СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(18–31.01)

2016 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(18–31.01)
№ 2

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

Відповідальний редактор
Л. Чуприна, канд. наук із соц. комунікацій

Упорядник
Т. Касаткіна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2016

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 17
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 21
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 30
Інформаційно-психологічний вплив мережевого спілкування на особистість 30
Маніпулятивні технології 32
Зарубіжні спецслужби і технології «соціального контролю» 37
Проблема захисту даних. DDOS та вірусні атаки 42

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Блог NewsWhip вивів п’ять напрямів, які матимуть значний вплив на новинні редакції та видавців у новому році, повідомляє «Телекритика» з посиланням на MMR.

По-перше, після того як вертикальні відео стали популярними на мобільних пристроях завдяки Snapchat Discover, автори публікації очікують, що популярність такого формату зросте на всіх типах пристроїв. А інструмент Facebook Mentions дасть змогу легко вести відеотрансляції для своєї аудиторії.

Instagram стане самостійною контент-платформою. Так, представник BBC Sport І. Сінглтон повідомив, що зростання їх профілю в Instagram перевищує більшість інших соціальних платформ.

У 2016 р. NewsWhip очукує збільшення кількості користувачів месенджерів. Як зазначали в нещодавньому дослідженні Tow Center: «Месенджери дають хорошу можливість залучати нових або важкодосяжних демографій». Можливо, 2016 р. стане роком запуску ефективних CMS для месенджерів, які значно полегшать життя видавцям, зауважуть автори публікації.

Також у цьому році задаватиме тон швидкісне споживання контену. Проект Google AMP (Accelerated Mobile Pages) запустять найближчим часом. Він дасть змогу пришвидшити доступ до новин у пошуковій видачі. До кінця року використання схожих сервісів повинно стати поширеним. Сайти, погано оптимізовані для мобільних приладів, навряд чи будуть популярними у 2016 р.

Крім того, виданням доведеться бути більш вибагливими у тому, на що їм варто тратити час. Великий обсяг матеріалів викликає мінімальний інтерес. Водночас хороші відгуки отримують ті історії, у яких читач бачить цінність, які хочеться читати й ділитися ними ***(Чого чекати виданням від соціальних медіа у 2016 // Телекритика (http://www.telekritika.ua/internet/2016-01-26/113048). – 2016. – 26.01).***

***

Соцмережа Facebook додала у свій офіційний додаток для Android підтримку підключення через анонімну мережу Tor, пише «Телекритика». Нова експериментальна функція повинна з’явитися у всіх користувачів найближчими днями, повідомляє VC.

Нововведення дасть змогу користувачам оминати блокування сайту місцевою владою, а також пригодиться тим, хто хвилюється за безпеку свого підключення, зазначає The Next Web.

Для підключення до Facebook через Tor користувачам потрібно буде встановити додаток Orbot для роботи з анонімною мережею. Після цього в налаштуваннях додатку з’явиться можливість активувати зашифроване підключення через Tor.

У 2014 р. Facebook створила спеціальну адресу для входу через мережу Tor. «Це рішення підвищило безпеку підключень до Facebook через Tor, вилучивши кроки, в яких трафік виходив за межі захисту Tor», – зазначили в компанії ***(Facebook дозволив підключення через анонімну мережу Tor у додатку для Android // Телекритика (http://www.telekritika.ua/internet/2016-01-20/112996). – 2016. – 20.01).***

***

За последние девять месяцев показатели роста и вовлечённости Instagram пережили значительное падение, пишет «Телекритика». Об этом сообщается в новом отчёте аналитической компании Locowise, передает Search Engines.

В декабре 2015 г. показатель роста подписчиков составил всего 0,23 % – на 88,21 % ниже, чем в апреле того же года (1,95 %).

Что касается вовлечённости, в апреле этот показатель достиг 2,8 %, а в декабре – 1,08 %. Таким образом, за этот период он упал на 61,43 %.

В то же время, по состоянию на декабрь 2015 г. Instagram по-прежнему опережает Facebook и Twitter по показателям роста аудитории и вовлечённости пользователей. В частности, в декабре Instagram демонстрировал вовлечённость на уровне 1,08 %; Twitter – 0,1 %, Facebook – 0,37 %.

По данным Locowise, изображения составляют 91,87 % от всех публикаций в Instagram и демонстрируют более высокие показатели вовлечённости, чем другие виды публикаций ***(Показатели роста и вовлеченности Instagram в 2015 году значительно упали, – исследование // Телекритика (http://www.telekritika.ua/internet/2016-01-20/112998). – 2016. – 20.01).***

***

Компания Google запатентовала алгоритм, который сможет генерировать статусы в социальных сетях, основываясь на информации пользователя. Соответствующая заявка была опубликована Ведомством по патентам и товарным знакам США (USPTO).

Разработчики отмечают, что электронная почта сегодня не является оптимальным механизмом распространения ссылок или приглашения к участию в разговоре. Патент описывает схему создания поста в социальной сети по электронному письму.

Если, к примеру, вы получили от друга по электронной почте ссылку на книгу, вы сможете кликнуть по специальной кнопке в окне почтового сервиса. Google проанализирует информацию, а затем выдаст варианты сопутствующего текста с этой ссылкой и релевантные хэштэги для размещения в социальной сети. Здесь же можно выбрать группу друзей, которым будет показан материал, и просмотреть другие ссылки по теме.

Конечно же, патентование технологии ещё не означает, что на его основе будет создан реальный продукт. Однако многие идеи компании, как показывает практика, всё же воплощаются в жизнь достаточно быстро ***(Google будет***

писать статусы в социальных сетях за вас // InternetUA (http://internetua.com/Google-budet-pisat-statusi-v-socialnih-setyah-za-vas). – 2016. – 24.01).

***

«ВКонтакте» готовит новую соцсеть на основе своего фотоприложения Snapster – она будет работать на домене snapster.io. Об этом сообщили «Известия» со ссылкой на несколько источников, знакомых с планами компании.

Мобильное фотоприложение Snapster вышло в июле 2015 г. По своему принципу работы оно копирует фотосоцсеть Instagram, принадлежащую Facebook, с той разницей, что российская компания разработала более функциональный набор фотофильтров.

Snapster позволяет более детально работать с цветовой гаммой – например, можно выбрать цвет, который нужно сделать более ярким или обесцветить. Фильтром, который создал пользователь, здесь можно поделиться с друзьями. Кроме того, Snapster сильно интегрирована с «ВКонтакте»: фото, загруженное в приложение, дублируется в отдельный фотоальбом в самой соцсети. А в ленте новостей пользователя отображаются фотографии, опубликованные его друзьями не только в Snapster, но и в самой «ВКонтакте». Именно с этим и связаны главные претензии к новому проекту – по сути, приложение не дает ничего нового, оно лишь по-другому выводит фотографии из «ВКонтакте».

Изначально «ВКонтакте» стала создавать свой фотосервис, увидев конкуренцию своей площадке со стороны Instagram. Этот сервис стал быстро наращивать популярность среди российских пользователей на мобильных устройствах. По данным статистики TNS, за июль 2015 г. мобильная месячная аудитория Instagram достигла 5,1 млн, «ВКонтакте» – 9,2 млн. Пытаясь защитить свой сервис Snapster, администрация «ВКонтакте» сделала переход из своей соцсети в Instagram неудобным для пользователей: ссылки на американскую фотосоцсеть внутри «ВКонтакте» стали неактивными. Чтобы перейти по ссылке, нужно было ее скопировать и затем вставить в браузер.

В настоящее время идет работа над новым приложением и над сайтом snapster.io. В основе новой соцсети будет концепция «фотокомнат». Это, по сути, такие же паблики и сообщества, как в «ВКонтакте», но с обязательной картинкой к каждому посту. Для любой «комнаты» можно будет назначить нескольких авторов, которые смогут публиковать или редактировать фотографии и текст. Источник отметил, что в новом сервисе все фотографии не будут перемешиваться в единой новостной ленте, как это происходит в Instagram или «ВКонтакте».

«Когда площадка становится неудобной, с нее начинают уходить. В Instagram много спама, из-за этого читать комментарии и общаться там невозможно. И здесь нишу может занять Snapster. Известно, что “ВКонтакте” удачно борется со спамом, и если это сохранится в новом сервисе, будет

отлично, – рассуждает блогер А. Коробков-Землянский. – “ВКонтакте” надо обратить внимание на зарождающиеся тренды – например, дать возможность делать видеотрансляции в Snapster. Этим бы они выделились на фоне Instagram. Им нужен новый функционал, из-за которого к ним пойдут», – заявил А. Коробков-Землянский.

У «ВКонтакте» уже были попытки создать сторонние сервисы на основе основной соцсети. Это, например, сервис по поиску работы «ВШтате» и видеосервис «ВКадре». Они не нашли поддержки у пользователей и в результате через какое-то время были закрыты.

В пресс-службе «ВКонтакте» не прокомментировали информацию о создании новой соцсети. «Подробности развития Snapster мы сообщим позже», – отметил официальный представитель соцсети Г. Лобушкин ***(«ВКонтакте» готовит «убийцу» Instagram // InternetUA (http://internetua.com/vkontakte--gotovit--ubiicu--Instagram). – 2016. – 21.01).***

***

Facebook запустила раздел Sports Stadium, с помощью которого рассчитывает упростить пользователям поиск комментариев и новостей, связанных с тем или иным спортивным событием. Сообщение об этом появилось в официальном блоге компании, пишет lenta.ru.

Запуск приурочили к соревнованиям по американскому футболу, в дальнейшем планируется освещать баскетбольные и футбольные состязания.

В разделе сделали четыре вкладки. Одну отвели под относящиеся к текущему матчу комментарии друзей, во вторую попали комментарии от экспертов – спортивных комментаторов с верифицированными аккаунтами, спортсменов и других знаменитостей. Отдельные вкладки зарезервировали для текстовой трансляции матчей и для сведений о том, где ту или иную игру можно посмотреть по телевизору.

В Facebook рассчитывают, что Sports Stadium послужит дополнением к телетрансляциям. Пока сервис доступен для владельцев iPhone в США, в дальнейшем его планируют адаптировать для других платформ, на которых представлен Facebook, и расширить охват стран. Согласно подсчетам компании, среди пользователей социальной сети насчитывается 650 млн спортивных фанатов ***(Facebook дал юзерам повод не отрываться от социальной сети при просмотре матчей // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45959/118/lang,ru/). – 2016. – 21.01).***

***

Сервис микроблоггинга Sina Weibo, популярный в Китае настолько, что его называют «китайским Twitter», скоро отменит ограничение длины сообщения в 140 символов. Об этом сообщает агентство «Синьхуа» со ссылкой на сообщение в Weibo, которое разместил в среду генеральный директор сервиса В. Гаофэй.

Часть пользователей сможет воспользоваться сервисом в новом формате в тестовом режиме уже с 28 января, а с 28 февраля ограничение будет отменено для всех пользователей.

Отображаться будет, как и прежде, 140 символов, но внизу появится ссылка. Чтобы читать сообщение дальше, нужно будет щёлкнуть по ней ***(«Китайский Твиттер» отменит лимит в 140 знаков с 28 января // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2016/01/20/Weibo-remove-140-character-limit.html). – 2016. – 21.01).***

***

Количество украинских пользователей в Facebook возросло на 30 % за год. В абсолютных цифрах прирост составил 1,2 млн, сообщает watcher.com.ua. По состоянию на январь 2015 г. в Украине было 3850 тыс. пользователей Facebook, в январе 2016 г. эта цифра составила 5 млн. По методологии Facebook пользователями соцсети являются люди, которые хотя бы раз в течение последних 30 дней заходили в соцсеть, будучи при этом залогинены. Статистика не учитывает, например, зарегистрированных пользователей, которые не заходят в соцсеть в течение последних 30 дней, а также людей, которые не зарегистрированы в соцсети, но просматривают ее контент ***(Количество украинских пользователей в Facebook выросло на 30 % за год // Marketing Media Review (http://mmr.ua/show/kolichestvo_ukrainskih_polyzovateley_v_facebook_vyroslo_na_30_za_god). – 2016. – 25.01).***

***

Компания Facebook намерена тесно интегрировать принадлежащий ей мессенджер WhatsApp с функциями социальной сети. Об этом сообщил независимый разработчик Х. Сантос, который изучил бета-версию WhatsApp для Android и обнаружил в настройках приложения новую опцию, позволяющую поделиться некоторой информацией об аккаунте с Facebook.

Включив эту опцию, пользователи помогут «улучшить опыт Facebook». Тем не менее, не уточняется, какой именно информацией мессенджер будет обмениваться с социальной сетью. Можно предположить, что приложение начнет получать данные о «лайках», чтобы пользователю было проще связаться с брендами посредством WhatsApp.

Кроме того, тесная интеграция с Facebook позволит превратить WhatsApp в полноценную социальную сеть. В настоящее время пользователи мессенджера могут находить новых друзей только зная их телефонный номер.

Также в бета-версии Android-приложения WhatsApp появился новый раздел, разъясняющий нюансы шифрования сообщений. Там сказано, что программа использует метод сквозного шифрования (end-to-end) – из одного конца в другой, так чтобы содержимое послания могли видеть только отправитель и получатель, но не третье лицо, включая сам WhatsApp

(WhatsApp начнут интегрировать с Facebook // InternetUA (http://internetua.com/WhatsApp-nacsnut-integrirovat-s-Facebook). – 2016. – 26.01).

***

Птичка спела: почему из Twitter уходят топ-менеджеры

Утром 25 января в прессе появились сообщения, что компанию Twitter покидает сразу пять топ-менеджеров. Речь шла о руководителе инженерного подразделения А. Реттере, главе HR-департамента Б. Шиппере, руководителе департамента по продукту К. Вайли, руководителе медиадепартамента К. Стэнтон и руководителе видеосервиса Vine Д. Тоффе, пишет Forbes Украина.

Каждый из них проработал в компании несколько лет. Позже, в тот же день, CEO Twitter Д. Дорси подтвердил, что информация об уходе с руководящих постов пятерых сотрудников соответствует действительности.

Впрочем, как сообщают инсайдеры, массовый уход топ-менеджеров предприниматель не считает проблемой. Это была его собственная инициатива.

«Свежим голосом» Д. Дорси стало предложение о сокращении 8 % сотрудников компании. Из 4100 людей, которые трудились в Twitter, новый CEO уволит 336. Д. Дорси уверен, что сокращение персонала поможет уменьшить затраты и сконцентрировать внимание на развитии сервиса. Чтобы снизить напряжение в компании, он даже пообещал отдать 1 % своих акций в качестве премии всем сотрудникам.

Вместе с тем Д. Дорси начал активно реорганизовывать компанию, запуская новые сервисы и отсекая старые уникальные «фишки». В начале октября появилась информация, что в сервисе появится кнопка Buy Now, которую торговые площадки смогут добавлять под своими товарами. Согласно данным Twitter, в появлении подобной функции было заинтересовано свыше 150 тыс. сообществ внутри сервиса.

Тогда же появилась и новая функция под названием Moments. Это подборка новостей, видео, картинок и другого контента, соответствующего одной теме. К примеру, важному спортивному соревнованию. Весь контент отбирается вручную кураторами по мере развития событий.

Для пользователя Moments должен был стать удобным способом потребления тематического контента. В целях развития нового направления Twitter подписал соглашения о сотрудничестве с популярными изданиями, которые помогут в формировании подборок.

Наиболее значительные перемены ожидают Twitter уже в I квартале текущего года. Д. Дорси лично подтвердил, что сервис микроблогов больше не будет таковым: каноническое ограничение в 140 символов уберут, и пользователи смогут писать рассказы до 10 тыс. символов.

«Twitter не начинался с ограничения в 140 символов. Мы сделали это на первых этапах, для того чтобы уместиться в одно sms-сообщение (160 символов)», – отметил Д. Дорси, поясняя причины снятия текстового лимита,

которое станет одним из самых больших изменений со времен запуска проекта в далеком 2006-м.

Впрочем, акционеров и инвесторов реформы, проведенные под руководством Д. Дорси, не впечатлили. За последние полгода стоимость акций Twitter упала вдвое, с 35 до 17 дол. за штуку. Капитализация компании просела до ничтожных 12 млрд, хотя еще не так давно Twitter оценивался в 32 млрд дол. В чем же дело?

Причиной такого падения называют опять-таки медленное развитие сервиса. Представитель Firsthand Technology Value Fund – фонда, владеющего акциями компании – К. Ландис после прихода Д. Дорси предупредил, что новому CEO необходимо сконцентрироваться на инновациях и активном развитии. «Самое страшное, что сейчас Twitter выглядит точно так же, как и два года тому назад», – констатировал К. Ландис ***(Кабачинский И. Птичка спела: почему из Twitter уходят топ-менеджеры // Forbes Украина (http://forbes.ua/business/1409741-ptichka-spela-pochemu-iz-twitter-uhodyat-top-menedzhery). – 2016. – 26.01).***

***

Facebook исполнит давнюю мечту пользователей соцсети

Основатель Facebook М. Цукерберг наконец-то прислушался к мольбам пользователей популярнейшей социальной сети. По информации издания Bloomberg, сотрудники компании работают над проектом Reactions, при помощи которого любой желающий сможет выразить свои эмоции по поводу поста одним нажатием кнопки Like («Нравится»), пишет RG Digital.

Речь идет об усовершенствовании стандартного «лайка». Многие пользователи уже давно отмечали, что одной этой кнопки недостаточно, чтобы показать весь спектр своих эмоций. Например, в посте-некрологе кнопка Like, равно как и Dislike, была бы явно неуместна. Поэтому разработчики решили добавить к «лайку» сразу шесть универсальных смайликов, изображающих разные эмоции: Love, Haha, Yay, Wow, Sad и Angry.

Над проектом работает вице-президент по продуктам Facebook К. Кокс. По сообщению журналистов, новый «лайк» уже прошел тестирование в нескольких странах: эмотиконы опробовали в Испании, Чили, Португалии, Филиппинах и Японии. Кроме того, шесть новых эмоций успешно закончили испытания в Великобритании и США. В скором времени проект должен запуститься во всем мире.

«Пользователи просили о кнопке “Не нравится” многие годы, – заявил он в ходе конференции в штаб-квартире соцсети в Калифорнии. – Мы услышали эту просьбу и работаем над тем, чтобы ответить нуждам всего сообщества» ***(Facebook исполнит давнюю мечту пользователей соцсети // Grifonsoft (http://grifonsoft.ru/news/4217-new-like-button.html). – 2016. – 28.01).***

***

Гиганты интернет-торговли и социальные сети могут в скором времени потеснить традиционные банки на рынке финансовых услуг. Об этом в интервью заявил глава консалтинговой и аудиторской компании PwC International Д. Нелли.

«Банки в том виде, в котором мы их знаем сегодня, полностью изменятся в ближайшем будущем. Этот сектор претерпит глубочайшие изменения в результате использования новых технологий», – сказал он. По мнению Д. Нелли, компании, специализирующиеся на интернет-торговле, в частности китайская Alibaba и американский Amazon, а также социальная сеть Facebook смогут скоро составить конкуренцию обычным банкам благодаря накопленным базам данных о пользователях.

«Эти организации идут в финансовые услуги, создают собственные банки и с помощью больших данных начинают оказывать услуги, похожие на услуги традиционных банков», – сказал глава PwC International.

«Традиционные банки начинают агрессивно использовать новые технологии, для того чтобы менять свои модели бизнеса и оставаться конкурентоспособными», – сказал Д. Нелли ***(Alibaba и Facebook могут потеснить традиционные банки, – эксперт // Finance.ua (http://news.finance.ua/ru/news/-/367532/alibaba-i-facebook-mogut-potesnit-traditsionnye-banki-ekspert). – 2016. – 19.01).***

***

Facebook уже имеет свой веб-браузер, хотя и в виде встроенного в мобильное приложение Facebook. Таким образом, Facebook позволяет пользователям самой популярной социальной сети быстрое открытие веб-сайтов без необходимости выхода из приложения Facebook. При нажатии на ссылку меняется, правда, интерфейс программы, но это все тот же Facebook.

Похоже, что команда Facebook тестирует новое воплощение своего встроенного браузера в виде полноценной программы. В сети появился скриншот тестовой версии нового браузера Facebook, который разместил Г. Уилмер с BBC.

До сих пор встроенный веб-браузер Facebook позволяет загрузить веб-страницу из готовой ссылки, на этом его возможности заканчиваются. Тестируемая новая версия, по-видимому, содержит адресную строку, с помощью которой можно открыть любую веб-страницу. Браузер имеет также систему закладок и пару других популярных решений, которые можно встретить в независимых интернет-браузерах.

Решение Facebook до сих пор значительно уступает конкурентам, но новая тестовая версия четко показывает направление развития.

По неофициальным данным говорится, что тестирование нового браузера, встроенного в приложение Facebook, продолжается с начала декабря прошлого года. Пока не известно, когда команда Facebook намерена выпустить финальную версию ***(Кошманюк Я. Facebook тестирует собственный***

браузер // Prostotech (http://prostotech.com/internet/2671-facebook-testiruet-sobstvennyj-brauzer.html). – 2016. – 19.01).

***

Facebook запускает новую функцию, которая позволит людям вести прямые видеотрансляции, а также показывать своим друзьям жизнь в режиме реального времени, пишет Vector News.

Помимо знакомых пользователя видео смогут смотреть и другие люди социальной сети по всему миру, если поставить соответствующие настройки.

Вероятно, в компании решили обойти Twitter, который ранее выпустил приложение для передачи потокового видео под название «Перископ», имеющие схожую функциональность.

Отмечается, что после трансляции с телефона видеопоток пользователя будет размещен в ленте новостей, и это видео смогут увидеть друзья в записи ***(Facebook запускает новую функцию // Vector News (http://vnews.agency/news/technology/27197-facebook-zapuskaet-novuyu-funkciyu.html). – 2016. – 30.01).***

***

Компания Google объявила об окончательном отделении социальной сети Google+ от ещё одного своего продукта – Play Games, сообщает «Багнет» со ссылкой на 3DNews.

Если раньше для активации аккаунта на игровой платформе был необходим аккаунт в социальной сети, то теперь Play Games будет оснащена новой системой входа. В дополнение к этому игрокам теперь понадобится войти в свой аккаунт лишь один раз на каждом устройстве – ранее вход осуществлялся при каждой загрузке игры с поддержкой платформы.

Google объяснила в своём блоге, что такой подход нацелен на уменьшение количества проблем со входом и, в частности, на снижение числа ненужных запросов, направленных на серверы компании. Однако во многом такой ход важен потому, что он является ещё одним большим шагом к отделению от Google+ – проекта, который некогда был для компании одним из самых ключевых. Прошлым летом пропала необходимость в наличии аккаунта в социальной сети для входа в YouTube, после чего фотосервисы компании также стали независимы от Google+.

Если учесть, что на сегодняшний день зарегистрировано примерно 1,5 млрд активных устройств на базе Android, то можно лишь догадываться, сколько аккаунтов в социальной сети компании было создано только ради возможности использовать Play Games. Аккаунты эти, конечно, закрыты не будут, но в будущем игроки на Android никак к Google+ привязаны не будут ***(Google разделила Google+ и свою игровую платформу // Багнет (http://www.bagnet.org/news/tech/279744). – 2016. – 26.01).***

***

Імперія Facebook: далі – тільки вниз?

Першою насправді масовою соціальною мережею у світі став MySpace, але сьогодні про неї вже мало хто пам’ятає.

У світі сучасних медіа-платформ зміни відбуваються настільки швидко, що MySpace, мабуть, і не помітила наближення свого кінця. У певний момент вона перестала надавати сервіс, який від неї очікували, і бути лідером інновацій. «MySpace схожа на сайт 2004 року», – казали користувачі, які надали перевагу Facebook.

Виявляється, для соціальної мережі оцінка користувача – це все, що має значення. Навіть якщо ми не живемо в часи нової спекулятивної бульбашки доткомів, хоча подібних свідчень вистачає, компанії народжуються, щоб стати лідерами, та йдуть у небуття, щоб назавжди спочити в базі даних великого хмарного сервісу.

Зворотний відлік

Прогнозів щодо приреченості Facebook багато. Наступний особливо цікавий, і не тільки тому, що підготовлений дослідниками Принстонського університету, а й тому, що в ньому порівнюється розвиток соцмереж з поширенням епідемій. Дослідники стверджують, що Facebook, як і бубонна чума, зійде нанівець.

За даними вчених, що базуються на кількості пошукових запитів у Google, Facebook поширювалася як інфекційне захворювання. Проте з часом люди стають все стійкішими до нього, тому мережа може втратити левову частку активних користувачів до кінця 2017 р. За іншим сценарієм – до 2020 р.

У будь-якому випадку те, як ми використовуємо соцмережі, і те, для чого вони нам потрібні, швидко змінюється. Facebook стає пасивним центром соціальних взаємодій в Інтернеті, принаймні на ключових ринках США та Великобританії.

Дедалі частіше користувачі відвідують свої сторінки, щоб перевірити повідомлення, без активної взаємодії з іншими користувачами. Тимчасом дрібніші мережі та додатки для мобільних телефонів забирають все більшу частину аудиторії.

...і статистика

У компанії Facebook поспішили спростувати та висміяти дослідження, його методологію та авторів. Заявили, що з таким же успіхом зникнуть і абітурієнти університету. Однак все не так однозначно, як про це жартують у Facebook.

Компанія стикається з негативною демографічною тенденцією. З 2011 р. по 2013 р. кількість підлітків – користувачів мережі скоротилася приблизно на 25 %, тоді як кількість користувачів від 55 років і більше зросла на 88 %. «Старіння» мережі навряд чи може бути ознакою майбутнього розвитку.

Іншою проблемою стає «розмивання» уваги користувачів. Якщо у 2012 р. користувач Facebook у середньому був активний лише на 2,5 платформи соцмереж, то нині він використовує 4,1 платформи.

За даними GlobalWebIndex – GWI – за I квартал 2015 р., кількість активних користувачів Facebook за два роки знизилася з 53 до 42 %. Facebook – єдина велика мережа, активне використання якої впало протягом 2014 р. – мінус 9 %.

Чому тоді Facebook продовжує звітувати про збільшення активного використання мережі? Як часто буває із статистикою, це питання визначень. Якщо порівняти дані GWI про відвідувачів та активних користувачів, то все стає зрозумілим. Темпи відвідування залишалися стабільними, тоді як активність використання падала. Тож навіть якщо люди не почнуть знищувати акаунти вже завтра, можна впевнено сказати, що взаємодія користувачів з мережею пішла на спад.

Facebook vs адепти вільного ринку

Однак проблеми можуть чекати на Facebook не тільки з боку користувачів.

Більшість маркетологів не впевнені, що їх маркетинг у Facebook ефективний. За дослідженням Global Web Index Social за I квартал 2015 р., тільки 45 % маркетологів вважали, що їх зусилля у Facebook працюють. Особливо погоджувалися з цим маркетологи, націлені на споживачів: 51 % опитаних.

Як повідомляє digiday.com, у 30 найбільш залежних від мережі видань – The Huffington Post, Fox News, Buzzfeed – із січня по жовтень 2015 р. трафік впав на 32 %, а серед топ-10 – на 42,7 %. Чим більше ресурс покладався на соцмережу, тим більшим було падіння. Проте Facebook знову спростовувала наявність проблеми.

Не секрет, що Facebook має чітку стратегію відтворення всього зовнішнього Інтернету під брендом Facebook, щоб користувачам не було необхідності залишати «кордони» мережі. Це веде до необхідності для власників майже будь-якого бізнесу мати сторінку в мережі, щоб їх бізнес функціонував нормально.

Однак часто змінюючи алгоритми показу подій у стрічці новин, мережа знижує охоплення аудиторії для таких сторінок, змушуючи компанії платити за рекламу.

Схоже, Facebook намагається залишити єдиний шлях для зростання аудиторії компаній у мережі – тільки через рекламу. Стає все більш очевидним, що Facebook – це лише ще один рекламний майданчик, який насправді нічого не пропонує користувачам і все дорожче продає свої послуги рекламодавцям.

Монетизація може бути непростою справою, якщо у вас нема почуття міри.

Крах єдинорогів?

Труднощі Facebook можуть мати і зовнішні причини. Це може стати проблемою для всієї високотехнологічної галузі, якщо уявити, що на зміну доткомам прийшли єдинороги – стартапи, які оцінюються більш ніж 1 млрд дол.

На думку венчурного капіталіста Д. Бреєра, який інвестує з 1987 р. та був свідком не одного економічного циклу, кінець нинішнього циклу з імовірністю 50 % слід очікувати протягом одного-двох років.

Водночас мільярдер М. Кубан, який заробив на бульбашці доткомів на початку 2000-х, встигнувши продати свою частину Broadcast.com за 5,7 млрд дол., також вважає, що сценарій повторюється, або буде набагато гірший сценарій.

Він пише, що занепокоєний високими очікуваннями від стартапів. На думку автора, якщо минулого разу технологічна бульбашка поховала гігантів – Broadcast.com, AOL, Netscape, – то цього разу це можуть бути Uber, Twitter і Facebook.

Крім того, додає він, індекс технологічного ринку Nasdaq перебуває близько до рівнів краху доткомів. Хоча багато аналітиків вважають, що нині галузь більш зріла, питання залишається відкритим, особливо коли на ринку є всі ознаки бульбашки.

Не останньою причиною нинішнього буму технологічних компаній стала ера дешевих грошей після початку програми кількісного пом'якшення в США.

Цей час вже добіг кінця. Тепер компаніям доведеться довести, що їх бізнес-модель може існувати в умовах конкурентного ринку, а не тільки тоді, коли в них інвестували мільйони задовго до їх прибуткової роботи.

Цукрова гора для М. Цукерберга

Багатомільярдна капіталізація Facebook майже повністю залежить від величезної бази користувачів мережі та очікування невпинного зростання, що компанія і намагається показувати кожен квартал. Проте у світлі перерахованих факторів майбутнє компанії не здається таким вже безхмарним.

Якщо процес накопичення та утримування користувачів піде у зворотному напрямі, це може швидко призвести до важких наслідків.

На початку ери Facebook М. Цукерберг, здавалося, пропонував світу нову вільну соціальну мережу для всіх, але сьогодні це все менше схоже на правду. Коли ця ідея вкорениться в умах критичної маси користувачів, буде занадто пізно.

Як і будь-яка імперія, Facebook охоче стає все більш зарегульованою системою, забуваючи, що її влада і багатство в кінцевому підсумку походить від користувачів системи, а отже, може бути відкликана в будь-який момент.

Можливо, не слід очікувати краху Facebook «найближчими днями», але якщо побудувати графік для будь-якої системи, то можна побачити тенденцію: якщо рухатися вгору вже нема куди, залишається лише один шлях ***(Дубенський В. Імперія Facebook: далі – тільки вниз? // Економічна правда (http://www.epravda.com.ua/publications/2016/01/29/578128/). – 2016. – 29.01).***

***

Приложение, созданное украинскими разработчиками, носит название One Day Auction (ODA). Оно объединяет в себе социальную сеть, торговую и образовательную площадки.

Как рассказала НВ О. Никитова, CEO ODA, в мире существуют площадки по продаже предметов искусства (к примеру, Paddle8, ArtNet, Artsy, Saatchi Online). Однако идея объединения ее с социальной сетью – ноу-хау, которого у конкурентов нет.

По словам О. Никитовой, на ODA пользователи смогут ставить лайки и оставлять комментарии, читать о художниках и скульпторах, подписываться на дополнительные сервисы. Вскоре возможностей станет еще больше. Приложение обзаведется группами по интересам, лентой активности друзей и списком лайков. Кроме того, пользователи смогут следить за выставками, аукционами и другими культурными событиями и создавать ивенты.

Совершать покупки на ODA можно через однодневные аукционы. Работы, не купленные в ходе торгов, не будут пропадать. Их также можно будет купить, но «по другой цене и без азарта аукционных торгов», отмечает О. Никитова.

«Мировой рынок онлайн-продаж предметов искусства постоянно растет. – рассказывает О. Никитова. – В 2013 г. объем мирового онлайн арт-рынка в денежном выражении составил – 1,57 млрд дол., в 2014 г. этот же показатель составил 2,64 млрд дол. Прогноз на 2019 г. – 6,3 млрд дол. Эта ниша на мировом рынке не заполнена. В Украине ее вовсе пока не существует».

Со временем ассортимент будет включать «все, что можно коллекционировать – от предметов декоративно-прикладного искусства и живописи, до коллекционного вина и раритетных автомобилей».

Выставлять работы для демонстрации и покупки на ODA смогут аукционные дома, галереи и частные дилеры. Причем перед этим им потребуется пройти «надежную систему проверки». Художники смогут выставлять свои работы только через них.

Впрочем, приложение должно заинтересовать не только профессионалов. «Аудитория огромна, как в Украине, так и в мировом масштабе. Это все, кому интересно искусство. И не только его покупка или продажа, но и изучение», – говорит CEO One Day Auction.

Образовательная часть на ODA будет обеспечиваться контентом, собираемым со всего мира и обновляемым ежедневно. Таким образом, приложение будет служить «библиотекой по искусству разных стран мира».

Приложение работает со всеми видами мобильных платформ, и доступно бесплатно ***(В Украине создана соцсеть для любителей искусства // Sostav.ua (http://sostav.ua/publication/v-ukraine-sozdana-sotsset-dlya-lyubitelej-iskusstva-69893.html). – 2016. – 29.01).***

***

Facebook установил, что 934 млн пользователей социальной сети ежедневно заходили в свои учетные записи в IV квартале 2015 г., используя мобильные устройства. Об этом свидетельствует финотчет, опубликованный на сайте компании, пишет lenta.ru

Общее число юзеров, которые ежедневно прибегали к услугам ресурса в IV квартале, составило 1,04 млрд человек, как указывается в документе. Соответственно, только 10 % из них использовали для доступа к соцсети десктопную версию Facebook. Число ежемесячно активных в Facebook пользователей по итогам IV квартала возросло на 14 % по сравнению с аналогичным периодом за 2014 г. и составило 1,59 млрд. Согласно отчетности, прибыль Facebook за весь 2015 г. возросла на 25 % – с 2,94 млрд до 3,69 млрд дол. ***(Facebook пересчитал активных пользователей мобильной версии соцсети // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/46049/118/lang,ru/). – 2016. – 29.01).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Компанія Burson-Marsteller провела дослідження World Leaders on Facebook, яке включає аналіз активності акаунтів політиків та державних інституцій у соціальній мережі Facebook.

Згідно з даними дослідження, сторінка Адміністрації Президента України опинилася на шостому місці у світі за кількістю чекінів у Facebook ***(Адміністрація Президента України стала однією з найпопулярніших державних інституцій в світі за кількістю чекінів // UkrainianWatcher (http://watcher.com.ua/2016/01/19/administratsiya-prezydenta-ukrayiny-stala-odniyeyu-z-naypopulyarnishyh-derzhavnyh-instytutsiy-v-sviti-za-kilkistyu-chekiniv/). – 2016. – 19.01).***

***

Голова Верховної Ради України В. Гройсман перед погоджувальною радою лідерів депутатських фракцій і груп, голів парламентських комітетів виступив із відеозверненням на своїй сторінці в соціальній мережі Facebook. Він зауважив, що започатковує такі «прямі трансляції» щопонеділка для обміну думками з людьми, врахування пропозицій і зауважень, зокрема, до порядку денного парламенту, щодо ухвалення важливих рішень, які допоможуть провести зміни в державі.

Голова Верховної Ради повідомив, що невдовзі такі «прямі трансляції» будуть започатковані й в інших соціальних мережах. «Раціональні думки, гарні поради будуть враховуватися», – пообіцяв керівник парламенту ***(Голова Верховної Ради започаткував «прямі трансляції» в соціальних мережах // Голос України: Інформаційний портал (http://golosukraine.com/publication/politika/ukrayina/52163-golovnim-prioritetom-na-2016-rik-ye-ekonomika-groj/). – 2016. – 25.01).***

***

Депутат Херсонского областного совета А. Шумей предложил реорганизовать официальную страничку Облсовета на Facebook таким образом, чтобы каждый депутат мог непосредственно выставлять свои выступления и материалы на страницу совета.

Аргументы депутата следующие: права администратора должны быть у депутатов всех фракций, а также у представителя областного совета.

Это вызвало немало комментариев со стороны общественности.

Так, политический эксперт и представитель КИУ В Херсонской области Д. Белый считает это хорошим предложением и тут же комментирует на своей Facebook странице. «Идея депутата в духе открытости электронной демократии. Конечно же, это еще непривычно для всех нас. Но за таким подходом депутата – будущее. И пусть аппарат поможет всем депутатам открыть свои профили в Фейсбуке – и пусть они пишут по каждому вопросу. А мы будем смотреть и, надеюсь, не прозревать, а сопереживать», – объясняет эксперт.

Д. Белый добавил, что по его «подсчетам только треть депутатов имеют страницы в социальной сети. Еще меньше – активно в них пишут». Такое предложение, по мнению эксперта, должно стать хорошим стимулом для развития областного совета».

По мнению многих пользователей сети, это даст возможность ускорить процесс взаимодействия между депутатом и жителями области, обратиться к народному избраннику напрямую и сделать это в считанные секунды.

Нашлись и противники такого предложения депутата, т. к. считают, что для того, чтобы партиец мог высказаться, существуют личные профили, а также виртуальные группы фракций.

По мнению Д. Белого, «странички фракций – это странички фракций. Это монолог. Нужен – открытый диалог. Кстати, это можно достичь только если это будет не страница, а открытая группа» ***(С проблемой ознакомлюсь на Facebook: депутат Херсонского облсовета за обсуждение вопросов виртуально // Херсонские Вести (http://visti.ks.ua/novosti/novosti-hersona/24010-s-problemoy-oznakomlyus-na-facebook-deputat-hersonskogo-oblsoveta-za-obsuzhdenie-voprosov-virtualno.html). – 2016. – 20.01).***

***

Чернігівська обласна державна адміністрація активізує роботу з упровадження електронного урядування.

Перший крок – надання публічних послуг в електронному вигляді. Про це Високому Валу повідомили в прес-службі облдержадміністрації.

«Як показує практика, досвід інших областей і недержавних організацій, запит суспільства на електронний формат будь-яких послуг є дійсно високим. Сучасні інформаційні технології потенційно дають змогу звертатися до органів влади, передавати й отримувати засвідчені копії, оформлювати довідки тощо заочно, через мережу Інтернет. Зрозуміло, що люди хочуть, аби така потенційна

можливість використовувалася на практиці», – переконаний голова ОДА В. Куліч.

Загалом для спрощення отримання адміністративних послуг в Україні має діяти Єдиний державний портал. Проте наразі функціонує лише його пілотна версія, яка надає інформацію про порядок і механізми одержання послуг, однак громадянам все одно доводиться ходити за ними по державних установах.

Саме тому Чернігівська ОДА налагоджує співпрацю з розробленим волонтерами порталом публічних послуг iGov.org.ua, який працює вже сьогодні. Перша послуга, яка стала доступною на Чернігівщині, – електронне звернення до голови ОДА. Подане через Інтернет, воно буде зареєстроване і розглянуте так само, як і паперове, але швидше й зручніше для заявника.

Спектр публічних послуг, які надаватимуться жителям Чернігівщини через Інтернет, постійно розширюватиметься. Надалі планується підключити до iGov послугу з надання доступу до публічної інформації. Після погодження з Міністерством економічного розвитку – послугу з надання разової ліцензії на здійснення суб'єктами ЗЕД зовнішньоекономічних операцій.

Для цього також уже сьогодні йде робота над створенням принципово нового сайту облдержадміністрації, який буде мати не лише інформативні, а й сервісні функції, надаватиме адміністративні послуги ***(Чернігівщина долучається до iGov // Високий вал (http://val.ua/uk/85122.html). – 2016. – 19.01).***

***

У соціальній мережі Facebook розпочав роботу проект «Побудовано в Івано-Франківську», який збирає, систематизує та публікує всю інформацію про будівництво, будівельні компанії та їхні об'єкти.

Автори проекту наголошують, що «Побудовано в Івано-Франківську» має на меті виявляти та не допускати в майбутньому будівельні афери та конфліктні ситуації за прикладом будинку по вулиці Мазепи, 35а в Івано-Франківську, коли мешканці новобудови стали заручником недобросовісного будівельника, передає колреспондент Фіртки.

«Для цього створено спеціальну рубрику "Чорний список забудов", публікуватиму інформацію про конфліктні, скандальні та сумнівні об'єкти. Список формується на основі публікацій в ЗМІ, відповідей на інформаційні запити та офіційні документи. Рубрика постійно оновлюватиметься», – кажуть активісти.

Проект «Побудовано в Івано-Франківську» на сьогодні працює тільки у Facebook. Тут, на публічній сторінці проекту, автори проекту готують новини, опитування, формують рейтинги, ТОП-5, списки корисних посилань та публікації щотижневих рубрик «Будівельна інспекція», «Забудівник під контролем», «Перший серед своїх», «Прокол тижня», «Цифра дня», «Ексклюзивно. Незаконно» ***(В Івано-Франківську формують «чорний список забудов» // Агенція новин Fіrtka.if.ua (http://www.firtka.if.ua/?action=show&id=97171). – 2016. – 19.01).***

***

Діяльність ініціативи Facebook буде спрямована на розробку методів протидії мові ненависті та поширення екстремізму онлайн. Проект сприятиме науковому вивченню тематики.

Компанія Facebook спробує зупинити зростання кількості негативних та агресивних коментарів, які поширюються на сторінках соціальної мережі. Для цього американська компанія за підтримки державних та громадських організацій запускає «Ініціативу громадської сміливості онлайн», заявила комерційний директор Facebook Ш. Сандберг у понеділок, 18 січня, перебуваючи в Берліні, повідомляє агентство AFP.

«Facebook – не місце для поширення мови ненависті чи закликів до насильства», – зазначила Ш. Сандберг. Ініціатива надасть неурядовим організаціям, чия діяльність пов'язана з боротьбою проти екстремізму, фінансову підтримку на суму близько 1 млн дол. США. Крім того, компанія має намір надавати консультації у сфері маркетингу. У рамках ініціативи планується, зокрема, розробити методи протидії екстремізму та сприяти науковому дослідженню цієї тематики.

Якщо до ініціативи долучаться й інші компанії, Facebook готова фінансувати цей проект у довгостроковій перспективі. Найпізніше за рік учасники проекту мають продемонструвати перші результати роботи, тобто представити методи для ефективної боротьби з онлайн-екстремізмом, зазначив менеджер зі зв'язків із громадськістю Facebook у Європі Р. Аллен.

Головний офіс ініціативи розташовуватиметься в Німеччині, де кількість активних користувачів соціальної мережі Facebook сягає приблизно 27 млн. Діяльність організації поширюватиметься й на інші європейські країни.

Німецький політолог П. Нойманн, який долучився до проекту, вважає, що видалення коментарів, які містять мову ненависті, упродовж 24 годин після публікації – лише один крок на шляху до розв'язання проблеми поширення мови ненависті онлайн. На його думку, щоб не вдаватися до тотальної цензури, потрібно створювати альтернативний громадський простір в Інтернеті, через який можна протидіяти негативу.

Крім того, за його словами, треба краще розуміти взаємозв'язок між процесом поширення ненависті онлайн та реальним насильством. Також варто активніше залучати поліцію та спецслужби до виявлення онлайн-екстремістів ***(Соколовська Н. Facebook запустить ініціативу проти мови ненависті в інтернеті // Deutsche Welle (http://www.dw.com/uk/facebook-запустить-ініціативу-проти-мови-ненависті-в-інтернеті/a-18988067?maca=ukr-rss-ukrnet-ukr-all-3816-xml). – 2016. – 18.01).***

***

Головний операційний директор Facebook Ш. Сандберг вважає, що перемогти терористичне угруповання «Ісламська держава» можна за допомогою «лайків» у соцмережі

Ш. Сандберг заявила про це в рамках Всесвітнього економічного форуму у Давосі в контексті своєї мови про те, як боротися з небезпечними угрупованнями в мережі, передає depo.ua з посиланням на The Guardian.

Вона також навела приклад того, як користувачі соцмережі раніше «атакували лайками» групу з неонацистськими поглядами. «Найкращий спосіб висловлювати протест проти вербування ІДІЛ – це голоси людей, які були завербовані, усвідомили свій досвід, вибралися і повернулися назад, щоб розповісти правду», – вважає Ш. Сандберг.

Проблема боротьби з бойовиками в мережі займає розуми і політиків, і глав технологічних компаній ***(Топ-менеджер «Фейсбук» пропонує боротися з ІДІЛ «лайками» // Depo.ua (http://www.depo.ua/ukr/svit/top-menedzher-feysbuk-proponue-borotisya-z-idil-laykami--22012016160600). – 2016. – 22.01).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Facebook запустила инструмент «Оптимизация аудитории», который поможет издателям достигнуть релевантной аудитории с помощью трех дополнительных характеристик: добавления к публикации тегов-интересов, ограничения охвата пользователей и показа уровня вовлечения по каждому тегу, сообщает «Телекритика» со ссылкой на VC.

Вместо того, чтобы ограничить объем всей аудитории, которая увидит заметку, к каждой публикации издатель может добавить несколько тегов, соответствующих интересам пользователей («дружба», «семья», «телевидение»). Эту опцию Facebook представила еще в декабре 2014 г.

Вторая функция – исключение нерелевантной аудитории из числа тех, кто увидит публикацию. Администратор страницы может ограничивать охват на основе локации, языка, возраста иди гендера.

Третья возможность – аналитика охвата и степени вовлечения пользователей по каждому тегу-интересу.

Новую функциональность Facebook запустит на следующей неделе среди англоязычных страниц. О внедрении опций для других рынков компания пока не сообщает ***(Facebook запустил инструмент «Оптимизация аудитории» // Телекритика (http://www.telekritika.ua/internet/2016-01-26/113049). – 2016. – 26.01).***

***

WhatsApp откроет платформу для брендов, но не для рекламы. Об этом заявил CEO Я. Кум на DLD конференции в Мюнхене. В этом году WhatsApp начнет тестировать инструменты, которые позволят потребителям общаться с интересующими их компаниями и организациями. К примеру, пользователи смогут сообщить банку о мошеннической сделке или получить уведомление о

задержании рейса. WhatsApp исключил использование сторонней рекламы, собираясь получить доход от привлечение сторонних брендов на платформу. Я. Кум отметил, что приложение откажется от ежегодной платы в 0,99 дол., чтобы больше пользователей смогли получить доступ к сервису ***(WhatsApp откроет платформу для брендов, но не для рекламы // Marketing Media Review (http://mmr.ua/show/whatsapp_otkroet_platformu_dlya_brendov__no_ne_dlya_reklamy). – 2016. – 18.01).***

***

Социальная сеть Instagram планирует укрепить свои рекламные позиции, фокусируясь на малом бизнесе и пользователях за пределами США, пишет adindex.ru

М. Левин, главный операционный директор Instagram, рассказала Financial Times, что сервис обмена фотографиями собирается как можно скорее увеличить свои доходы с помощью возможностей Facebook.

Компания купила Instagram в 2012 г. В момент покупки говорилось о том, что сервис будет независим от своего нового владельца. Теперь М. Левин заявила о том, что интеграция компаний будет усиливаться, так как Instagram хочет развивать свой рекламный бизнес.

«Когда мы запустили рекламу на Instagram два года назад, размещение было доступно только в восьми странах мира. В сентябре мы стали открыты для рекламодателей уже в 200 странах по всему миру. То, что вы видели до сих пор, – это работа с крупными брендами. Я думаю, что в 2016 г. нашу платформу будут использовать гораздо больше представителей малого бизнеса», – рассказала М. Левин в беседе с Financial Times.

Также она отметила, что глобальный отдел продаж Facebook уже начал предлагать рекламные услуги Instagram малому бизнесу, направляя их конкретным группам пользователей, как рекламу на Facebook ***(Instagram собирается использовать Facebook для продажи рекламы // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45914/118/lang,ru/). – 2016. – 18.01).***

***

60 % украинцев не обращают внимание на рекламу в мессенджерах

Для 40 % опрошенных реклама в мессенджерах – раздражающий фактор, который отвлекает от общения. Не приемлют рекламу в любых ее проявлениях 16 % респондентов. 23 % относятся к коммерческим сообщениям положительно, если информация полезна и актуальна. 12 % опрошенных готовы терпеть рекламу, так как это залог бесплатного пользования приложениями. 60 % участников исследования отметили, что вовсе не обращают внимания на рекламу в мессенджерах.

22 % респондентов акцентируют внимание на рекламе в Skype, 10 % замечают коммерческие сообщения в Viber. По результатам iVOX Ukraine, эти

два мессенджера являются самим известными среди украинских интернет-пользователей: 94 % и 84 % соответственно знают или что-то слышали о них. На третьем месте ICQ (69 %), который больше по душе людям старшего возраста. Им пользуются 14 % респондентов в возрасте 45–59, 12 % опрошенных в возрасте от 30 до 44 лет и только 9 % молодых людей, которые приняли участие в опросе.

О WhatsApp, Google Hangouts и Telegram знают 46, 30 и 24 % украинцев, которые приняли участие в опросе соответственно. Уровень осведомленности об этих приложениях среди мужчин выше, чем среди женщин. Самый высокий уровень проникновения у Skype. Им пользуются 78 % украинцев, для 46 % это любимый мессенджер. На втором месте Viber: 56 % респондентов отметили, что время от времени общаются с его помощью, 32 % являются приверженцами этого приложения.

Messenger от Facebook занимает третью позицию. Среди юзеров приложения 29 % украинских интернет-пользователей, 8 % выбирают его в качестве основного приложения для обмена сообщениями через Интернет ***(iVOX Ukraine: 60 % украинцев не обращают внимание на рекламу в мессенджерах // Marketing Media Review (http://mmr.ua/show/ivox_ukraine_60_ukraintsev_ne_obrashtayut_vnimanie_na_reklamu_v_messendzherah). – 2016. – 20.01).***

***

Крупнейшая глобальная соцсеть Facebook апгрейдила функционал своего инструмента Lead Ads, запущенного этой осенью и предоставляющего возможность размещения рекламы с автозаполнением подписных форм. Об этом пишет cossa.ru.

Теперь новый рекламный продукт Facebook, избавляющий пользователей процедуры заполнения личной информации в разных формах и анкетах на мобильных устройствах, доступен также и на десктопах.

Кроме того, социальная сеть представила два обновления в Lead Ads, разработанных специально для того, чтобы предоставить пользователям больше информации о компании, прежде чем просить их подтвердить свои данные.

Во-первых, пользователи смогут просматривать так называемые «контестные карты», которые будут появляться по клику на объявление, но до момента показа анкеты с данными. В этих карточках компании смогут разместить больше информации о себе, чтобы продемонстрировать ее потенциальным покупателям.

Во-вторых, Lead Ads стали доступны в формате карусели, что позволяет рекламодателям размещать до пяти разных изображений с заголовками, которые увидят пользователи, прежде чем перейти к анкете ***(«Фейсбук» запустил рекламу для лидов на десктопах и сделал ее карусельной // МедиаБизнес***

(http://www.mediabusiness.com.ua/content/view/45955/118/lang,ru/). – 2016. – 21.01).

***

Рекламный отдел киевского штаба «ВКонтакте» поделился с AIN.UA свежими данными, которые могут быть полезны рекламодателям. В частности, рассказал о том, как украинская аудитория реагирует на рекламу, какие возрастные категории активнее всего кликают по объявлениям и во сколько обходятся рекламодателям их клики. А еще назвал 15 самых крупных сообществ украинских брендов. На первом месте, как и следовало ожидать, сообщество «Розетки».

На конец 2015 г. украинская аудитория «ВКонтакте» насчитывала 13 млн человек без учета мобильных пользователей. За год количество пользователей мобильных устройств возросло на 23 %, при этом на 15 % сократилась доля десктопа и на 8 % – одновременно десктопа и мобайла. В соцсети это связывают с активным развитием мобильного Интернета в стране. Впрочем, о реакции пользователей на рекламу в зависимости от устройств во «ВКонтакте» не рассказали.

Самой отзывчивой аудиторией оказались пользователи в возрастной категории старше 35 лет. А самой дорогой – от 27 до 29 лет (цена за клик 1,92 грн).

Охотнее всего пользователи «ВКонтакте» кликают по рекламе в категориях «Развлечения» и «Красота и мода». На третьем месте по CTR «Дом и семья». Хуже всего воспринимают товары и услуги, авто/мото и финансы.

Рекламисты киевского «ВКонтакте» советуют рекламодателям внимательнее относится к изображениям, которые они присваивают своим объявлениям. «Как показал опыт, крайне важно делать предварительное тестирование изображений. Разница в конверсии одного и того же объявления с самым эффективным и самым неэффективным изображением может составлять до 300 % у одинаковой аудитории», – пояснили в компании.

В киевском штабе также сообщили, что украинская аудитория очень хорошо реагирует на видеорекламу в соцсети: CTR в пререллах достигает 6,5 %. Это короткие 30-секундные рекламные ролики, которые вставляются перед лицензионным видео во «ВКонтакте». Из настроек рекламодателям доступен таргетинг по социально-демографическим параметрам и географии. Стоимость такого формата составляет от 30 грн за тысячу показов (CPM).

Также социальная сеть опубликовала рейтинг сообществ по количеству подписчиков брендов (за исключением торговцев одеждой). На первом месте сообщество интернет-гипермаркета «Розетка» (более 750 тыс. подписчиков), на втором магазина электроники «Алло» (почти 650 тыс.), на третьем месте сообщество сети минимаркетов «АТБ» (400 тыс.). Замыкает топ-15 паблик сети магазинов техники «Фокстрот» (менее 100 тыс.) ***(«ВКонтакте» назвал топ-15 сообществ брендов и стоимость аудитории в Украине за 2015 год // AIN.UA (http://ain.ua/2016/01/21/627779). – 2016. – 21.01).***

***

Многие бренды предпочитают загружать видео прямо в Facebook – такие данные компании Quintly. Видео с YouTube составляют только одну-четвертую всех видео, размещенных брендами в социальной сети. Почти две-трети видео (65 %) были опубликованы брендами непосредственно в Facebook, и только 24 % содержали ссылки на видео в YouTube. Другое исследование компании Locowise обнаружило, что охват «родных» видео в Facebook выше, чем у видео, добавленных с YouTube – 13,2 % против 7,9 %. Согласно результатам исследования, 96,4 % размещенных видео были «родными» видео с Facebook, и только 3,5 % – с YouTube ***(Исследование: Facebook обошел YouTube по охвату видео // Marketing Media Review (http://mmr.ua/show/issledovanie_facebook_oboshel_youtube_po_ohvatu_video). – 2016. – 26.01).***

***

Сервис микроблогов отказался от показа рекламных объявлений самым активным пользователям. Об этом сообщает adindex.ru со ссылкой на издание Re/code.

За последние несколько месяцев компания сильно сократила, а в некоторых случаях прекратила показы рекламы для своих самых знаменитых и активных пользователей с большим количеством подписчиков. Для этих людей Twitter стал гораздо удобнее.

Источники Re/code утверждают, что сервис предпринял подобный шаг, чтобы увеличить вовлеченность и лояльность своих так называемых VIP-клиентов, несмотря на то, что компания в первую очередь нацелена на привлечение новой аудитории.

Twitter ограничил показ рекламы не только звездам. Одним из критериев по отбору пользователей в эту немногочисленную «элитную» группу является количество публикуемых твитов.

Сервис вполне может себе позволить выключить рекламу для небольшого количества пользователей, однако выручка Twitter в 2015 г. могла составить 2,2 млрд дол., и практически вся сумма – это доход от рекламы ***(Twitter не показывает рекламу популярным пользователям // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/46001/118/lang,ru/). – 2016. – 26.01).***

***

У Twitter з’явилися 30-секундні відеоролики формату pre-roll, пише «Телекритика». Через шість секунд перегляду рекламу можна пропустити, повідомляє Searchengines із посиланням на Digiday.

За інформацією джерел, Twitter бере 30 % доходу від реклами і віддає решту її творцям. Такі умови є більш вигідними за ті, які пропонує YouTube або Facebook, і мають залучити до мікроблогу більше якісного відеоконтенту. Деякі партнери вже бачать успіх у цій сфері.

Поки що до pre-roll мають доступ партнери програми Amplify. До них належать, зокрема Fox Sports, Fullscreen, Vox, TechCrunch, BuzzFeed ***(Twitter тестує новий формат відеореклами // Телекритика (http://www.telekritika.ua/internet/2016-01-26/113050). – 2016. – 26.01).***

***

Социальная сеть Instagram в последнее время стала показывать намного больше рекламы. Представители Facebook предупреждали об этом в июне прошлого года, заявив инвесторам, что Instagram вскоре начнёт приносить «большие деньги». Об этом пишет 3dnews.ru.

К сожалению, Facebook не предоставляет информацию о доходах от Instagram, поэтому относительно точные цифры стали доступными общественности после того, как официальный рекламный партнёр соцсети компания Brand Networks опубликовала собственный отчёт о работе.

В августе прошлого года Brand Networks осуществила 50 млн показов рекламных банеров через Instagram. Уже в сентябре эта цифра удвоилась, а в декабре она достигла 670 млн. Таким образом, менее чем за полгода количество показов рекламы увеличилось более чем в 13 раз.

Обычно увеличение количества показанных баннеров влечёт за собой сокращение их стоимости. На Instagram данная закономерность не повлияла – несмотря на то, что рекламы стало намного больше, её эффективность не уменьшилась. Судя по цифрам, предоставленным Brand Networks, цена 1000 показов в рекламы в сервисе надёжно закрепилась в районе 5 дол., за отчётный период упав на 1 дол.

О точных данных касательно общих заработков Instagram говорить сложно, так как информация была предоставлена только одним из поставщиков рекламы ***(Количество рекламы в Instagram за полгода значительно увеличилось // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/46019/118/lang,ru/). – 2016. – 27.01).***

***

Как использовать свою страницу в Facebook с пользой

Как утверждают представители компании Facebook, эта социальная сеть имеет более 1,4 млрд пользователей каждый месяц и очень привлекательна для бизнеса. Однако многие люди не умеют правильно пользоваться своим профилем. Однако если вы хотите извлечь максимальную пользу со своей странички, вам стоит воспользоваться десятью лучшими советами, которые собрал Entrepreneur, пишет Hyser.

1. Загрузите личные фотографии

Представьте, что вы ищете какого-то консультанта. Вы нажали на объявление и оказались на сайте. Все выглядит красиво и хорошо, но нигде нету ни единой фотографии самого консультанта. Если на вашей страничке в

Facebook нету ни единой фотографии или видео с вами, то вы являетесь анонимным пользователем.

2. Загружайте видео и создавайте плейлисты

Из загруженных на Facebook, но не на YouTube, видео можно создавать плейлисты. Покажите новый продукт, его возможности. Избегайте формальностей и будьте ближе к людям.

3. Используйте кнопку-призыв к действию

На страницах в Facebook могут быть кнопки-призывы к действию. Если в вашем Facebook была включена такая кнопка, то вы увидите кнопку «Создать призыв к действию» в правом нижнем углу вашей страницы. Обычно, наличие подобной функции заметно увеличивает посещение страниц. Лучше всего начать с кнопок «Смотреть видео», «Купить», «Контакты».

4. Добавляйте эксклюзивные предложения

Дайте людям повод вернуться на вашу страницу в определенные сроки. Разыгрывайте различные призы и специальные предложение в течение 24 часов. Если вы уже проводили подобные мероприятия, попробуйте еще больше ограничивать сроки – давайте людям 60 минут на выполнение каких-то условий. К примеру, можно просить сфотографироваться с вашим продуктом, выложить фото на страничке и собрать наибольшее количество голосов.

5. Проводите конкурсы

Основной причиной того, почему люди проводят так много времени на Facebook – заинтересованность. Публикуйте смешные фото и проведите конкурс среди подписчиков, чтобы как можно больше людей посещали вашу страницу. Необязательно предлагать победителям конкурсов финансовое вознаграждение, но можете предоставить скидки или небольшие подарки.

6. Взаимодействуйте с другими страницами на Facebook

Оставлять комментарии со своей страницы на других бизнес-страницах на Facebook, отметки «нравится» на страницах сотрудников, компаний, которые к вам близки, помогут более четко составить картинку того, в каком направлении вы работаете. Подобные действия направлены на то, чтобы вызвать ответную реакцию, чтобы на вашей странице тоже оставляли отметки «нравится», комментировали ваши записи и, таким образом, рекламировали вас.

7. Отмечайте различные события

Пускай ваши подписчики знают, что происходит в вашей компании. Так они будут чувствовать себя причастными к вам. Соответственно, это увеличит вероятность того, что люди будут комментировать и делать перепосты ваших записей на своих страницах. Делайте акцент на том, где вы находитесь. Это поможет увеличить аудиторию и количество заинтересованных людей за счет жителей вашего города.

8. Создавайте вкладки

Вкладки требуют ресурсов, но они помогут продемонстрировать на кого ориентирована ваша работа. Создайте вкладки, благодаря которым люди смогут связаться с вами, узнать больше информации о вашей деятельности. Это

может быть чат, история, анонсы событий, подписки, веб-семинары, различный контент, такой как книги, исследования. Это может быть что угодно, на что хватит вашей фантазии.

9. Исследуйте свои возможности

Изучите, какие заметки привлекают больше всего внимание пользователей. Вы можете спросить у своих подписчиков, что для них наиболее интересно, создав опрос на своей странице. Также вы можете экспериментировать с разным контентом. К примеру, выкладывайте один тип информации в понедельник и четверг, а другой – во вторник и пятницу. Через пару недель поменяйте дня местами. Через несколько недель вы поймете, какая информация наиболее интересна для ваших читателей.

10. Делайте ссылки на свои страницы из других социальных сетей

Facebook может стать довольно эффективной рекламой ваших профилей в Instagram, «ВКонтакте», Twitter и других соцсетей. Таким образом ваши подписчики смогут больше узнать о вас, а вы сможете более разносторонне рассказать о себе. Кроме того, это позволит вам больше развиваться, а не остановиться на создании профильной странички на Facebook ***(Как использовать свою страницу в Facebook с пользой // Hyser (http://hyser.com.ua/life_style/kak-ispolzovat-svoyu-stranicu-v-facebook-s-polzoj-11841). – 2016. – 24.01).***

***

Пять простых способов увеличить количество подписчиков в социальной сети Instagram.

1. Выкладывайте маркетинговые и упаковочные материалы.

Сделайте яркими и заметными маркетинговые материалы и продукты. Вероятность того, что кто-нибудь подумает, что у вас есть аккаунт в Instagram и станет искать вас, меньше, чем если бы вы выставляли материалы для клиентов.

2. Отправляйте продукцию авторитетам Instagram.

На какие аккаунты подписана ваша целевая аудитория? Найдите владельцев этих аккаунтов и узнайте, смогут ли они сделать для вас рекламные посты. Идеально, если они согласятся сделать пост взамен на бесплатную продукцию. Однако бывает и так, что они просят дополнительную плату за свои посты. Если на вашем сайте возможно использование промо-кодов, узнайте, согласится ли владелец популярного аккаунта на пользовательский промо-код, где вы будете платить ему. Если один из его подписчиков что-то заказывает, выигрываете и вы, и владелец популярного аккаунта.

3. Комментируйте.

Пытайтесь активнее взаимодействовать с владельцами других аккаунтов с помощью комментариев. Конечно, хорошо ставить лайки на фотографиях, но ваше имя и профиль получит больше внимания благодаря комментариям.

4. Отмечайте друзей.

Организовывайте розыгрыши, в которых вашим подписчикам надо будет отмечать друзей в комментариях. Тогда ваша аудитория приведёт больше подписчиков, которые ещё о вас не слышали. Недавно мы организовали розыгрыш, в котором наши подписчики должны были отметить в комментариях друга и написать про него историю смайликами emoji. Мы получили больше подписчиков, чем когда-либо в розыгрышах.

5. Дайте людям стимул подписаться на вас.

Дайте людям стимул, вместо того, чтобы просто говорить «Подпишитесь на нас в Instagram». Например, наша компания имеет благотворительную цель и мы вдохновляем людей подписываться на нас, чтобы увидеть результат от их покупок. Если у вас модные продукты, сообщите подписчикам, что они могут получить стильное вдохновение на вашем аккаунте. Стимулируйте их контентом, который выкладываете, вместо того, чтобы просто просить о подписке ***(5 способов увеличить количество подписчиков в Instagram // ReklaMaster.com (http://reklamaster.com/marketing-and-advertising/5-sposobov-uvelichit-kolichestvo-podpischikov-v-instagramm). – 2016. – 22.01).***

***

Свежее совместное исследование популярной микроблоговой соцсети, аналитических компаний MarketShare и Millward Brown показало, что большинство опрошенных пользователей Twitter считают себя ранними последователями брендов и охотно рекомендуют их друзьям в случае положительного опыта.

Любопытно, что таких респондентов оказалось вдвое больше среди «твиттерян» – всего 53 %, – чем среди тех, кто не пользуется микроблоговой платформой.

Twitter со своей стороны выяснил, что многие из опрошенных считают себя открытыми новому опыту и коммуникациям брендов внутри социальной сети. 34 % приверженцев мобильного онлайн-шопинга и посетителей рекрутинговых площадок признались, что читают в Twitter отзывы о товарах и услугах и смотрят другую информацию о компаниях.

Также значительная часть респондентов обращается к Twitter, чтобы задать вопросы о товарах или найти людей, которые тоже интересуются конкретным продуктом. 76 % ответили, что готовы рекомендовать бренд после персонализированной и дружественной коммуникации.

Среди других инсайтов исследования: реклама в Twitter на смартфонах на 2,4 % эффективнее, чем в других медиа; пользователи сервиса стали вовлекаться в коммуникации с брендами в 2,5 чаще, чем два года назад ***(Пользователи Твиттера стали лояльнее к брендам // Sostav.ua (http://sostav.ua/publication/polzovateli-tvittera-stali-loyalnee-k-brendam-69745.html). – 2016. – 18.01).***

***

Facebook расширила показ рекламы Audience Network на мобильный Интернет. Ранее он производился только в приложениях.

Нововведение призвано привлечь новых издателей к использованию платформы. Кроме того, оно позволит 2,5 млн текущих рекламодателей Facebook охватить более широкую аудиторию.

Audience Network для мобильного Интернета запущена в режиме беты ***(Facebook расширил охват Audience Network на мобильный интернет // Sostav.ua (http://sostav.ua/publication/facebook-rasshiril-okhvat-audience-network-na-mobilnyj-internet-69864.html). – 2016. – 27.01).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Бельгийские ученые выявили прямую зависимость между фотографией профиля, размещенной в Facebook, и перспективами занять желаемую должность. При оценке потенциального кандидата работодатели во многом полагаются на его фото в социальной сети, причем выгодный снимок может увеличить шансы попасть на собеседование до 40 %.

«Кандидат с наиболее благоприятной фотографией профиля в Facebook получил на 21 % больше положительных откликов на заявление, чем тот, который разместил наименее удачный снимок», – говорит профессор С. Баерт из Гентского университета. Чтобы убедиться в этом, исследователи разослали 2112 фальшивых резюме реальным компаниям в Бельгии, искавшим новых сотрудников.

Анкеты «соискателей» отличались только степенью образования, именами и снимками в соцсети. Кроме того, было создано столько же поддельных аккаунтов в Facebook, причем доступ к информации профиля, за исключением фотографий, был закрыт.

Как выяснилось, снимки с удачными фотографиями больше благоприятствуют получению работы. Кроме того, странички в Facebook более образованных людей проверяют чаще, чем менее образованных. Ученые связали это с тем, что последние быстрее отсеиваются в процессе рассмотрения резюме ***(Фото профиля в соцсетях влияет на карьерные перспективы // InternetUA (http://internetua.com/foto-profilya-v-socsetyah-vliyaet-na-karernie-perspektivi). – 2016. – 18.01).***

***

Британские психологи под руководством Р. Данбаро определили максимально возможное число реальных друзей, которые могут быть у пользователя социальной сети Facebook. Результаты своих исследований авторы опубликовали в Royal Society Open Science, а кратко о них сообщает ABC News.

В своей работе ученые опирались на другое исследование психолога и антрополога Р. Данбаро, проведенное в 1990-х годах, согласно которому индивид способен поддерживать устойчивые социальные связи со 100–230 людьми. Специалист получил такие результаты, изучив поведение стадных приматов и их мозговую активность.

В новой работе психологи показали, что в отношении социальных сетей, например Facebook, эта теория также верна. По мнению ученых, в среднем у человека может быть пять близких друзей и не более 150 приятелей. Остальные люди из Facebook, согласно Р. Данбаро, – просто знакомые.

В своем исследовании ученые использовали два опроса, в которых приняли участие 3,3 тыс. человек из Великобритании. Первая группа включала людей, у каждого из которых в среднем было 155 друзей в Facebook, а вторая – 183. В среднем у каждого респондента оказалось по четыре настоящих друга из Facebook. За сочувствием, но не реальной поддержкой, опрошенные могли бы обратиться к 14 своим друзьям из социальной сети.

Р. Данбаро отметил, что среди участников опроса оказались респонденты с 300 друзьями на сайте, с которыми они вряд ли хорошо знакомы. «Нам следует быть осторожными, чтобы в исследовании не учитывать профессиональных пользователей, например Д. Бибера, журналистов, конгрессменов, писателей, певцов и других, которые используют Facebook в качестве фан-клуба», – указал психолог ***(Определено число настоящих друзей в Facebook // InternetUA (http://internetua.com/opredeleno-csislo-nastoyasxih-druzei-v-Facebook). – 2016. – 21.01).***

***

По словам ведущих медицинских работников, социальная сеть Twitter, позволяет определять людей, имеющих психологические расстройства.

Как сообщают научные специалисты, им удалось проанализировать более 8 млрд сообщений от интернет-пользователей. Итоги эксперимента показали, что благодаря подобным смысловым оповещениям, ученые могут выявить часть населения, которая страдает нарушениями в работе нервной системы.

Отмечается, что при изучении поведенческих характеристик добровольцев, исследователи учитывали не только определенные слова, но и грамматические конструкции, выражения и прямые упоминания пользователей о заболеваниях. Специалисты уверены, что Twitter позволит врачам обнаружить такие недуги, как посттравматическое стрессовое расстройство, депрессию и биполярное аффективное расстройство.

Следует заметить, что все перечисленные болезни нуждаются в незамедлительном лечении, поскольку нездоровое состояние человека может со временем перейти в хроническую форму. При этом психологи утверждают, что сервис для публичного обмена сообщениями может существенно улучшить сложившуюся ситуацию.

По словам экспертов, некоторые люди предпочитают делиться своими диагнозами с другими читателями, и именно это поможет ученым контролировать уровень заболеваемости психологическими недугами в разных странах мира ***(Twitter помогает медикам ставить диагнозы // GoGetNews.info (http://www.gogetnews.info/news/health/114818-twitter-pomogaet-medikam-stavit-diagnozy.html). – 2016. – 25.01).***

Маніпулятивні технології

В YouTube з'явився відеоролик, у якому озброєні чоловіки, що представилися бійцями полку «Азов», українською та англійською мовами пообіцяли «знищувати нідерландців», якщо не буде терміново ратифікована Угода про асоціацію.

Про це пише «Європейська правда».

Ролик опублікований невідомими на новоствореному YouTube-акаунті, хоча оформлений так, щоби створити враження офіційного відео «Азову».

Його автори не приховують, що ролик створений до референдуму щодо Угоди з Україною, який відбудеться в Нідерландах 6 квітня, а аудиторією є голландські ЗМІ. Наприкінці ролика актори спалюють прапор Нідерландів.

«Азов» на офіційному сайті та на своєму YouTube-каналі спростував свою причетність до відео із закликами до терору проти Нідерландів.

В «Азові» висловили переконання, що цей ролик є «фейком від російського агітпропу» та зазначили низку помилок авторів відео. «Відсутність полкових шевронів, нестатутне взуття, нехарактерний однострій тощо. Але, чим дане відео просто викликає сміх – це страйкбольні автомати. Кожен, хто хоч мінімально розуміється на зброї, відразу помітить це», – ідеться в заяві полку.

Також вони зазначили, що не є прихильниками членства Україні в ЄС, як стверджується в ролику. «Від початку полк стояв на позиції єдності європейських народів у боротьбі проти азійської навали, яку б форму вона не приймала (пострадянську чи ісламську). Тож, спалювати прапор європейського народу-союзника, а тим більше з аргументацією "за ЄС", бійцям "Азову" немає жодного сенсу», – ідеться в заяві.

За даними «Європейської правди», про пропагандистську атаку повідомлені МЗС Нідерландів та Посольство України в цій державі ***(В Інтернеті з'явився фейковий ролик, де «Азов» нібито погрожує знищувати нідерландців // Західна інформаційна корпорація***

(http://zik.ua/news/2016/01/19/v_interneti_zyavyvsya_feykovyy_rolyk_de_azov_niby to_pogrozhuie_znyshchuvaty_663759). – 2016. – 19.01).

***

В социальных сетях промышляют псевдоучастники АТО

В Украине появился новый вид мошенничества – социальные сети бомбардируют псевдоучастники АТО с просьбой о помощи. Как не попасть на удочку обманщиков, выяснял «Вечерний Харьков».

«У моего мужа украли фотографии из соцсетей, завели аккаунт в Facebook, использовав ту же центральную фотографию, что стоит на его странице, и просили у друзей, знакомых и подписчиков деньги на покупку мобильного телефона – мол, срочно нужен, – поделилась своей историей харьковчанка Виктория – Муж увидел, написал модератору, поддельный аккаунт закрыли».

Волонтеры подтверждают – это не единственный случай вымогательства мошенниками денег у добросердечных граждан якобы на нужды наших ребят, воющих на передовой. Мошенники изобретательны. Под видом бойцов АТО они рассылают СМС с просьбой «скинуть пару гривен на телефон». В социальных сетях к пользователям обращаются подозрительные люди в военной форме, которые представляются офицерами АТО и просят помочь деньгами. Нередко мошенники, прикидываясь участниками волонтерской организации, просят граждан открыть на себя кредитную карту или дать номер и код банковской карты. Лжеучастники АТО пишут слезные истории в «личку» пользователей соцсетей с просьбой перечислить деньги на счет.

«Вот совсем свежий пример. Человек представлялся Димой – бойцом 92-й бригады, который якобы координирует вывоз раненых из точек столкновения, – и просил перечислить средства на его счет. Такие сообщения пришли моим знакомым в “личку”, – рассказывает координатор волонтерской группы Help Army Т. Бедняк. – Кто может координировать вывоз раненых? Медики, но уж никак не случайный человек с улицы. Я тесно общаюсь с этой бригадой, знаю всех медиков, знаю начмеда – никакого Димы среди них нет. Не может он действовать и на волонтерских началах – среди волонтеров такого человека тоже нет. Соответственно, в данном случае для меня даже не было необходимости проверять информацию – сразу понятно, что этот человек – мошенник. Если он и является бойцом 92-й бригады – все равно такой способ добыть деньги является мошенническим».

«Если вы не знакомы лично с человеком, бросившим клич о помощи, найдите общих знакомых (сослуживцев, сотрудников, кумовьев, соседей), которые могли бы его отрекомендовать, то есть подтвердить, что это действительно реальный человек, который служит там-то и там-то, либо волонтер и помогает тому-то и тому-то, – советует координатор волонтерской группы Help Army Т. Бедняк. – Если человек представляется бойцом определенной бригады или подразделения – попытайтесь найти в данном подразделении или воинской части знакомых, которые могут подтвердить, что

ситуация там действительно такова, как человек описывает, и требует вмешательства. Такую информацию можно получить через волонтеров, военнослужащих. Сейчас многие пользуются Facebook, и это не проблема – посмотреть там общих друзей и разобраться в ситуации.

Если обращаются бойцы и указывают номер телефона – желательно позвонить по этому номеру, выяснить максимум деталей, а затем получить подтверждение в подлинности истории у волонтеров, которые ездят на передовую».

«Например, человек говорит: “Я нахожусь в районе Станицы Луганской, доставки еды нет, и мы тут голодаем”. Понятно, что ситуация патовая – нужно срочно все бросать и ехать. Можно через Facebook найти волонтеров, которые там бывают, либо бойцов подразделений, которые находятся рядом, и попытаться уточнить, действительно ли ситуация требует немедленного вмешательства, – подсказывает Т. Бедняк. – В данном случае я бы рекомендовала даже не заниматься собственным расследованием – а просто выложить в Facebook эту просьбу о помощи. Если проситель – мошенник, он всегда допускает ошибки, которые быстро всплывают в публичной плоскости. Например, говорит, что он боец 128-й бригады, которая стоит в определенном месте. А волонтеры знают, что в данном секторе такого подразделения нет вообще. Становится очевидно, что действует мошенник.

Если за помощью обращаются от организации – будь то благотворительный фонд или общественное объединение, – не лишним будет определить уровень доверия к ней».

«За время войны у организации, которая активно помогала, уже есть своя история – есть отчеты на Facebook, на собственном сайте, – продолжает Т. Бедняк. – Если организация зарегистрировалась полторы-две недели назад и уже просит помощи – возвращаемся к пункту первому: находим общих знакомых и ищем рекомендации» ***(В социальных сетях промышляют псевдоучастники АТО // Вечерний Харьков (http://vecherniy.kharkov.ua/news/115711/). – 2016. – 26.01).***

***

В течение праздников в социальных сетях вспыхнула очередная интернет-война между российскими «либералами» и украинскими блогерами. Эта война подтвердила ряд закономерностей, о которых уже давно говорили специалисты по сетевым медиа.

Любовь к фейкам

Отечественная блогосфера оказывается очень уязвимой в плане распространения неподтвержденной информации. Здесь злую шутку с пользователями играет вполне нормальная возможность одним кликом копировать информацию к себе на страницу, разнося слухи по всему Интернету.

Чаще всего это происходит с сообщениями о гибели военных, с придуманными цитатами политиков и общественных деятелей, просто с

информацией о несчастных случаях, ДТП, падениях самолетов и крушениях поездов. Чем более «страшной» и волнительной кажется такая информация, тем быстрее ее пытаются перепостить взбудораженные пользователи социальных сетей.

Понятно, что свое влияние на такое поведение оказывает война. В мирное время распространению фейковых сообщений было бы проще противостоять. Но когда на Донбассе погибают люди, в соседней стране продолжают озвучивать антиукраинские бредни, а до мира еще очень далеко, публике хочется верить в любые слухи и сплетни.

При этом даже беглый взгляд на ту или иную информацию, на название сайта и на его новостной ряд может помочь людям в определении фейковости сообщения. Для того, чтобы легко фильтровать увиденную информацию, многим пользователям мешает обычная лень.

А лидеры кто?

Сетевые войны в украинском сегменте Интернета вспыхивают по разным причинам. Но, кроме политических, идеологических и иных скучных мотивов, можно вспомнить еще одну причину.

И здесь мы подходим к еще одному заметному явлению в украинской блогосфере. Речь идет о так называемых «лидерах мнений». Эти люди зачастую формируют повестку дня в социальных сетях и пытаются влиять на настроения людей.

Но кто эти люди? Иногда они прячутся за аватарками, на которых нет их фотографий. В их популярности немало накрученного трафика, купленных и автоматически выставляемых лайков и репостов. Не все из этих мастеров клавиатуры смогут успешно выступить на митинге и повести за собой людей.

Но их почему-то называют лидерами мнений. А ведь фактически речь идет о публицистах, регулярно собирающих на своей странице пару тысяч или в лучшем случае десятков тысяч читателей, но считающих, что их узкая аудитория олицетворяет всю страну.

Не все из этих авторов широко известны за пределами социальных сетей. Не всегда их популярность имеет крепкую основу и способна выдержать проверку временем. Лидеры мнений известны в сетях не только своим не очень подтвержденным статусом, но и манерой информировать общественность о том, что ей не всегда нужно знать. Часть из таких спикеров имеет отношение к армии, волонтерскому движению, что позволяет получать доступ к оперативной и служебной информации.

Тяга к личной популярности иногда заставляет блогеров сообщать публике о передвижениях воинских частей, о деталях ситуации на передовой, о личных данных военных, выполняющих специальные задания.

Разумеется, что возможность одним из первых сообщить секретную информацию всему Интернету позволяет таким авторам быстро и резко увеличивать свой сетевой рейтинг. Активные обсуждения подобной оперативной информации в публичном пространстве только усиливают их самомнение. О последствиях никто не думает. Противнику при таком

свободном режиме и при таком отсутствии ответственности со стороны лидеров мнений даже не надо создавать свою агентурную сеть. Необходимую информацию можно собрать просто из социальных сетей.

Такая ситуация сложилась еще весной 2014 г., когда многие нынешние лидеры мнений еще не были таковыми. С тех пор прошло почти два года, а общее положение не сильно изменилось.

Как только у известного блогера появляется информация, способная собрать тысячи лайков и репостов, он уже не думает о негативной стороне такого опубликования. В погоне за славой авторы теряют чувство реальности и постят то, что не нужно предавать широкой огласке.

Это все было бы не так важно и заметно, но блогеры в последнее время стали переоценивать силу социальных сетей и требовать особого статуса для себя и своего мнения. Реальная политика при этом делается на улице и на фронте, и там мнение видных блогеров далеко не всегда может иметь значение ***(Михайловский Ф. Подростковые войнушки в Сети // From-UA.Новости Украины (http://www.from-ua.com/articles/367796-podrostkovie-voinushki-v-seti.html). – 2016. – 19.01).***

***

ЕС объявили «войну»: украинцам посоветовали готовиться к информационной атаке, пишет «Обозреватель».

В последние две недели перед запланированным на 6 апреля в Нидерландах референдумом по Соглашению об ассоциации Украина – ЕС, ожидается наибольшее количество информационных атак. Об этом сообщил посол по особым поручениям Министерства иностранных дел Украины Д. Кулеба, передает «Крым.Реалии».

В связи с этим он призвал всех, кто следит за этой темой, внимательно относиться к информации, которая появляется, отметив, что «это тот момент, когда лучше трижды проверить перед тем, как однажды нажимать кнопку Enter и запустить информацию для широкого круга».

Д. Кулеба рассказал, что противники соглашения об ассоциации будут использовать «аргументы войны и коррупцию».

«Референдум не убьет Соглашение об ассоциации, но однозначно создаст политический и юридический фон, чтобы соглашение полностью юридически и официально не вступило в силу, хотя его применение продолжится в том порядке, в котором оно применяется в настоящее время», – отметил Д. Кулеба.

По словам дипломата, запланированный референдум «не столько против Украины, сколько против ЕС, это атака на европейские ценности». Избирательный совет Нидерландов назначил референдум по Соглашению об ассоциации Украина – ЕС на 6 апреля 2016 г. В этом органе подчеркнули, что референдум не имеет обязывающего характера, его результаты не могут заставить правительство отозвать соглашение.

Как ранее сообщал «Обозреватель», в Нидерландах заподозрили Россию в давлении на референдум по ассоциации Украина – ЕС ***(ЕС объявили «войну»:***

украинцам посоветовали готовиться к информационной атаке // Обозреватель (http://obozrevatel.com/politics/96537-es-obyavili-vojnu-ukraintsam-posovetovali-gotovitsya-k-informatsionnoj-atake.htm). – 2016. – 19.01).

Зарубіжні спецслужби і технології «соціального контролю»

Компания Google добилась отмены блокировки YouTube в Пакистане, запустив в стране специальную версию видеосервиса, позволяющую правительству удалять ролики, содержание которых оно считает оскорбительным. Доступ к YouTube был заблокирован в Пакистане в сентябре 2012 г. – после появления на сайте антиисламского видео «Невинность мусульман», снятого в США. Загрузка этого видео вызвала волну жестоких протестов в стране.

Министерство информационных технологий и телекоммуникаций Пакистана в своём официальном заявлении сообщило, что, согласно правилам новой версии YouTube, Телекоммуникационное ведомство Пакистана имеет полное право требовать блокировки оскорбительного контента. Сообщается, что Google полностью организовала систему, которая позволяет ведомству напрямую делать запросы на блокировку в пределах страны тех или иных роликов.

Во многом блокировка YouTube в 2012 г. была связана с богохульством, к которому в Пакистане относятся крайне щепетильно. Множество людей в стране погибает из-за подозрений в неверности Исламу – богохульство в Пакистане может караться смертной казнью.

За последние несколько лет правительство Пакистана заблокировало доступ к тысячам сайтов, содержимое которых оно считает крайне нежелательным ***(Пакистан снял блокировку YouTube // IGate (http://igate.com.ua/lenta/12747-pakistan-snyal-blokirovku-youtube). – 2016. – 19.01).***

***

Остается открытым вопрос по блокировке на территории России аккаунта французского сатирического журнала Charlie Hebdo. Представители Twitter не спешат блокировать его, мотивировав свое решение тем, что пока сомневаются в этой необходимости, пишет izvestia.ru.

Помимо аккаунта Charlie Hebdo, Twitter также пока не заблокировал ряд страниц с экстремистской информацией о «Хизб ут-Тахрир», призывами к убийству россиян, федерализации Сибири, а также материалы с детской порнографией.

Как рассказали в пресс-службе Роскомнадзора, в ходе встречи обсуждались вопросы исполнения компанией Twitter, Inc. требований

российского законодательства о персональных данных, а также норм российского законодательства, связанного с ограничением доступа к противоправной информации.

Согласно данным федеральной службы, в адрес компании Twitter, Inc. направлялись 1,9 тыс. уведомлений по блокировке интернет-страниц с информацией о наркотиках, способах самоубийства, детской порнографии и пр., признанной запрещенной по решению суда, а также 300 уведомлений по блокировке информации и незамедлительному ограничению доступа к экстремистским материалам, пропаганде терроризма и призывам к участию в несанкционированных массовых мероприятиях по требованию Генеральной прокуратуры.

«Совместная работа ведется. В первом случае исполнено 97 % требований, а во втором – 93 %», – заявили в пресс-службе Роскомнадзора.

Источник в ведомстве подтвердил «Известиям», что в число незаблокированных экстремистских материалов входит аккаунт журнала Charlie Hebdo.

«Если судить по цифрам исполненных требований, диалог, конечно, конструктивный. Но всё же есть случаи, как, к примеру, вышеупомянутый, когда вопрос остается открытым», – добавил собеседник «Известий».

Другой источник, также принимавший участие во встрече, подчеркнул, что представители компании не говорят о своем жестком отказе блокировать те или иные запрещенные страницы, а скорее пока уклоняются от исполнения требований ***(Twitter в России отказывается блокировать аккаунт Charlie Hebdo // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/45957/118/lang,ru/). – 2016. – 21.01).***

***

Google і Facebook «рано чи пізно» будуть змушені дотримуватися російського законодавства, в іншому випадку вони можуть бути заблоковані в Росії.

Про це заявив в інтерв'ю Газеті.ru радник президента Росії по Інтернету Г. Клименко.

«Що станеться, якщо держава заборонить Google і Facebook? Відповідь шалено проста: "Яндекс" і інші почнуть заробляти більше, якщо отримають більшу частину пирога. Google же їсть наші пироги», – сказав він.

Г. Клименко зазначив, що деякі ЗМІ з цього твердження роблять висновки, що він пропонує побудувати в Росії китайський фаєрвол, але це не відповідає дійсності. «Для того, щоб у нас побудувати китайський фаєрвол, у нас повинні бути китайські громадяни. Не можна перетягнути будь законодавче рішення в тому чи іншому вигляді», – сказав він.

Технічно блокування можливе, зазначив Г. Клименко, але додав, що особисто не планує займатися підготовкою такого законопроекту. «Якщо ви

мене запитаєте, напишу я завтра закон про блокування, – ні. У мене немає цих повноважень», – додав радник президента.

Як писав MediaSapiens, у Росії від Facebook і Twitter зажадали співробітництва з правоохоронними органами. Раніше Роскомнагляд повідомив, що цього року проведе понад тисячу перевірок у IT- та інтернет-компаніях, торгових мережах і банках, щоб з'ясувати, чи виконується закон про зберігання персональних даних росіян у Росії ***(У Росії допускають блокування Google і Facebook // MediaSapiens (http://osvita.mediasapiens.ua/media_law/government/u_rosii_dopustili_blokuvannya_google_i_facebook/). – 2016. – 28.01).***

***

Великий Китайский Фаервол заблокировал социальную сеть «ВКонтакте». Любимая сеть русскоговорящей аудитории больше недоступна на территории Китая.

Ресурс greatfirewallofchina.org подтверждает данную информацию. Первоначально пользователи сообщали, что веб-версия была заблокирована, но работало мобильное приложение, теперь заблокировали и его. Причин блокировки, как это уже стало принято, никто не называл.

У китайского населения данная социальная сеть не была столь распространенной, но она продолжала пользоваться популярностью у русскоговорящего населения, которые либо переехали в Китай на постоянное место жительства, либо находятся там по-работе ***(ВКонтакте заблокирован в Китае // ForNote.net (http://fornote.net/2016/01/vkontakte-zablokirovan-v-kitae/). – 2016. – 26.01).***

***

Директор Агентства національної безпеки (АНБ) адмірал М. Роджерс повідомив, що США витратили п'ять років на розробку новітньої кіберзброї і обіцяв у найближчі місяці продемонструвати її в дії.

На сьогодні триває дискусія, коли саме слід вести «наступальні дії» даною кіберзброєю проти окремих груп чи держав. «Можна сказати, що зараз для нас настав переломний момент», – цитує слова М. Роджерса The Wall Street Journal.

«Потужність і можливості (таких озброєнь. – Ред.) вже почали виявлятися в режимі онлайн і вже почали виправдовувати (своє призначення. – Ред.) у цілком відчутних аспектах. Ви побачите, як ми почнемо застосовувати їх (кіберрозробки. – Ред.) більш широко», – додав глава АНБ. За його словами, більшість громадян США не помічають зростання чисельності кіберармій і кіберзлочинців, які впливають на їхнє повсякденне життя. Однак, як сказав М. Роджерс, масовані кібератаки здатні завдати шкоди, що може бути порівняно із застосуванням традиційної зброї.

Нагадаємо, що Сполучені Штати розглядають запровадження санкцій проти російських і китайських приватних осіб і компаній через кібератаки на США.

Уряд США зазнав цього року кількох кібератак. Одна з таких атак на керування персоналом Білого дому була пов'язана з Китаєм. Цей кібернапад дав потенційним іноземним шпигунам масу даних про американських держслужбовців ***(АНБ обіцяє показати новітню кіберзброю США // iPress (http://ipress.ua/news/glava_anb_obitsyaie_anons_novitnoi_kiberzbroi_ssha_151994.html). – 2016. – 22.01).***

***

Президент Таджикистану Е. Рахмон підписав закон про створення Єдиного комутаційного центру, який, за словами критиків, запроваджує додатковий урядовий контроль за Інтернетом і стільниковим зв'язком, пише Радіо Свобода.

Згідно з документом, підписаним 25 січня, всі оператори зв'язку і провайдери в Таджикистані повинні будуть надавати міжнародні послуги зв'язку та Інтернету тільки через нову структуру.

Голова Асоціації інтернет-провайдерів Таджикистану П. Ібодова повідомила, що новий центр дасть можливість уряду закрити певні сайти.

Останнім часом у Таджикистані кілька разів переривався доступ до низки сайтів, зокрема Facebook, Twitter, сайту Таджицької і Російської служби Радіо Свобода й інших новинних ресурсів.

У листопаді парламентарі Таджикистану ухвалили закон, який дає змогу владі блокувати телефонну й інтернет-системи під час проведення «антитерористичних операцій» ***(Влада Таджикистану бере під контроль інтернет // Радіо Свобода (http://www.radiosvoboda.org/content/news/27511841.html). – 2016. – 26.01).***

***

В Калифорнии на публичное рассмотрение выставлен законопроект, обязывающий производителей смартфонов продавать только те устройства, которые поддаются дистанционной разблокировке или расшифровке. Законопроект требует, чтобы любое мобильное устройство, произведенное после 1 января 2016 г. и продаваемое, либо сдаваемое в лизинг, предполагало возможность извлечения информации по требованию полиции.

Законопроект можно рассматривать как ещё один шаг законодателей навстречу интересам правоохранительных органов – в случае принятия подобной инициативы они получат доступ к смартфонам пользователей и смогут читать зашифрованные данные.

В iOS 8 Apple внесла изменения в систему шифрования данных, благодаря чему доступ к пользовательской информации получает только владелец мобильного устройства. Ранее у компании хранились ключи

шифрования, позволявшие разблокировать гаджеты по запросу правоохранительных органов, но в случае с iOS 8 этого нет.

Новый закон обяжет Apple заложить возможность дешифрования iPhone и iPad. Требование наличия подобных «жучков» подогревает длительные споры правительства США и Кремниевой долины на тему шифрования: законодатели требуют от производителей обеспечить доступ к зашифрованной информации в интересах национальной безопасности.

В свою очередь технологические компании отстаивают интересы пользователей. Apple категорична в своей позиции – она приравнивает бэкдоры в смартфонах к ящику Пандоры: если однажды открыть его, то закрыть уже не получится. Бреши в безопасности не смогут оставаться долгое время незамеченными и будут использоваться злоумышленниками.

Несколько дней назад схожий законопроект выставили на обсуждение в Нью-Йорке. Принятие этого закона будет означать, что при наличии судебного ордера сотрудники правоохранительных органов и спецслужб смогут получить доступ к фотографиям, сообщениям и другим персональным данным, которые хранятся в памяти iPhone и iPad.

За нарушение этого требования предполагается установить административный штраф в размере 2500 дол. за каждый проданный гаджет с полным шифрованием ***(Новый законопроект обязывает Apple внедрить «жучки» для слежки за пользователями // InternetUA (http://internetua.com/novii-zakonoproekt-obyazivaet-Apple-vnedrit--jucski--dlya-slejki-za-polzovatelyami). – 2016. – 22.01).***

***

В Запорожье СБУ задержала местного жителя, который занимался в соцсетях пропагандой так называемых «ДНР» и «ЛНР». Об этом сообщили в пресс-службе ведомства.

Как выяснилось, мужчина за деньги выполнял поручения одного из сепаратистов «ДНР», который присылал ему сообщения для размещения. Материалы были антиукраинскими и направленными на поддержку самопровозглашенных республик, отметили в СБУ.

В своих сообщениях запорожец призывал к насильственной смене конституционного строя Украины. Также он агитировал граждан не подчиняться действующей власти и размещал инструкции по уклонению от мобилизации.

При обыске силовики изъяли у мужчины компьютерное оборудование. В настоящее время проходят следственные действия ***(В Запорожье задержали пропагандиста ДНР в соцсетях // InternetUA (http://internetua.com/v-zaporoje-zaderjali-propagandista-dnr-v-socsetyah). – 2016. – 30.01).***

***

В Украине хотят без суда блокировать сайты и социальные сети за нарушение авторских прав. Это следует из законопроекта – № 3081-д, который был принят 29 января в первом чтении.

В частности, документ предлагает внести изменения в закон об авторских и смежных правах, в частности, в ст. 1, 50, 51, 52, где предлагается внести норму, предполагающую только судебную защиту таких прав, дополнить выражением «защита таких прав, в том числе – судебная».

Так, в ст. 52 «Порядок прекращения и предотвращения нарушений авторского права и смежных прав в сети Интернет и локальных сетях» субъект авторского права может обращаться напрямую к нарушителю, чтобы тот убрал пиратский контент.

При этом сам субъект несет ответственность в случае, если он соврал насчет наличия у него авторских прав на контент. Владелец сайта обязан не позднее чем в течение 24 часов прекратить доступ к этому контенту. И в течение 48 часов уведомить об этом заявителя.

Также субъект авторского права может обратиться к хостеру за информацией о владельце сайта. Если ему эту информацию не предоставили в течение суток, хостер будет обязан заблокировать сайт в течение 24 часов с момента поступления жалобы.

Ранее Американские ассоциация правообладателей и ассоциация кинокомпаний представили правительству США свои списки нарушителей авторских прав. В него попали сразу три украинских сайта: популярный файлообменник EX.ua, онлайн-кинотеатр Kinogo.co и торрент-трекер Extratorrent.cc ***(Рада в первом чтении разрешила закрыть EX.ua и ВКонтакте // Антикор (http://antikor.com.ua/articles/84629-rada_v_pervom_chtenii_razreshila_zakrytj_ex.ua_i_vkontakte). – 2016. – 30.01).***

Проблема захисту даних. DDOS та вірусні атаки

Программы-импланты могут следить за переговорами в конфиденциальных мобильных мессенджерах, предупреждают эксперты «Лаборатории Касперского». Новый тип вредоносного программного обеспечения позволяет полностью контролировать устройство и получать всю информацию, которая отправляется его владельцу.

Опасные звери

Программы-импланты просматривают текстовые сообщения, изображения и файлы других типов, которые хранятся в памяти смартфона или принимаются мессенджерами. Кроме того, зловреды могут отслеживать местоположение устройства, уровень заряда батареи, факт замены SIM-карты, и

другие параметры, включать камеру и микрофон для записи действий жертвы, запоминать использованные точки доступа Wi-Fi и пр.

Эксперты считают программы-импланты идеальным инструментом для кибершпионажа и подчеркивают, что они активно используются в целевых атаках на высокопоставленных лиц и организации.

Даже самое надежное шифрование, которое используется для отправки данных из мобильных мессенджеров и других подобных программ, не защищает от утечки информации.

Вредоносное ПО может атаковать все актуальные мобильные платформы – Android, iOS, Windows Mobile, Blackberry. «Лаборатория Касперского» подтвердила факт использования программ-имплантов в шести крупных кибератаках, которые имели место в последние два года.

Как защититься

Чаще всего программы-импланты проникают на устройства, на которых установлена операционная система с джейлбрейком. Обычно смартфоны и планшеты заражаются через USB-порт компьютера при зарядке, реже – через дорогие, но эффективные эксплойты (при проведении атаки на конкретное устройство).

Чаще всего программы-импланты проникают на устройства, на которых установлена операционная система с джейлбрейком.

Чтобы не стать жертвой киберпреступников, рекомендуется не делать джейлбрейк операционной системы, а также регулярно обновлять её и мобильные приложения. При подключении к Интернету желательно использовать VPN-соединение, а также не заряжать гаджеты от ПК. Кроме того, эксперты советуют контролировать процессы, которые выполняются в памяти устройства, чтобы своевременно обнаружить угрозу, и не пренебрегать антивирусом ***(В интернете появилось вредоносное ПО нового типа // InternetUA (http://internetua.com/v-internete-poyavilos-vredonosnoe-po-novogo-tipa). – 2016. – 19.01).***

***

ИБ-исследователь Ш. Кэссиди разработал способ атаки на популярный сервис управления паролями LastPass, позволяющий злоумышленникам раскрыть мастер-пароль жертвы. Мастер-пароль необходим для получения доступа к сохраненным в LastPass логинам и паролям пользователя.

По данным Ш. Кэссиди, если во время браузинга сессия LastPass истекает, соответствующее уведомление отображается в контексте открытого сайта. Страница повторной аутентификации также отображается в контексте открытого ресурса. Это позволяет злоумышленнику в ходе фишинг-атаки перенаправить жертву на сайт, уязвимый к межсайтовому скриптингу, и похитить мастер-пароль.

После удачной эксплуатации уязвимости Ш. Кэссиди опубликовал на GitHub PoC-код в виде утилиты LostPass. С помощью LostPass можно провести автоматизированную фишинг-атаку на пользователей LastPass и получить

мастер-пароли жертв. Вдобавок ко всему, злоумышленник может проверить предоставленные жертвой логин и пароль с помощью LastPass API и запросить код двухфакторной аутентификации. В случае успешного получения кода хакер сможет раскрыть любой логин и пароль пользователя.

В настоящее время утилита работает в браузере Chrome. Специалист обещает в скором времени создать экспериментальную версию LostPass для Firefox.

Исследователь сообщил разработчикам LastPass об обнаруженной ошибке. Тем не менее, создатели ПО для управления паролями отказались выпускать исправление, предупредив пользователей о недопустимости ввода мастер-пароля через веб-сайт. Уведомления также отображаются в контексте открытого веб-сайта. Хакеры могут заблокировать отображение подобных сообщений ***(В LastPass обнаружена опасная уязвимость // InternetUA (http://internetua.com/v-LastPass-obnarujena-opasnaya-uyazvimost). – 2016. – 18.01).***

***

Эксперты компании Perception Point обнаружили серьезную уязвимость в ядре Linux (CVE-2016-0728), позволяющую локальному пользователю получить административный доступ и скомпрометировать систему. Эксплуатация ошибки позволяет атакующему удалять файлы, просматривать конфиденциальную информацию, устанавливать нежелательные программы и пр. Как отмечается, проблема присутствовала в ядре с 2012 г., но была выявлена только сейчас.

Ошибка затрагивает версии ядра Linux 3.8 и выше, а также распространяется на устройства под управлением Android KitKat и более поздних версий операционной системы. По словам экспертов, уязвимыми являются десятки миллионов персональных компьютеров и серверов на базе ОС Linux и 66 % всех Android-устройств.

Уязвимость CVE-2016-0728 присутствует в хранилище keyring(7), встроенном в различные версии ОС Linux. В задачи Keyring входит шифрование и хранение учетных данных, ключей шифрования, цифровых сертификатов, а также взаимодействие с приложениями в ОС.

Согласно отчету исследователей из Perception Point, уязвимость заключается в утечке ссылок на объекты и может позволить злоумышленнику выполнить произвольный код на целевой системе в контекста ядра Linux.

Приложения уровня пользователя предоставляют возможность ядру управлять криптографическими ключами. Поскольку функционал обладает доступом к уровню ядра ОС и выполняет код не в пространстве пользователя, злоумышленник может повысить свои привилегии на системе.

Механизмы предотвращения выполнения кода SMEP (Supervisor Mode Execution Protection) и SMAP (Supervisor Mode Access Protection) усложняют выполнение кода на Linux-серверах.

Эксперты уже проинформировали о проблеме команду разработчиков Linux. Исправление ошибки будет выпущено в самое ближайшее время.

В настоящее время нет сведений об активной эксплуатации уязвимости. Более подробный анализ и PoC-код к уязвимости опубликованы на портале для разработчиков GitHub ***(В ядре Linux обнаружена уязвимость повышения привилегий // InternetUA (http://internetua.com/v-yadre-Linux-obnarujena-uyazvimost-povisheniya-privilegii). – 2016. – 20.01).***

***

Функциональные возможности вредоносных программ для ОС Linux расширяются день ото дня: среди них нередко встречаются программы-шпионы, шифровальщики и троянцы, предназначенные для организации DDoS-атак.

Вирусные аналитики компании «Доктор Веб» исследовали очередное творение вирусописателей, получившее наименование Linux.Ekoms.1, – эта вредоносная программа умеет с определенной периодичностью делать на инфицированном компьютере снимки экрана и загружать на зараженную машину различные файлы.

После своего запуска Linux.Ekoms.1 проверяет наличие в одной из подпапок домашней директории пользователя файлов с заранее заданными именами и при их отсутствии сохраняет собственную копию в одной из них (выбор осуществляется случайным образом), а затем запускается из новой локации. После успешного запуска троянец соединяется с одним из управляющих серверов, адреса которых «зашиты» в его теле. Все данные, которыми Linux.Ekoms.1 обменивается с управляющим центром, шифруются.

С периодичностью в 30 секунд троянец делает на зараженном компьютере снимок экрана (скриншот) и сохраняет его во временную папку в формате JPEG. Если поместить файл на диск по каким-либо причинам не удалось, Linux.Ekoms.1 пытается выполнить сохранение в формате BMP. Содержимое временной папки загружается на управляющий сервер по таймеру с определенными временными интервалами.

Один из создаваемых троянцем потоков в ОС Linux генерирует на инфицированном компьютере список фильтров для имен файлов вида «aa*.aat», «dd*ddt», «kk*kkt», «ss*sst», поиск по которым осуществляется во временной папке, и загружает подходящие под эти критерии файлы на управляющий сервер. Если в ответ поступает строка uninstall, Linux.Ekoms.1 загружает с сервера злоумышленников исполняемый файл, сохраняет его во временную папку и запускает оттуда. Также троянец обладает возможностью загрузки с управляющего сервера других произвольных файлов и их сохранения на диске компьютера.

Помимо функции создания снимков экрана в коде троянца присутствует специальный механизм, позволяющий записывать звук и сохранять полученную запись в файл с расширением .aat в формате WAV, но практически эта возможность нигде не используется. Сигнатура Linux.Ekoms.1 добавлена в

вирусные базы, и потому этот троянец не представляет опасности для пользователей Антивируса Dr.Web для Linux ***(Троянец для Linux делает скриншоты // ITnews (http://itnews.com.ua/news/79664-troyanets-dlya-linux-delaet-skrinshoty). – 2016. – 20.01).***

***

На электронные адреса предприятий электроэнергетики злоумышленники проводят массовую рассылку поддельных электронных сообщений от имени Национальной энергетической компании «Укрэнерго» об изменении даты общественных обсуждений Плана развития объединенной энергосистемы Украины.

В теле сообщения вложен поддельный файл, в котором якобы содержится проект указанного плана, который заражен вирусом BlackEnergy, ранее поразившим системы международного аэропорта «Борисполь» в Киеве.

«Укрэнерго» официально заявляет, что не осуществляет таких рассылок по электронной почте. Об инциденте проинформированы специалисты украинского подразделения по борьбе с киберпреступностью CERT.UA.

В дальнейшем, в случае получения подозрительных сообщений по электронной почте от «Укрэнерго», Национальная энергокомпания просит не открывать вложенные файлы без их предварительной проверки последней версией антивирусного ПО ***(Хакеры ведут вирусную рассылку BlackEnergy от лица «Укрэнерго» // InternetUA (http://internetua.com/hakeri-vedut-virusnuua-rassilku-BlackEnergy-ot-lica--ukrenergo). – 2016. – 21.01).***

***

Новый троян-загрузчик Nemucod активизировался в Интернете. Как сообщает разработчик антивирусного программного обеспечения ESET, вредоносное программное обеспечение распространяется через вложения в электронной почте и вымогает биткоины.

Фактически Nemucod используется для распространения шифратора TeslaCrypt – именно он непосредственно ограничивает пользователям доступ к их файлам. Электронные письма, которые рассылают злоумышленники, включают вложение в виде ZIP-архива и имитируют счет-фактуру.

Так как рассылка «писем счастья» происходит с электронных адресов пользователей, компьютеры которых заражены вирусом, адресаты часто ни о чем не подозревают. Отличие новой кампании – в том, что ZIP-архив содержит не исполняемый файл (к примеру, с расширением .exe), а файл JavaScript, и это позволяет обойти защиту почтовых серверов, детектирующих ряд потенциально опасных форматов файлов.

Заражение компьютера сопровождается загрузкой в систему новой модификации шифратора TeslaCrypt, который ранее уже использовался в кибератаках. Шифруются документы, видео, изображения, и часто даже после оплаты и получения ключей пользователь не может восстановить доступ к этим данным.

Пока вирус наиболее активен в Австралии и Великобритании, а также в Канаде и Японии. В некоторых регионах 75 % в общем объеме обнаруженных вредоносных программ составлял именно Nemucod ***(Новый троян вымогает деньги у пользователей // InternetUA (http://internetua.com/novii-troyan-vimoqaet-denqi-u-polzovatelei). – 2016. – 21.01).***

***

Еще три года назад в анонимной сети Tor функционировал черный рынок Silk Road. Воплощение мечты любого криптоанархиста, сайт был доверенной торговой площадкой, защищенной от контроля со стороны властей. Сегодня же ситуация иная: Silk Road больше не существует, а создатель сайта Р. Ульбрихт отбывает пожизненное заключение, пытаясь оспорить приговор в апелляционном суде.

После прекращения работы Silk Road в анонимных сетях появилось множество аналогичных торговых площадок, но клоны «Шелкового пути» существовали недолго – через некоторое время ресурсы закрывались, а администраторы исчезали из поля зрения, забрав большую часть средств клиентов. В результате, как отмечает издание Wired, анонимные торговые площадки изменились далеко не в лучшую сторону для пользователей.

По словам исследователя Калифорнийского университета в Беркли Н. Уивера, администраторы анонимных торговых площадок начали чаще прибегать к обману пользователей. Боясь столкнуться с правоохранительными органами, владельцы ресурсов без предупреждения прекращают работу сайтов, при этом присваивая часть средств пользователей.

Случаи внезапного отключения анонимных торговых площадок начались примерно через год после исчезновения Silk Road. Первым подобным сайтом стал Evolution – наиболее популярная после Silk Road торговая площадка. В марте 2015 г. ресурс стал недоступен, потери пользователей составили порядка 12 млн дол. в биткоинах. Через несколько месяцев ситуация повторилась, на сей раз с торговой площадкой Agora. Вскоре из сети пропали сразу несколько менее популярных ресурсов наподобие Abraxas, Amazon Dark, Blackbank и Middle Earth.

Последней крупной функционирующей торговой площадкой в настоящее время является Alphabay. Ресурс предлагает приобрести наркотики, нелегальные химикаты и похищенные учетные данные. Судя по жалобам пользователей AlphaBay, администраторы торговой площадки уже несколько раз похищали биткоины жертв, обвиняя пострадавших в использовании слабых паролей или открытии фишинговых писем. «Администрацию AlphaBay подозревают в похищении средств пользователей, и не зря», – отметил один из пользователей ресурса.

По мнению экспертов, аналогичные «исчезновения» ресурсов будут продолжаться и дальше. Основными причинами подобных инцидентов считаются боязнь столкнуться с правоохранительными органами и преступные намерения администраторов сайта ***(Администраторы анонимных торговых***

площадок похищают средства пользователей // InternetUA (http://internetua.com/administratori-anonimnih-torgovih-plosxadok-pohisxauat-sredstva-polzovatelei). – 2016. – 20.01).

***

Подтвердились слухи об утечке базы данных пользователей Nexus Mods – сайта, содержащего игровые моды для более 230 игр. Сообщество ресурса насчитывает порядка 10 млн пользователей. В результате инцидента были скомпрометированы учетные записи 5 915 013 пользователей портала.

Впервые информация о возможной утечке появилась в декабре прошлого года. Тогда один из пользователей форума Reddit призвал всех посетителей Nexus Mods сменить пароли. Как оказалось, в сети был обнаружен дамп базы данных Nexus Mods. После тщательного изучения базы администрация ресурса разослала всем пользователям уведомление с просьбой сменить пароли.

По словам одного из администраторов сайта, известного как Dark0ne, дамп базы данных содержит информацию об учетных записях, зарегистрированных не позже 22 июля 2013 г. Как сообщается, финансовая информация пользователей не была скомпрометирована. База данных содержала имена пользователей, адреса электронной почты, хеши и пароли.

Предположительно, утечка произошла в результате компрометации учетных записей трех авторов различных модов, установивших довольно простые пароли. Под видом легитимных файлов неизвестные загрузили на сервер Nexus Mods вредоносное ПО, позже использованное для хищения информации ***(В сеть утекли данные 6 млн пользователей Nexus Mods // IGate (http://igate.com.ua/lenta/12776-v-set-utekli-dannye-6-mln-polzovatelej-nexus-mods). – 2016. – 21.01).***

***

Антивирусная компания «Доктор Веб» сообщила о весьма интересной «находке».

Как оказалось, в прошивке смартфона Philips s307 «обнаружился» вирус под названием Android.Cooee.1.

Со своей стороны специалисты «Доктор Веб» уже сообщили в офис CEC (China Electronics Corporation) – компании, которая обладает эксклюзивной лицензией на продвижение и продажу мобильных телефонов Philips и Xenium о своей «находке».

Android.Cooee.1 представляет собой некий лончер, который помимо классических возможностей обладает также дополнительной вредоносной функциональностью, навязывающей рекламу, а также загрузку и установку нежелательного программного обеспечения ***(«Доктор Веб» обнаружила вирус в прошивке смартфона Philips s307 // ITnews (http://itnews.com.ua/news/79685-quotdoktor-vebquot-obnaruzhila-virus-v-proshivke-smartfona-philips-s307). – 2016. – 21.01).***

***

Спамеры с каждым днем разрабатывают новые персонализированные кампании и увеличивают качество рассылаемых сообщений. Об этом сообщает технический директор ИБ-компании Agari В. Аппарао.

Злоумышленники пользуются услугами небольших хостингов, где отсутствует защита от мошенничества и вредоносных действий. Отправляемые спамерами сообщения почти не отличаются от оригиналов и требуют подробной проверки для выявления несоответствий. Подобные атаки, получившие название «снегоступы» (snowshoe attacks), способны обходить защиту от спама.

Большинство сообщений, отправляемых в ходе подобных атак, успешно обходят спам-фильтры и попадают в папку «Входящие». По современным стандартам это считается крупным достижением – в настоящее время ПО для блокировки спама отсеивает до 99,99 % вредоносных писем.

В качестве примера В. Аппарао привел атаку на пользователей Apple во Франции, осуществленную в октябре 2015 г. Неизвестные злоумышленники отправили порядка 5 тыс. сообщений, имитирующих ответ от службы поддержки Apple и содержащих перенаправление на поддельную страницу аутентификации. Большинство писем успешно обошли защиту от спама и в течение порядка 8 часов не обнаруживались спам-фильтрами.

Действия спамеров становятся все большей проблемой, вынуждая представителей отрасли кибербезопасности вводить новые стандарты защиты. В настоящее время ведется разработка технологии DMARC – глобального реестра доверенных рассылок. Компании смогут зарегистрировать серверы, используемые для массовой отправки сообщений. Письма, полученные якобы от имени компаний, но с других серверов, будут автоматически помечены как спам.

По данным отдела исследования киберугроз Cisco Talos, ежедневно злоумышленники отправляют порядка 400 млрд вредоносных сообщений. Большинство подобных писем не попадут в почтовые ящики пользователей, но некоторым сообщениям все же удается попасть в папку «Входящие» ***(Спамеры прибегают к новым техникам осуществления атак // InternetUA (http://internetua.com/spameri-pribegauat-k-novim-tehnikam-osusxestvleniya-atak). – 2016. – 25.01).***

***

Системы глобального позиционирования широко используются не только для планирования маршрутов, но для синхронизации технологических процессов в индустрии. Взлом GPS, таким образом, чреват значительными последствиями.

О серьёзности проблемы позволяет судить хотя бы тот факт, что Военно-морские силы США, в 2006 г. отказавшиеся от навигации по звёздам в пользу GPS, теперь вновь учат офицеров пользоваться секстантами.

«GPS применяется где-то с 1992 г. С 2002 г., когда стало известно о её уязвимости, было предложено много контрмер, но до сих пор не разработано стратегии, которая обеспечила бы защиту от всех атак», – заявила К. Поппер, возглавляющая группу Информационной безопасности в Институте Хорста Горца (HGI) Рурского университета в Бохуме (Германия). Предложенный ею метод обещает в значительной мере уменьшить уязвимость систем позиционирования и заключается в одновременном применении нескольких GPS-приёмников.

Хакер, атакующий GPS, может использовать для этой цели симулятор спутника. Такая программа будет генерировать ложный спутниковый сигнал, выглядящий как настоящий, и передавать его на приемник, например, автомобильной системы навигации. Таким способом, атакующий может обмануть приёмник, заставив его выдать координаты, не совпадающие с текущей позицией автомобиля.

К. Поппер рассмотрела, что происходит, если используются несколько приёмников, разнесенных между собой на некоторое расстояние. Если принимаются подлинные сигналы спутников, расположенных в разных точках орбиты, то времена их прихода на разные приемники будут несколько отличаться друг от друга. Если же сигналы поступают от симулятора, то, несмотря на обманчивую аутентичность, они будут полностью одинаковы для всех приёмников.

Согласно последним результатам, минимальное расстояние между приёмниками, позволяющее улавливать разницу во времени прихода подлинных спутниковых сигналов, составляет 2–3 м. Это позволяет легко реализовать данную схему для крупных автомобилей или судов. «Для устройств, имеющих небольшие пространственные габариты, например, смартфонов, предстоит найти какое-нибудь другое решение», – отмечает К. Поппер ***(Персональные системы навигации остаются уязвимы для хакеров // InternetUA (http://internetua.com/personalnie-sistemi-naviqacii-ostauatsya-uyazvimi-dlya-hakerov). – 2016. – 27.01).***

***

Компания Apple может перехватывать персональные данные миллионов пользователей iCloud, несмотря на строгие меры безопасности и использование сквозного шифрования. Об этом сообщает издание Hacker News.

Проблема затрагивает всех пользователей, подключивших услугу резервного копирования данных iCloud Backup. В рамках iCloud Backup информация пользователей автоматически сохраняется и шифруется на серверах Apple. В процессе используется неподконтрольный пользователю ключ. Компания может получить доступ к персональным и конфиденциальным данным пользователей.

iCloud Backup используется по умолчанию на всех устройствах Apple. Функцию можно отключить, но пользователю придется осуществлять

резервное копирование данных вручную и хранить копии на локальном хранилище.

По мнению экспертов, подобная ошибка со стороны Apple может поставить под угрозу конфиденциальность пользовательской информации. К примеру, правоохранительные органы или спецслужбы могут потребовать предоставить доступ к данным на основании законодательства США ***(Apple может перехватывать персональные данные пользователей iCloud // InternetUA (http://internetua.com/Apple-mojet-perehvativat-personalnie-dannie-polzovatelei-iCloud). – 2016. – 26.01).***

***

Неизвестные хакеры создали специальную страничку в Интернете, после посещения которой практически все мобильные устройства начинают перезагружаться, пишет Gizmodo. Интересно, что из-за огромной популярности сервера этого сайта «упали».

www.crashsafari.com делает именно то, что указано в его названии: «обрушивает» стандартный браузер для iOS-устройств. Этот же трюк проходит и с гаджетами на операционной системе Android. Дело в том, что при загрузке страницы срабатывает специальный скрипт, из-за которого в строке браузера автоматически добавляются тысячи символов. В итоге смартфон не справляется с такой серьезной нагрузкой и начинает перезагружаться: даже выход из браузера не решает проблему.

Владельцам ПК и ноутбуков также не рекомендуется переходить по этой ссылке, ведь пользователей «настольных» версий браузеров Safari и Chrome может ждать та же участь, что и обладателей смартфонов. Хотя в большинстве случаев выход из интернет-проводника должен помочь.

Страничка была зарегистрирована 29 апреля 2015 г., однако популярность в соцсетях сайт набрал только 25 января нынешнего года: пранкеры начали маскировать ссылку, чтобы поиздеваться над своими читателями. По информации TJ, на уловку попалось более 100 тыс. человек ***(«Убивающий» смартфоны сайт не выдержал наплыва посетителей // InternetUA (http://internetua.com/ubivauasxii--smartfoni-sait-ne-viderjal-napliva-posetitelei). – 2016. – 26.01).***

***

Посетители по крайней мере пяти сайтов знакомств подверглись атаке, в ходе которой злоумышленники распространяют вариант червя TheMoon. Вредонос инфицирует маршрутизатор, после чего зараженное устройство становится частью ботнета, сообщают эксперты компании Damballa. Как удалось выяснить специалистам, владельцем всех пяти ресурсов является один и тот же человек.

О черве TheMoon стало известно в феврале 2014 г. Вредоносное ПО проникает сквозь защиту путем эксплуатации уязвимостей в протоколе HNAP

(Home Network Administration Protocol). Главной особенностью червя является его способность самостоятельно распространяться.

По всей вероятности, злоумышленники заманивают жертв при помощи проверенных методов: фишинга, набора эксплоитов или вредоносной рекламы. На каждом вредоносном сайте инфицирование проходит в два этапа. Заражение начинается с вредоносного «плавающего фрейма», внедренного в веб-страницу.

На первом этапе фрейм вызывает различные URL-ссылки с целью определить, использует ли маршрутизатор протокол HNAP. Затем фрейм выясняет наличие IP-адресов 192.168.0.1 и 192.168.1.1 для управления маршрутизатором и в качестве шлюзов.

На втором этапе фрейм загружает вторую URL-ссылку и самого червя. Жертвы атаки не могут использовать некоторые входящие порты маршрутизатора, а через исходящие порты осуществляется инфицирование других устройств.

На момент обнаружения оригинальной версии TheMoon исследователи не смогли определить наличие связи с каким-либо C&C-сервером, хотя в исходном коде вредоноса присутствовал соответствующий функционал. По состоянию на конец 2015 г. C&C-инфраструктура также не была выявлена. Как считают эксперты Damballa, разрастающийся ботнет находится на ранней стадии или проходит тестирование ***(Новый вариант червя TheMoon атакует посетителей сайтов знакомств // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2016/01/26/TheMoon.html). – 2016. – 26.01).***

***

Український департамент кіберполіції разом зі слідчими затримав німця, який перебуває у міжнародному розшуку. Арешт здійснили на запит правоохоронців ФРН, повідомляється на сайті нацполіції у вівторок, 26 січня. У Німеччини хакерові ставлять у провину вчинення 15 правопорушень, які завдали німецьким компаніям збитків на 2,6 млн євро.

Повідомляється, що Німеччина підозрює кіберзлочинця в організації DDoS-атак на інтернет-магазини, якими сайт-жертва закидається запитами, через що він виходить з ладу і стає недоступним. Крім того, хакер використовував потужні розподілені кібератаки як привід для шантажу – за їх припинення він вимагав понад 1,5 млн євро.

У повідомленні поліції зазначається, що хакера затримано 20 січня, і український суд уже вирішив питання про тримання його під вартою. Надалі українська поліція планує екстрадувати злочинця до Німеччини для притягнення до відповідальності ***(Українська кіберполіція затримала німецького хакера-шантажиста // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/ukrainska_kiberpolitsiya_zatrimala_nimetskogo_khakerashantazhista/). – 2016. – 27.01).***

***

Российские хакеры атаковали электронный почтовый ящик Председателя Верховной Рады Украины В. Гройсмана.

Как передает Цензор.НЕТ, об этом на странице в Facebook написал его пресс-секретарь Д. Столярчук.

«Сегодня на ряд адресов пришло электронное письмо якобы с почтового ящика председателя Верховной Рады. В теме указано “Новая Конституция Украины”, а прикреплена ссылка на видео-обращение одиозного экс-народного депутата-регионала В. Олийныка, который, как известно, скрывается после Революции Достоинства. В обращении говорится о необходимости принимать новую Конституцию на референдуме», – написал Д. Столярчук.

«В. Гройсман к этим письмам не имеет никакого отношения», – подчеркнул пресс-секретарь спикера, добавив, что «уже установлено, что письмо рассылалось с российского почтового сервера» ***(Российские хакеры атаковали электронную почту Гройсмана // InternetUA (http://internetua.com/rossiiskie-hakeri-atakovali-elektronnuua-pocstu-groismana). – 2016. – 27.01).***

***

Исследователи обнаружили новый вид вымогательского ПО Magic, основанный на учебном проекте с открытым исходным кодом EDA2. В течение последних нескольких дней вредонос активно распространялся и инфицировал компьютеры жертв.

Проект EDA2 был разработан турецким исследователем безопасности У. Сеном, ранее создавшим аналогичное вымогательское ПО Hidden Tear. Оба проекта У. Сен разработал исключительно в образовательных целях. Для предотвращения эксплуатации исследователь встроил в исходный код Hidden Tear и EDA2 бэкдоры, позволявшие восстановить зашифрованные данные.

Способ инфицирования жертв остается неизвестным. Вредонос шифрует файлы на компьютерах пользователей и меняет расширения на .magic. Вымогательское ПО использует алгоритм AES, но ключ шифрования хранится не на компьютере жертвы, а на C&C-сервере. За восстановление доступа к данным жертва должна отправить злоумышленникам выкуп в биткоинах.

Авторы вредоноса разместили C&C-сервер на бесплатном хостинге. К сожалению, администрация ресурса удалила учетные записи злоумышленников и все находящиеся на сервере данные, включая ключи расшифровки. Восстановить зашифрованные данные невозможно.

В связи с инцидентом У. Сен завершил работу над проектом EDA2 и удалил исходный код вредоноса из репозитория в GitHub. По словам исследователя, бэкдор был встроен в административную панель. Если бы C&C-сервер до сих пор функционировал, исследователь смог бы получить доступ к базе данных и расшифровать данные пострадавших пользователей ***(Обнаружено вымогательское ПО на основе исходного кода проекта EDA2 //***

InternetUA (http://internetua.com/obnarujeno-vimogatelskoe-po-na-osnove-ishodnogo-koda-proekta-EDA2). – 2016. – 27.01).

***

MAC-адреса мобильных телефонов могут использоваться в качестве средства слежения. Об этом со ссылкой на анонимного исследователя безопасности сообщает издание «Либератум».

Специалист во время отдыха во Франции обнаружил изменение стоимости доступа к гостиничному Wi-Fi на 20–70 % в зависимости от клиента. Аналогично менялись цены на прочие предоставляемые отелем услуги. Эксперту не удалось понять, каким образом администрация заведения устанавливала цены индивидуально для каждого клиента.

Как выяснилось позже, злоумышленники собирали базу данных аппаратных MAC-адресов с привязкой к посещенным заведениям. Сбор данных осуществлялся путем создания специальных точек доступа Wi-Fi с искусственно заниженной мощностью. Полученная от разных магазинов и заведений информация объединялась, и злоумышленники получали возможность проанализировать интересы и покупательскую способность каждого клиента. В дальнейшем стоимость товаров и услуг изменялась в соответствии с проанализированными данными.

Схема работает следующим образом. Владельцы магазинов или заведений устанавливают на входе сетевой маршрутизатор с искусственно пониженной мощностью и радиусом действия в 3–5 м. Устройство при этом настроено на работу в режиме открытой сети. Если у покупателя на телефоне включен Wi-Fi, мобильное устройство обнаруживает открытую сеть и отправляет специальный сигнал. В ходе данного взаимодействия точка доступа успевает определить и сохранить в базу данных уникальный аппаратный адрес адаптера Wi-Fi.

По мнению специалиста, в мире существуют целые сети по сбору и обмену подобной информацией, состоящие из множества крупных и мелких предприятий. Скорее всего, к обработке данных причастны аналитики, маркетологи и специалисты в сфере «больших данных» (Big Data). Законных способов прекращения шпионажа не существует – в настоящее время сбор данных о MAC-адресах не запрещен ни в одном государстве.

По мнению специалиста, единственным способом защититься от подобной слежки является отключение Wi-Fi на смартфоне ***(Хакеры следят за пользователями Wi-Fi по MAC-адресу мобильных устройств // InternetUA (http://internetua.com/hakeri-sledyat-za-polzovatelyami-Wi-Fi-po-MAC-adresu-mobilnih-ustroistv). – 2016. – 28.01).***

***

Антивирусная компания ESET отчиталась по статистике кибератак на программные продукты Windows от Microsoft в 2015 г. В частности, в отчете отмечается рост в четыре раза количества уязвимостей в различных

компонентах пользовательского режима ОС Windows, которые могут использоваться для удаленного запуска выполнения вредоносного кода на ПК или для получения максимальных прав в системе.

Всего за 2015 г. Microsoft закрыла 571 уязвимость в своем ПО, это на одну треть больше по сравнению с 2014 г. Лидером по количеству уязвимостей среди ПО Microsoft уже второй год подряд является браузер Internet Explorer. В 2015 г. таких уязвимостей найдено 231 штук, что составляет легкое снижение по сравнению с 243 уязвимостями в 2014 г. На долю нового браузера Microsoft Edge пришлось 27 уязвимостей ***(За год количество уязвимостей в Windows выросло в четыре раза // IGate (http://igate.com.ua/lenta/12932-za-god-kolichestvo-uyazvimostej-v-windows-vyroslo-v-chetyre-raza). – 2016. – 27.01).***

***

По данным ИБ-эксперта К. Викери, злоумышленники используют неправильно сконфигурированные принтеры корпоративного класса для хранения вредоносных кодов и обхода обнаружения антивирусными продуктами.

После обнаружения утечки данных 13 млн пользователей утилиты MacKeeper Викери был приглашен в компанию MacKeeper в качестве руководителя Центра исследования безопасности. В рамках исследований на новой должности эксперт обратил внимание на возможность использования принтеров злоумышленниками для хранения вредоносного ПО и обхода решений безопасности.

Как сообщил К. Викери, в настоящее время к Интернету подключены тысячи принтеров с гигабайтами внутренних хранилищ. Объектом его исследований стали устройства производства компании Hewlett-Packard. Злоумышленники получают доступ к принтерам HP через порт 9100 и используют их в качестве FTP-серверов. С помощью инструментов с открытым исходным кодом они загружают на принтер файлы, доступные через браузер по адресу http://<Printer_IP_Address> /hp/device /<File_Name>.

«Перед хакером открывается море возможностей. Злоумышленник может хранить на вашем принтере вредоносные страницы и скрипты, а также связывать их с потенциальными жертвами. […] Данные принтеры могут быть отличными репозиториями», – сообщает Викери в своем блоге.

Принтеры корпоративного класса обычно включены 24 часа в сутки и даже в спящем режиме могут играть роль хранилища. Дополнительный бонус для злоумышленников – мало кто проверяет содержимое жестких дисков принтеров, поэтому о сохранности файлов можно не беспокоиться. Из-за отсутствия в большинстве случаев системы авторизации шансы обнаружить атаку ничтожно малы ***(Злоумышленники используют принтеры для хранения вредоносного ПО // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-printeri-dlya-hraneniya-vredonosnogo-po). – 2016. – 28.01).***

***

Хакерская группировка, стоящая за Black Energy, сменила тактику и начала распространять данный троян через письма с вредоносным вложением в виде документа Microsoft Word. Специалисты глобального исследовательского центра «Лаборатории Касперского» (GReAT) обнаружили вредоносный документ Word, распространявшийся в рамках текущей атаки на критические объекты Украины.

Предположительно, русскоязычная группировка Black Energy является организатором кибератак на энергетические компании Украины, осуществленные в декабре прошлого года. По мнению экспертов, в данном случае целью злоумышленников являлся популярный украинский телеканал «СТБ».

С середины 2015 г. Black Energy в основном распространялся через документы Microsoft Excel и PowerPoint. Теперь злоумышленники решили опробовать новый вектор атаки. Как показал анализ, при открытии вредоносного Word-документа на экране отображается рекомендация включить макросы. Следование данной подсказке приведет к запуску скрипта, инициирующего загрузку Black Energy.

Согласно отчету компании SentinelOne, атаки Black Energy – работа инсайдеров. По данным специалистов, вариант Black Energy 3 эксплуатирует уязвимость в Office 2013, позволяющую удаленно выполнить произвольный код. Данная проблема была устранена некоторое время назад. Атака будет успешной только в случае, если на целевом компьютере установлена неисправленная версия ПО или сотрудник преднамеренно (или случайно) откроет инфицированный Excel-документ.

По мнению экспертов, данная модификация трояна уже присутствует на системах промышленного управления по всей Украине. В дальнейшем вредоносное ПО может использоваться для осуществления атак на объекты критической инфраструктуры, системы управления транспортом и организации здравоохранения ***(Новоя тактика рассылки трояна Black Energy, атакующего компании в Украине // HiTech-News.ru (http://hitech-news.ru/2016/01/30/novoya-taktika-rassylki-troyana-black-energy-atakuyushhego-kompanii-na-ukraine/). – 2016. – 30.01).***

***

Активно обсуждаемая в IT-отрасли тема «Интернета вещей» (Internet of Things, IoT) продолжает оставаться в центре внимания специалистов по информационной безопасности, выражающих уверенность в том, что уже совсем скоро киберпреступники смогут создавать DDoS-ботнеты невиданной ранее мощности, состоящие из уязвимых IoT-устройств.

По мнению экспертов компании Qrator Labs, занимающейся исследовательской деятельностью в области защиты от DDoS-атак, распространение «Интернета вещей» несёт в себе масштабную угрозу: производители всевозможных подключённых устройств (чайники, ТВ,

автомобили, мультиварки, весы, «умные» розетки и т. д.) далеко не всегда заботятся о должном уровне их защиты. Часто такие устройства используют старые версии популярных операционных систем (в частности, тот же Android), и разработчики не заботятся о регулярном их обновлении на новые версии, в которых устранены уязвимости. Как следствие, подключённые к глобальной сети IoT-устройства потенциально могут стать частью инфраструктуры злоумышленников и быть задействованы в DDoS-атаках.

Предвестники проблемы IoT уже прозвучали в 2015 г. В частности, специалистами Qrator Labs был обнаружен ботнет, построенный на сетевых маршрутизаторах, в которых не поменяли стандартные пароли. «Казалось бы, сетевое оборудование настраивается квалифицированными специалистами и в последнюю очередь должно оказаться под угрозой взлома. Но практика показывает обратное. Что уж говорить об уязвимостях пользовательских устройств. Мы прогнозируем, что очень скоро все смартфоны на старых версиях Android будут состоять как минимум в одном ботнете. За ними последуют все “умные” розетки, холодильники и прочая бытовая техника. Уже через пару лет нас ждут ботнеты из чайников, радионянь и мультиварок. “Интернет вещей” принесёт нам не только удобство и дополнительные возможности, но и много проблем. К этому следует готовиться уже сейчас», – уверен А. Лямин, глава Qrator Labs ***(«Интернет вещей» открывает новые возможности для кибератак // InternetUA (http://internetua.com/internet-vesxei--otkrivaet-novie-vozmojnosti-dlya-kiberatak). – 2016. – 30.01).***

***

В России выявлен новый вид мошенничества – хищение средств с карт, оснащенных технологиями бесконтактной оплаты товаров. Как сообщают «Известия» со ссылкой на данные компании Zecurion, в минувшем году при помощи самодельных терминалов (RFID-ридеров) злоумышленники похитили 2 млн р. По словам ряда экспертов, преступники научились списывать деньги с карт, используя смартфоны с чипами NFC.

Технологии бесконтактной оплаты товаров применяются платежными системами Visa (PayWave) и Mastercard (PayPass) для упрощения безналичной оплаты покупок. Карты с технологией PayPass выпускает 43 крупных российских банка, карты с PayWave – 16. Оплата такой картой не требует введения PIN-кода и подписи на чеке, если сумма покупки не превышает 1 тыс. р. По данным Zecurion, бесконтактными банковскими картами пользуется 2 млн россиян.

По сути, мошенническая схема похожа на перехват сигналов электрозамков угонщиками автомобилей. Злоумышленники списывают деньги с бесконтактных карт при помощи самостоятельно изготовленных считывателей, способных сканировать банковские карты с чипами RFID. В целом разработка представляет собой аналог легального бесконтактного PoS-терминала – RFID-ридера, посылающего электромагнитные сигналы.

По словам руководителя аналитического центра Zecurion В. Ульянова, изобретение хакеров имеет сходство с легальным устройством, но обладает более широкой функциональностью. Преступнику достаточно приблизить такой считыватель к карте с чипом RFID на 5–20 см, и вся необходимая информация будет получена. Похищенные данные злоумышленники записывают или передают на карты-клоны, используемые для дальнейших операций.

Стоимость легального считывателя для PayPass и PayWave составляет не менее 20 тыс. р. Изготовление собственного ридера обходится хакерам в 100 дол. Самый простой считыватель состоит из специального контроллера, антенны для приема сигнала, интерфейса для подключения к компьютеру и программного обеспечения.

Как отмечает замдиректора департамента аудита защищенности компании Digital Security Г. Чербов, для осуществления транзакции или изготовления дубликата магнитной полосы карты злоумышленникам достаточно получить номер и конечную дату обслуживания карты ***(Небезопасный PayPass: хакеры научились воровать с кредитных карт «по воздуху» // МедиаВектор (http://mediavektor.org/7551-nebezopasnyy-paypass-hakery-nauchilis-vorovat-s-kreditnyh-kart-po-vozduhu.html). – 2016. – 25.01).***

***

Вирусные аналитики компании «Доктор Веб» обнаружили в официальном магазине Google Play десятки игровых приложений, скрывающих в себе троян. Основное предназначение вредоносного кода Android.Xiny.19.origin – загрузка, установка и запуск программ по команде злоумышленников. Кроме того, троян способен показывать навязчивую рекламу, сообщили в «Доктор Веб».

Вирусописатели встроили данного трояна в более чем 60 игр, которые затем разместили в каталоге Google Play от имени более чем 30 разработчиков, в частности Conexagon Studio, Fun Color Games, BILLAPPS и многих других. «Доктор Веб» уже оповестил Google о данном инциденте, но на момент публикации компанией данного материала заражённые игры ещё оставались в Google Play – рекомендуется не скачивать игры из каталога в ближайшие часы на устройствах, не защищённых антивирусом.

На первый взгляд, выявленные программы мало чем отличаются от множества других подобных приложений – несмотря на то что качество их весьма посредственное, после запуска они все же предоставляют владельцам Android-смартфонов и планшетов заявленный функционал. Однако если бы пользователи заранее знали о скрытом в них трояне, они вряд ли согласились бы на инсталляцию данного ПО. Дело в том, что Android.Xiny.19.origin передает на сервер информацию об IMEI-идентификаторе и MAC-адресе зараженного устройства, версии и текущем языке ОС, наименовании мобильного оператора, доступности карты памяти, имени приложения, в

которое встроен троян, а также о том, находится ли соответствующая программа в системном каталоге.

Однако главная опасность Android.Xiny.19.origin заключается в том, что по команде злоумышленников он может скачивать и динамически запускать произвольные apk-файлы. При этом данная функция трояна реализована весьма интересным способом. В частности, для маскировки вредоносного объекта вирусописатели прячут его в специально созданных изображениях, фактически применяя метод стеганографии. В отличие от криптографии, когда исходная информация шифруется, а сам по себе факт шифрования может вызвать подозрение, стеганография позволяет скрывать те или иные данные незаметно. Судя по всему, находчивые вирусописатели подобным образом решили усложнить жизнь вирусным аналитикам с расчетом на то, что они не обратят внимания на внешне безобидные картинки.

Получив от управляющего сервера нужное изображение, Android.Xiny.19.origin при помощи специального алгоритма извлекает из него спрятанный apk-файл, который в дальнейшем запускает на исполнение.

Android.Xiny.19.origin обладает и другими вредоносными функциями. В частности, троян может загружать и предлагать владельцу зараженного устройства установить различное ПО, а при наличии в системе root-доступа и вовсе инсталлировать и удалять приложения без ведома пользователя. Помимо этого, вредоносная программа способна показывать всевозможную рекламу.

Специалисты призывают владельцев мобильных Android-устройств не устанавливать сомнительное ПО, даже если оно находится в официальном каталоге. Все приложения, которые содержат трояна Android.Xiny.19.origin, детектируются и обезвреживаются антивирусными продуктами Dr.Web для Android ***(В Google Play обнаружены десятки приложений с Android-трояном // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/v-google-play-obnaruzheny-desyatki-prilozheniy-s-android.html). – 2016. – 28.01).***

***

Пользователи Facebook стали жертвами новой вредоносной кампании

Исследователи из Comodo Threat Research Lab сообщили о новой спам-кампании, направленной на сотрудников и клиентов различных предприятий. Злоумышленники рассылают вредоносные письма, замаскированные под уведомления Facebook о получении голосового сообщения. Адрес и имя отправителя заставляют думать, будто письмо получено от соцсети, однако домен, откуда оно отправлено, в реальности не имеет к Facebook никакого отношения.

Для обхода спам-фильтров в теме уведомления указываются случайные символы (например, «Доставлено новое голосовое сообщение Lucqmc»). В прикрепленном к письму файле содержится вариант трояна Nivdort, предназначенный для похищения информации. После установки вредонос

копирует себя в директорию C:\ и добавляет в реестр Windows, благодаря чему может запускаться после каждого включения или перезагрузки компьютера.

Модифицируя файл hosts, троян пытается закрыть жертве доступ к сайтам поставщиков антивирусных продуктов. Путем внесения изменений в реестр Nivdort деактивирует сообщения о подозрительной активности из Центра уведомлений Windows.

В начале текущего месяца эксперты Comodo Threat Research Lab зафиксировали аналогичную кампанию, направленную на пользователей WhatsApp. По мнению экспертов, за обе операции ответственна одна и та же группировка ***(Пользователи Facebook стали жертвами новой вредоносной кампании // InternetUA (http://internetua.com/polzovateli-Facebook-stali-jertvami-novoi-vredonosnoi-kampanii). – 2016. – 25.01).***

***

По мнению высокопоставленных немецких чиновников, к прошлогодней атаке хакеров на бундестаг может быть причастна российская военная разведка, сообщает издание Spiegel.

Как заявил изданию один из источников в спецслужбах, слова которого приводятся в статье, хакерские атаки на бундестаг были схожи с несколькими аналогичными нападениями в Германии и ряде других стран НАТО.

Отмечается, что федеральная прокуратура 15 января начала расследование дела об атаке. Известно, что хакеры получили доступ к 14 серверам, в том числе к одному из основных серверов немецкого парламента. Однако, как отмечается, до сих пор неясно, какая именно информация была похищена ***(В ФРГ заподозрили российские спецслужбы в кибератаках на бундестаг // InternetUA (http://internetua.com/v-frg-zapodozrili-rossiiskie-specslujbi-v-kiberatakah-na-bundestag). – 2016. – 30.01).***

***

В среду, 20 января, хакерская группировка из Азербайджана Anti-armenia Team взломала 47 армянских сайтов, в том числе ресурс Министерства иностранных дел Армении. Жертвами атаки также стали сайты посольств и консульств Армении в США, России, Аргентине, Австрии, Беларуси, Бельгии, Бразилии, Болгарии, Канаде, Китае и т. д. Как сообщают азербайджанские СМИ, злоумышленники также не обошли стороной ресурсы армянских международных организаций, в том числе сайты миссий в Совете Европы, ООН, НАТО, ОБСЕ и ОЧЭС.

На скомпрометированных ресурсах хакеры опубликовали материалы, посвященные трагедии 20 января 1990 г., когда в результате ввода советских войск в Баку погибло более сотни человек. Этот день вошел в историю Азербайджана как «Черный январь» или «Кровавый январь» и в настоящее время считается днем скорби.

На момент написания новости восстановить работу удалось только сайту Министерства иностранных дел Армении, остальные ресурсы оставались

недоступными ***(Сайт МИД Армении подвергся атаке азербайджанских хакеров // InternetUA (http://internetua.com/sait-mid-armenii-podvergsya-atake-azerbaidjanskih-hakerov). – 2016. – 22.01).***

***

В наборе эксплоитов Angler появилась поддержка уязвимости в Flash, исправленной в декабре прошлого года. Речь идет об ошибке CVE-2015-8651, позволяющей выполнить произвольный код с помощью специально сформированного файла с расширением SWF.

Как сообщил китайский исследователь безопасности под псевдонимом ThreatBook, обновленная версия набора эксплоитов используется для осуществления фишинг-атак в рамках вредоносной компании DarkHotel. Злоумышленники атакуют компьютеры высокопоставленных чиновников с помощью скомпрометированных гостиничных сетей Wi-Fi.

В ходе эксплуатации уязвимости на ПК жертвы загружается вредоносное ПО с именем update.exe. Вредонос замаскирован под набор утилит для генерации ключей SSH. Троян способен обнаруживать установленное на компьютере антивирусное ПО и обходить песочницы.

Набор эксплоитов также используется для распространения вымогательского ПО Cryptowall. По словам исследователя безопасности Kaffeine, обновленная версия Angler появилась совсем недавно и уже получила широкое распространение. Эксплоит затрагивает Flash версии 20.0.0.235.

Конкурентные наборы эксплоитов в настоящее время не внедрили эксплоит для Flash. К примеру, Nuclear, Magnitude и Neutrino до сих пор используют исправленную в октябре прошлого года уязвимости CVE-2015-7645, в то время как в RIG и Sundown применяется эксплоит для исправленной в июле 2015 г. уязвимости CVE-2015-5122 ***(В Angler добавлен эксплоит для опасной уязвимости в Adobe Flash // InternetUA (http://internetua.com/v-Angler-dobavlen-eksploit-dlya-opasnoi-uyazvimosti-v-Adobe-Flash). – 2016. – 29.01).***

***

Киберпреступления по всему миру за 2015 г. нанесли ущерб в 158 млрд дол., передает RNS со ссылкой на отчет по кибербезопасности компании Symantec.

По оценке компании, всего жертвами киберпреступлений за прошедший год стали 594 млн человек. Преступления обошлись в среднем в 358 дол. на человека.

Отмечается, что на устранение последствий кибератак в среднем уходил 21 час ***(Потери от кибератак в 2015 году составили $158 млрд // InternetUA (http://internetua.com/poteri-ot-kiberatak-v-2015-godu-sostavili--158-mlrd). – 2016. – 26.01).***

***

Эксперты компании Symantec сообщили о начавшихся в 2015 г. вредоносных кампаниях по распространению двух семейств троянов для удаленного доступа (RAT). Жертвами Backdoor.Breut и Trojan.Nancrat становятся представители малого бизнеса в Индии, Великобритании и США.

Атаки осуществляются с помощью социальной инженерии, а не эксплоитов. Злоумышленники рассылают фишинговые письма ответственным за финансовые операции сотрудникам компаний с целью хищения средств. Преступники не сосредотачиваются на какой-то определенной отрасли или организации – скомпрометировав одну компанию, они переходят к другой.

Рассылка вредоносных писем осуществляется со взломанных учетных записей. По данным Symantec, 18 % подобных атак заканчиваются успешно, поэтому фишинговые письма являются популярных инструментом у распространителей RAT. В теме таких сообщений чаще всего значатся Re:Invoice, PO, Payment Advise, Quotation Required, Transfer Copy, TT Payment и пр.

Как правило, письмо содержит вложение с zip-файлом. После открытия файла на компьютере устанавливаются Backdoor.Breut и Trojan.Nancrat, предоставляющие злоумышленнику полный контроль над зараженной системой. Атакующий получает доступ к веб-камере и микрофону, может фиксировать нажатия на клавиши клавиатуры, похищать файлы и пароли и многое другое ***(Два семейства RAT атакуют малый бизнес // InternetUA (http://internetua.com/dva-semeistva-RAT-atakuuat-malii-biznes). – 2016. – 24.01).***

Соціальні мережі

як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»

Упорядник **Касаткіна** Тетяна

Редактори: Т. Дубас, О. Федоренко, Ю. Шлапак

Свідоцтво про державну реєстрацію КВ № 5358 від 03.08.2001 р.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, просп. 40-річчя Жовтня, 3
Тел. (044) 524-25-48, (044) 525-61-03
E-mail: siaz2014@ukr.net
www.nbuv.gov.ua/siaz.html

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців виготівників
і розповсюджувачів видавничої продукції
ДК № 1390 від 11.06.2003 р.