопку «Отключить» ***(Уязвимость в нативном браузере Android ставит под угрозу учетные записи в Facebook // InternetUA (http://internetua.com/uyazvimost-v-nativnom-brauzere-Android-stavit-pod-ugrozu-ucsetnie-zapisi-v-Facebook). – 2014. – 30.12).***

***

Apple заблокировала уязвимость iCloud, которая позволяла злоумышленникам взламывать аккаунты пользователей методом перебора.

Программа iDict подбирала пароли из числа существующих вариантов. Все желающие могли, зная имя пользователя Apple ID (в этой роли, как правило, выступает почтовый адрес), методом перебора вариантов узнать секретную комбинацию символов. Программа подбирала пароли, используя словари для брута в количестве 500 самых популярных комбинаций. Среди них Password, Butterfly1, Welcome, November, Internet и другие.

5 января, как выяснил обозреватель Business Insider Д. Кук, Apple закрыла уязвимость iCloud. Издание ссылается на создателей iDict. «iDict больше не работает. Теперь ее лучше не использовать, если не хотите, чтобы заблокировали аккаунт», – написал в Twitter создатель инструмента Pr0x13. На то, чтобы заблокировать решение для взлома iCloud, у Apple ушло четыре дня ***(Apple закрыла уязвимость iCloud, которую использовали для взлома аккаунтов пользователей // InternetUA (http://internetua.com/Apple-zakrila-uyazvimost-iCloud--kotoruua-ispolzovali-dlya-vzloma-akkauntov-polzovatelei). – 2015. – 7.01).***

***

Хакери Anonymous обіцяють «взяти реванш» за теракт проти французького сатиричного тижневика Charlie Hedbo, повідомляє CNN.

У відео, розміщеному на YouTube, інтернет-угруповання хакерів заявило, що відстежуватиме сайти й соціальні мережі, пов’язані з ісламськими терористами й виводитиме їх з ладу.

«Ми, Anonymous в усьому світі, – говориться в ньому, – вирішили оголосити війну вам – терористам».

Це – месседж помсти «Аль-Кайді», «Ісламській державі в Іраку і Леванті (ISIS) й іншим терористичним організаціям за вчинене 7 січня жорстоке убивство 10 співробітників французького сатиричного журналу Charlie Ebdo та двох поліцейських.

«Ми маємо намір взяти реванш від їхнього імені, – стверджують Anonymous. – Ми відстежуватимемо вашу діяльність у мережі й закриватимемо ваші акаунти у соціальних мережах».

Угруповання Anonymous, що з'явилося на початку двохтисячних й досі зберігає свою утаємниченість, об'єднує численних користувачів мережевих спільнот у глобальному анархічному цифровому мозку.

Воно стало всесвітньо відомим з 2008 р., відколи здійснило хакерський проект проти Церкви саєнтології. Після цього ним була вчинена велика кількість акцій проти урядових установ, організацій та інших об'єктів, що набули світового розголосу. Збитки від них оцінюють у мільярди доларів.

Найпоширеніші гасла Anonymous: «Наше ім'я – Легіон», «Анонімус це кожен з нас і жоден з нас», «Ми як одне ціле, поділене на Нуль», «Анонімус не пробачає. Анонімус не забуває».

Останнє з них має безпосередній стосунок до розміщеного на YouTube відео у відповідь на теракт ісламістів у редакції Charlie Hebdo ***(Anonymous оголосили кібервійну ісламським екстремістам // Телекритика (http://www.telekritika.ua/kontekst/2015-01-11/102369). – 2015. – 11.01).***

***

Исследователи раскрыли новый вид сложных атак на АТМ

Злоумышленники взламывают физически взломанные банкоматы, применяя методы скимминга.

Как следует из сообщения в блоге ИБ-эксперта Б. Кребса, исследователи безопасности обнаружили ранее неизвестный сложноорганизованный метод проведения атак на АТМ. Злоумышленники физически взламывают банкоматы, комбинируя атаку со скиммингом.

В рамках нового вида нападения, получившего название black box, устройство выдачи купюр отключается от управляющего им компьютера, встроенного в АТМ. Система управления аппаратным обеспечением банкомата заменяется на ту, что создали мошенники и выполняет их команды, регулирующие выдачу банкнот.

По предварительным данным, в описанном Б. Кребсом случае злоумышленникам не удалось завладеть средствами жертв. Однако исследователи уверены, что мошенники имели большие шансы похитить деньги до того, как владеющая АТМ компания заподозрит неладное.

Напомним, что эксперты Positive Technologies неоднократно предупреждали о недостаточном уровне безопасности большинства АТМ, размещаемых сегодня банковскими организациями. Так, некоторые из ранее обнаруженных уязвимостей позволяют потенциальному злоумышленнику получить доступ к сервисной зоне банкомата без ключа или даже перевести

банкомат в сервисный режим ***(Исследователи раскрыли новый вид сложных атак на ATM // InternetUA (http://internetua.com/issledovateli-raskrili-novii-vid-slojnih-atak-na-ATM). – 2015. – 10.01).***

***

Греческий эксперт по шифрованию Д. Чатзисофронью, известный также под псевдонимом sophron, опубликовал на сайте GitHub инструмент социальной инженерии для похищения учетных данных и номеров кредитных карт пользователей из защищенных сетей Wi-Fi.

WiFiPhisher способен находить, а затем копировать сети, защищенные WPA. Инструмент отправляет легитимной точке доступа пакеты деавторизации, вызывая сбой в работе, из-за чего пользователь вынужден искать другие доступные сети. Далее пользователю предоставляется вредоносная сеть, маскирующаяся под доверенную точку доступа.

«WiFiPhisher – это инструмент безопасности для быстрого осуществления фишинговых атак на сети, защищенные WPA, с целью похищения кодовой фразы без необходимости брутфорса», – сообщил sophron.

После того как пользователь подключается к предложенной точке доступа и пытается открыть веб-страницу, WiFiPhisher открывает поддельную страницу, запрашивающую подтверждение пароля WPA якобы для обновления прошивки маршрутизатора. Правда, для подключения к незащищенной сети пользователь должен будет проигнорировать множество уведомлений об опасности ***(Эксперт создал инструмент для похищения данных из сетей, защищенных WPA // InternetUA (http://internetua.com/ekspert-sozdal-instrument-dlya-pohisxeniya-dannih-iz-setei--zasxisxennih-WPA). – 2015. – 7.01).***

***

Уязвимость Spotlight позволяет шпионить за пользователями OS X Yosemite

Известно, что OS X Yosemite собирает персональные данные пользователей и передает их на серверы Apple. Речь идет не о записи всех нажатий клавиш или перемещений курсора, как в Windows 10, а о поисковых запросах Spotlight, список которых отправляется в Apple и третьим лицам. Однако не только сама компания может получить персональные данные «маководов» благодаря фирменному поиску OS X. Согласно отчету немецких экспертов в области информационной безопасности, уязвимость механизма Spotlight позволяет это делать злоумышленникам.

Суть проблемы состоит в том, что функция загрузки содержимого из других источников в приложении Apple Mail позволяет зафиксировать отправителям, включая рассыльщикам спама, IP-адрес владельца Mac, ряд данных из браузера Safari, версии операционной системы и Quick Look. Это помимо прочего увеличивает шансы на успех тому, кто решит провести

хакерскую атаку. По этой причине функцию настоятельно рекомендуется отключать.

В свою очередь технология Spotlight, индексирующая содержимое электронной почты, в том числе контент на удаленных серверах, выполняет подгрузку данных и обращается на серверы отправителя. Она игнорирует отключенную в Mail функцию «Загружать содержимое из других источников». Другими словами, у пользователей фирменного почтового приложения Apple нет возможности защититься от слежки.

Единственный на сегодняшний день способ ограничить сбор данных для Spotlight состоит в отключении в настройках опции «Почта и сообщения». Ее можно найти в разделе Spotlight –> Результаты поиска настроек OS X Yosemite ***(Уязвимость Spotlight позволяет шпионить за пользователями OS X Yosemite // InternetUA (http://internetua.com/uyazvimost-Spotlight-pozvolyaet-shpionit-za-polzovatelyami-OS-X-Yosemite). – 2015. – 11.01).***

***

Мікроблог Центрального командування збройних сил США в соціальній мережі Twitter зазнав масованої хакерської атаки. Про це в понеділок, 12 січня, повідомляє The Telegraph, пише ZAXID.NET (http://zaxid.net/news/showNews.do?hakeri_atakuvali_twitter_ta_youtube_storinki_komanduvannya_zbroynih_sil_ssha&objectId=1336561).

Віртуальні зловмисники заявили, що вони діють від імені «Ісламської держави» (ІД).

На мікроблозі були опубліковані заяви з погрозами на кшталт – «Американські солдати, ми йдемо, будьте обережні».

Крім того, хакери поширили імена та номери телефонів військовослужбовців, слайди PowerPoint і карти. Хакери перейменували Twitter-сторінку у «Кіберхаліфат», а в підзаголовку написали «Ми любимо ІД».

Кіберзлочинці також атакували канал Центрального командування на відеохостингу YouTube. На ньому було розміщено кілька відеороликів екстремістів, у яких були показані військові операції і вибухи ***(Ганкевич Р. Хакери атакували Twitter та YouTube сторінки командування збройних сил США // ZAXID.NET (http://zaxid.net/news/showNews.do?hakeri_atakuvali_twitter_ta_youtube_storinki_komanduvannya_zbroynih_sil_ssha&objectId=1336561). – 2015. – 12.01).***

***

Д. Синегубко, специалист из ИБ-компании Sucuri, сообщает о бэкдоре, который эксплуатирует уязвимость в ранних версиях плагина RevSlider. Типичный представитель этого вида вредоносного ПО заинтересовал эксперта выбором удаленного сервера для размещения своего кода. Выяснилось, что для хостинга кода был использован веб-ресурс Pastebin.

Собственного говоря, злоумышленники использовали Pastebin по его прямому назначению – для обмена фрагментами кода. Pastebin.com позволяет скачивать код в «сыром формате», то есть, без разметки на языке HTML и элементов интерфейса сайта.

Эксперт обращает внимание на то, что для хостинга кода обфусцированной программы на Pastebin.com индонезийские хакеры пользуются специальным кодировщиком под названием PHP Encryptor by Yogyakarta Black Hat (либо by FathurFreakz).

Сервис Pastebin неоднократно использовался для хранения информации, похищенной в результате хакерских атак, в том числе на компанию Sony Pictures. Однако в последнее время, замечает эксперт, участились случаи, когда данный ресурс напрямую задействован в атаках. Прежде чем размещать коды на Pastebin, следует изменять их таким образом, чтобы при загрузке в «сыром» формате они становились неисполняемыми, советует специалист по безопасности ***(Бэкдор эксплуатирует уязвимость в ранних версиях плагина RevSlider // InternetUA (http://internetua.com/bekdor-ekspluatiruet-uyazvimost-v-rannih-versiyah-plagina-RevSlider). – 2015. – 13.01).***

***

Согласно утверждению известного исследователя безопасности Б. Кребса, DDoS-сервис LizardStresser хакерской группировки LizardSquad, взявшей на себя ответственность за взломы игровых сетей Sony Playstation и Microsoft Xbox Live, поддерживается с помощью ботнета, в большинстве своем состоящего из взломанных интернет-маршрутизаторов.

«Ботнет состоит не только из домашних маршрутизаторов – некоторые из инфицированных устройств являются коммерческими сетевыми устройствами, расположенными в университетах и компаниях», – пояснил Б. Кребс.

По словам специалиста, преимущество, которым обладают маршрутизаторы, объединенные в ботнет, во многом связано со способом распространения ботнета, однако не исключено, что вредоносное ПО может инфицировать устройства под управлением ОС Linux, в том числе настольные серверы и камеры с интернет-подключением.

Для инфицирования устройств хакеры используют модификацию бэкдора для Linux, подробности которого в прошлом году опубликовали специалисты ИБ-компании Dr. Web. Помимо превращения скомпрометированных устройств в «зомби»-машины, вредонос осуществляет сканирование Интернета в поисках других маршрутизаторов, которые могут быть взломаны с помощью использования установленных по умолчанию учетных данных.

Правоохранительные органы и интернет-провайдеры пытаются нарушить работу ботнета путем отключения зараженных систем. Тем временем вредоносное обеспечение продолжает распространяться, используя

маршрутизаторы, защищенные только именами пользователей и паролями, установленными по умолчанию ***(DDoS-сервис группировки LizardSquad поддерживается при помощи взломанных интернет-маршрутизаторов // InternetUA (http://internetua.com/DDoS-servis-gruppirovki-LizardSquad-podderjivaetsya-pri-pomosxi-vzlomannih-internet-marshrutizatorov). – 2015. – 12.01).***

***

Неизвестные хакеры всё активнее наносят удары по пользовательским учётным записям в социальной сети Instagram, пишет Блог Imena.UA (http://www.imena.ua/blog/xakery-voruyut-paroli-instagram/).

Агентство EyeMedia, специализирующееся на продвижении страниц в сети Instagram, предупреждает, что в последнее время группы неизвестных всё активнее взламывают персональные учётные записи пользователей, переправляя их на фишинговые сайты.

В настоящее время эта активность приобретает масштабы эпидемии.

Пользователь социальной сети получает письмо, якобы от администрации, и переходит по специальной ссылке. Затем пользователь вводит свои данные для входа на сайт, которые отправляются непосредственно хакерам.

Письма от хакеров полностью копируют дизайн официальных писем от технической поддержки Instagram, так что неопытный пользователь не заподозрит обман.

Кроме того, письма сделаны так, что в почтовом клиенте получателя в поле «От кого» отображается официальный адрес социальной сети, с которого обычно и происходит отправка различных уведомлений.

Представители EyeMedia предупреждают, что в таких письмах ссылка вместо сайта instagram.com ведёт на сайт злоумышленников instagram-password.com. Специалисты предостерегают от перехода по этим ссылкам и вводу любых пользовательских данных.

Ранее стало известно, что 500 тыс. пользователей установили приложение InstLike, которое увеличивает количество подписчиков в Instagram, но снижает уровень защищённости данных пользователя ***(Пользователей Instagram атакуют хакеры // Блог Imena.UA (http://www.imena.ua/blog/xakery-voruyut-paroli-instagram/). – 2015. – 13.01).***

***

Разработчики CryptoWall обновили вирус-вымогатель сложным функционалом

С момента появления в открытом доступе вируса-вымогателя CryptoWall прошло более года, и на протяжении этого времени создатели вредоноса периодически обновляли его функционал. Так, одно из наиболее крупных дополнений, расширяющих функционал вируса, было выпущено в период новогодних праздников.

Напомним, что CryptoWall, жертвами которого успело стать множество частных лиц, а также огромное количество коммерческих и правительственных организаций, шифрует информацию на инфицированной системе с целью получения выкупа. Более того, разработчики вымогателя создали целую систему безопасной передачи платежей и генерации соответствующих ключей шифрования для согласившихся на оплату выкупа жертв.

В настоящее время в CryptoWall 2.0 реализован функционал, способный отключать целый перечень механизмов безопасности в операционных системах Windows. Кроме того, вредоносное приложение способно самостоятельно переключаться между 32-ух и 64-разрядной архитектурой, сообщают исследователи из Cisco.

Не менее удивительным является наличие команды поддержки, способной в круглосуточном режиме помочь пользователям правильно осуществить оплату выкупа. В некоторых случаях стоящие за CryptoWall люди могут даже снизить стоимость ключа шифрования ***(Разработчики CryptoWall обновили вирус-вымогатель сложным функционалом // InternetUA (http://internetua.com/razrabotcsiki-CryptoWall-obnovili-virus-vimogatel-slojnim-funkcionalom). – 2015. – 13.01).***

***

Как сообщили исследователи TrendMicro, в Австралии зафиксирован всплеск заражения систем вымогательским ПО TorrentLocker. Эксперты подчеркнули, что вредонос быстро изменяется для того, чтобы успешно обходить системы безопасности.

ПО попадает на компьютеры жертв через фишинговые письма, замаскированные под почтовые или штрафные уведомления и содержащие ссылки на вредоносную страницу. Пользователям предлагается скачать информацию о штрафе (почтовом уведомлении) путем введения CAPTCHA, после чего на их системы загружаются ZIP-файлы с хостингового сервиса SendSpace. Примечательно, что электронные письма подделаны настолько искусно, что без труда обходят спам-фильтры.

ZIP-архив содержит ПО TorrentLocker, которое после разархивирования и выполнения шифрует документы на компьютере жертвы. При этом вредонос шифрует файлы с наиболее часто используемым расширением .DOCX, .PDF и .ZIP и требует от жертвы выплатить выкуп в биткоинах на сумму в 598 австралийских долларов. Если требование вымогателей не будет выполнено в течение 96 часов, сумма удвоится. Примечательно, что TorrentLocker не только шифрует файлы на зараженном компьютере, но также удаляет все резервные копии ***(В Австралии зафиксирован всплеск заражения систем вымогательским ПО TorrentLocker // InternetUA (http://internetua.com/v-avstralii-zafiksirovan-vsplesk-zarajeniya-sistem-vimogatelskim-po-TorrentLocker). – 2015. – 13.01).***

***

Эксперт из Accuvant Labs Д. Дрейк обнаружил уязвимость в маршрутизаторах ASUS, позволяющую злоумышленникам, имеющим доступ к локальной сети, выполнять произвольные команды. По словам Д. Дрейка, брешь CVE-2014-9583 присутствует в сервисе обнаружения локальной сети infosvr, работающем с правами суперпользователя.

Сервис «слушает» порт 9999, который может использоваться злоумышленниками для отправки пакетов, содержащих вредоносный код, с целью получить контроль над устройством. Д. Дрейк успешно осуществил атаки на маршрутизатор ASUS RT-N66U с версией прошивки 3.0.0.376.2524-g0013f52. ИБ-эксперт Д. Лонгенекер подтвердил наличие уязвимости и в наиболее новой модели RT-AC87U с версией прошивки 3.0.0.4.378_3754.

Д. Лонгенекер сообщил, что размер эксплоита для этой бреши не должен превышать 237 знаков, иначе устройство может выйти из строя из-за переполнения буфера. ASUS известно об уязвимости, и компания работает над ее исправлением. Отметим, что эксплоит доступен публично, поэтому пользователи должны принять меры по обеспечению безопасности.

Кастомизированная версия прошивки Asuswrt-Merlin, разработанная Э. Соважо, смягчает потенциальные атаки путем отключения функции, ответственной за удаленное выполнение кода ***(В маршрутизаторах ASUS обнаружена уязвимость // InternetUA (http://internetua.com/v-marshrutizatorah-ASUS-obnarujena-uyazvimost). – 2015. – 13.01).***

***

Эксперт по вопросам безопасности нашел способ установки на крошечный чип, встроенный в ноутбуки Apple, вредоносного кода который будет сопротивляться любой попытке удаления – даже замена жесткого диска не удаляет его.

Атаку, названную Thunderstrike, практически невозможно обнаружить виртуально, но для нее злоумышленнику потребуется получить доступ к компьютеру. Так как такой вид атаки совсем новый, антивирусное программное обеспечение не будет даже смотреть в его сторону.

Т. Хадсон из Нью-Йоркского хедж-фонда Two Sigma Investments, рассказал, что дыра в безопасности была найдена, когда его работодатель попросил оценить безопасность ноутбуков Apple. Его первым шагом стала разборка одного из ноутбуков, чтобы получить доступ к boot ROM, небольшому чипу, который содержит код, которому следует компьютер перед загрузкой основной операционной системы.

Вредоносный код может быть спрятан в этой boot ROM, и в отличие от обычного вируса, который «живет» на жестком диске, он не может быть удален. Этот способ известен как буткит-атака. Вредоносный код позволяет злоумышленнику делать что угодно – от тайного наблюдения за пользователем до похищения конфиденциальных данных, хранящихся на компьютере.

Хотя предыдущие исследователи обнаружили, что, изменение содержимого ROM в ноутбуках Apple делает полностью непригодным использование компьютера, так как системы безопасности анализируют изменения ROM и автоматически отключают ПК, если находят их. Однако Т. Хадсону удалось обойти эти проверки и установить любой код, какой он хотел.

Он сказал, что эти меры безопасности были всегда «обречены на провал» и «бесполезны», поскольку любой, кто может получить доступ к содержимому ROM также может получить доступ и к коду, который проверяет диск на изменения. Вместо этого, по его словам, должен быть неизменяемый аппаратный чип, который выполняет такую проверку.

Кроме того, было установлено, что атака может быть осуществлена без разборки компьютера на части, для того чтобы добраться до чипа. Можно просто использовать порт Thunderbolt. Теоретически, любое устройство – монитор, жесткий диск или принтер – можно использовать для установки вредоносного кода, просто подключив и сделав несколько простых шагов.

«Так как это первый буткит OS X прошивки, в ней нет ничего, что сканировало бы его присутствие. Он контролирует систему с самой первого инструкции, которая позволяет ему записывать нажатия клавиш, в том числе ключей шифрования диска, помещая бэкдоры в ядре OS X и обходя пароли доступа», – рассказал Т. Хадсон. «Переустановка OS X не удалит его. Замена SSD не удалит его – так как в бутките нет ничего, хранящегося на диске. Несколько минут наедине с вашим ноутбуком – и Thunderstrike позволяет перперошить ваш boot ROM, независимо от наличия паролей или шифрования диска. Thunderstrike в его нынешнем виде был эффективен против всех MacBook Pro/ Air/Retina с Thunderbolt, которые я проверял, большинство проверенных моделей производятся начиная с 2011 г.».

Т. Хадсон говорит, что Apple выкатила «частичный фикс», который остановит перезапись boot ROM с вредоносным кодом в некоторых обстоятельствах, но не во всех – например, когда машина будет перезагружена с подключенным вредоносным Thunderbolt-устройством. Он сообщил компании о дефекте в 2013 г., но говорит, что некоторые ноутбуки по-прежнему уязвимы, так как хакеры могут обмануть машины, делая даунгрейд до версии, которая не включает в себя новое исправление.

Единственное предложение Т. Хадсон для предотвращения такой атаки – перезаписать ROM с вашим собственным кодом, который блокирует любые удаленные атаки через порт Thunderbolt, а затем закрасить винты на вашем ноутбуке лаком для ногтей, чтобы обнаружить несанкционированный физический доступ к ROM, Тем не менее, это сложная мера, труднодоступная для всех, кроме продвинутых экспертов в области безопасности ***(Ноутбуки Apple уязвимы для вируса, который «не может быть удален» // InternetUA (http://internetua.com/noutbuki-Apple-uyazvimi-dlya-virusa--kotorii--ne-mojet-bit-udalen). – 2015. – 13.01).***

***

Український хакер Є. Докукін на честь Старого Нового року роздрукував повідомлення на мережевих принтерах сепаратистів та терористів. Хакер як пропаганду роздрукував антивоєнні гасла.

Зауважимо, що це – не перша подібна акція українських кібервійськ. «Якщо ваш мережевий принтер надрукує “Слава Україні!” чи різні поздоровлення з України, чи такі гасла, то знайте, що він під нашим контролем», – зауважив хакер ***(Український хакер зробив так, щоб принтери сепаратистів друкували антивоєнні гасла // InternetUA (http://internetua.com/ukra-nskii-haker-zrobiv-tak--sxob-printeri-separatist-v-drukuvali-antivo-nn--gasla). – 2015. – 14.01).***