СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(17–30.11)

2014 № 22

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(17–30.11)
№ 22

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Facebook разрабатывает новую социальную сеть, но на этот раз исключительного для делового общения, пишет Financial Times.

Facebook at Work будет похож на обычный Facebook, но пользователи смогут иметь два аккаунта – один «нормальный» социальный, а другой – профессиональный.

В новой профессиональной сети люди смогут общаться с коллегами, создавать связи и делиться документами.

Как пишет газета, Facebook at Work уже запущен для сотрудников самой компании. Его создатели, очевидно, надеются составить серьезную конкуренцию уже существующим каналам профессиональной коммуникации, таким как Google Drive, Microsoft Office и Linkedin.

Linkedin, созданный в 2003 г., в настоящее время остается крупнейшей профессиональной сетью. У этой компании 332 млн пользователей в более чем 200 странах.

К сентябрю у Facebook было 1,35 млрд активных пользователей, сообщила компания. Однако многие работодатели скептически относятся к идее использования социальных сетей на работе, и многие просто запрещают своим сотрудникам пользоваться Facebook в рабочее время.

«Facebook at Work, скорее всего, принесет определенную пользу компаниям, но не ту, что они думают», – говорит профессор А. Спайсер из Cass Business School. «Продуктивность служащих вряд ли повысится, но эта сеть поможет им быть в курсе того, что происходит в компании».

«Социальные сети, такие как Facebook, создают так называемые “слабые звенья” среди сотрудников, – говорит он. – Это люди, с которыми мы общаемся довольно редко и плохо их знаем».

Есть и другая проблема.

«Пользователи такой сети могут легко – и случайно – допустить утечку информации. Кроме того, соцсети, даже профессиональные, могут подорвать существующую иерархию в компании».

Также как и «традиционная» сеть Facebook, Facebook at Work может также отнимать слишком много времени.

Все может кончится тем, что служащие будут тратить все свое время на то, чтобы улучшить свой профиль в сети, вместо того, чтобы заниматься делом ***(Facebook создает новую соцсеть // ЗА Київ (http://zakyiv.com/index.php?nma=news&fla=stat&cat_id=5&page=1&nums=102267). – 2014. – 17.11).***

***

В Интернете появилась новая социальная сеть Durov.IM, название которой недвусмысленно намекает на участие в проекте создателя сети «ВКонтакте» П. Дурова. Домен Durov.im был зарегистрирован 4 апреля этого

года компанией EPAG Domainservices на А. Исмакова, по данным Whois проживающего в Израиле... Доменная зона .im относится к территории острова Мэн.

В настоящее время на домене размещена одноименная социальная сеть, которая проходит бета тестирование. Известно, что участники проекта никаких интервью не дают, однако в качестве домашнего адреса владельца указана Камышовая улица в Санкт-Петербурге, где расположена квартира П. Дурова.

Несмотря на то, что соцсеть существует буквально считанные дни, активность пользователей там довольно высока. На момент написания статьи по статистике портала зарегистрированных пользователей было 3805 человек, из них онлайн – 48. Пока портал не может похвастаться разнообразным функционалом, однако общая направленность проекта довольно очевидна. «А вообще мне нравятся. Соцсеть, центральное место в которой – не люди, а сообщества. "ВКонтакте", в общем-то, к этому пришел в конце своего пути, набрав по дороге костылей, а тут с этого все начинается», – делится впечатлениями Remote Viewer.

Что касается вопроса о том, имеет ли П. Дуров отношение к проекту, пользователи сети, похоже, нашли для себя исчерпывающий ответ: «Первое правило – не задавать вопросов. Второе правило проекта: никому никогда не говорить о проекте», – пишет Remote Viewer. Третье правило через несколько минут сформулировал М. Иванов: «Не упоминать Его, как создателя проекта».

Несмотря на секретность, а может и благодаря ей, о сайте известно довольно много, но все это информация, за стопроцентную достоверность которой ручаться нельзя. В частности, есть сведения, что соцсеть быстро стала популярной в Украине, что домен Durov.im выставлялся на торги и за него предлагали суммы от 25 до 720 тыс. дол.

Что касается перспектив проекта, то, по мнению Е. Максимовой, директора Российского союза ИТ директоров (СОДИТ), теоретически он вполне может вырасти до уровня «ВКонтакте», «Одноклассников», Facebook и других социальных сетей глобального масштаба. «Если создатели готовы вкладывать в проект большие деньги и у них найдется достаточно интересных идей – никаких препятствий к тому, чтобы стать в один ряд с крупнейшими соцсетями у проекта нет», – прокомментировала она ФБА «Экономика сегодня» ***(Появилась новая социальная сеть Durov.IM // Media бізнес (http://www.mediabusiness.com.ua/content/view/41396/118/lang,ru/). – 2014. – 17.11).***

***

Во время телефонной конференции для аналитиков Analyst's Day Conference Twitter поделился своими планами на будущее, среди которых расширение функционала сервиса микроблогов и создание абсолютно новых приложений.

Среди новых возможностей обсуждалось расширение использования личных сообщений (Direct Messages). Идея состоит в том, что пользователь сможет отправить публичный твит другому пользователю личным сообщением и продолжить общение на эту тему в приватном режиме.

Компания также планирует добавить возможность записи видео в режиме реального времени и его редактирования в собственной платформе. Это значит, что можно будет записать видео, находясь в мобильном приложении Twitter, и сразу опубликовать его в социальной сети. В настоящее время непонятно, как именно будет реализован этот функционал, но уже известно, что время записи ролика не будет ограничиваться 6 с, как, например, в приложении Vine.

Ещё одна функция названа «Пока вы отсутствовали» (While you were away). Она отбирает лучшие твиты из сети пользователя со времени его последнего посещения Twitter и располагает их в верхней части Хроники.

Введение этого функционала знаменует собой значительный разрыв с основной Хроникой Twitter, организованной в обратном хронологическом порядке. Сервис микроблогов также экспериментировал с показом твитов, понравившихся людям, на которых пользователи подписаны. Но это намного более агрессивный переход от неотфильтрованной ленты к отсортированной автоматически.

Новая опция Timeline Highlights – компромисс между неотсортированной классической новостной лентой Twitter и более фейсбукоподобной лентой, отсортированной автоматически. You Were Away прикрепляется наверху Хроники, оставляя остальные твиты в стандартном обратном хронологическом порядке. Это значит, что наиболее интересные для пользователя твиты не «утонут» под шквалом других многочисленных твитов в ленте.

Twitter также планирует создание бóльшего количества автономных приложений для расширения своей экосистемы. Какие именно продукты будут разрабатываться, осталось неизвестным.

Кроме того, сервис микроблогов планирует решить вопрос расширения своей аудитории и привлечения новых пользователей. В настоящее время у Twitter 500 млн пользователей, которые зарегистрированы в сети, но не публикуют твиты, а используют сервис периодически, переходя по ссылкам в поисковых результатах или на других сайтах. Компания надеется превратить этих пользователей в постоянных участников, вовлекая их с самого начала взаимодействия с сервисом. С этой целью планируется запуск нового процесса регистрации пользователей и новой «Мгновенной Хроники» (Instant Timeline).

Во-первых, Twitter собирается удалить многие шаги в существующем процессе регистрации. При этом самое важное нововведение – это предложение новым пользователям указать, какие темы им интересны. После того, как пользователь выберет интересующие его темы и завершит процесс регистрации, Twitter мгновенно заполнит его хронику релевантными

аккаунтами. Это важное изменение получило название Instant Timeline («Мгновенная Хроника»).

Вместо того чтобы искать компании или публичных лиц, в которых пользователь заинтересован, Twitter сразу предложит ему несколько таких аккаунтов и доставит их твиты в Хронику самом начале его работы с сервисом.

Также в процесс регистрации будет включен импорт контактов из адресной книги пользователя для поиска его друзей в сервисе микроблогов.

Однако наибольшей трудностью для компании будет поддержание вовлечённости существующих пользователей. В самом начале существования Twitter практически каждый участник соцсети искал интересных пользователей, чтобы подписаться на их твиты. Но со временем неотфильтрованные новостные ленты переполнились. Чтобы не потерять действительно интересный контент среди множества других твитов, пользователи стали более осторожно подходить к добавлению новых аккаунтов в свою ленту. В то же время, никому не нравится ощущение, что он говорит в пустоту.

«Twitter нужно помочь новым или неактивным пользователям получить подписчиков. Иначе, они решат, что их твиты бессмысленны, и перестанут их публиковать», – считает Д. Констайн, журналист издания TechCrunch.

Twitter также планирует увеличить объём поисковой рекламы сервиса. Этот шаг направлен на привлечение тех пользователей, которые производят поиск по запросам, относящимся к соцсети. Например: «Что такое хэштег?». Рекламные объявления будут направлять потенциальных пользователей на образовательные страницы, которые разъясняют работу Twitter и его преимущества.

«Вас может тошнить от селфи ведущей “Оскара” Э. ДеДженерес, но оно настолько культовое, что Twitter использует его в качестве примера ценности как шеринга, так и потребления твитов», – добавил Д. Констайн.

Кроме того, Twitter удвоит количество стран, где выступит партнёрской площадкой для местных новостных и развлекательных СМИ. Возможности сервиса микроблогов позволят представителям медиа публиковать запоминающиеся твиты, попадать в тренды; обеспечит максимально интерактивное взаимодействие с аудиторией за счёт запуска голосований и других социальных активностей ***(Twitter расширит функционал соцсети и создаст новые автономные приложения // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_rasshirit_funktsional_sotsseti_i_sozdast_novye_avtonomnye_prilozheniya). – 2014. – 18.11).***

***

Пользователи сервиса Instagram получили возможность редактировать подписи к фотографиям и коротким видеороликам после их публикации. Об этом говорится в официальном блоге Instagram.

Ранее пользователи, которые делали ошибку в первоначальной подписи к фото, хотели ее поменять или удалить, были вынуждены удалять фотографию или видеоролик в целом, после чего загружать их заново.

«Редактирование подписей было одной из наиболее запрашиваемых функций со стороны Instagram-сообщества. Вы можете найти новую функцію “Редактировать” в меню под фотографией», – говорят в Instagram.

Кроме того, сервис внес изменения во вкладку «Интересное» (Explore). Иконка вкладки поменялась на увеличительное стекло, а в ее рамках теперь доступны подразделы с потенциально интересными пользователю фотографиями и аккаунтами.

Обновленные приложения можно бесплатно загрузить из Apple App Store и Google Play. Аудитория Instagram превышает 200 млн пользователей ***(В Instagram появилась возможность менять подписи к фото // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_instagram_poyavilas_vozmozhnost_menyat_podpisi_k_foto). – 2014. – 17.11).***

***

Facebook запустил отдельное приложение для сервиса Groups, при помощи которого пользователи могут общаться в тематических группах. Программа доступна на iOS и Android. Об этом ЦП сообщили представители компании, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-prilozhenie-dlja-gruppovogo-obschenija-facebook-groups-42167/).

Сотрудники Facebook отмечают, что «Группы» популярны среди пользователей соцсети – более 700 млн используют функцию каждый месяц. В качестве примера они приводят студентов, которые совместно готовятся к занятиям, компанию друзей, живущих в разных городах и странах, но желающих поддерживать связь, или коллег, которые обсуждают рабочие вопросы в Facebook Groups.

Сервис Facebook Groups доступен как в веб-версии, так и в основном приложении Facebook. 18 ноября на iOS и Android появилось отдельное приложение, доступное во всех странах прямо на старте.

В приложении все группы пользователя собраны в одном месте, а те, которые посещаются чаще прочих, расположены выше.

Создать новую группу можно при помощи кнопки Create («Создать»).

Приложение позволяет управлять уведомлениями и отключать некоторые из них.

На вкладке Discover выводятся группы, которые могут быть интересными пользователю – список рекомендаций формируется в зависимости от места жительства, понравившихся страниц и групп, в которых состоят друзья.

Представители Facebook утверждают, что группы удобно использовать для общения, так как информация не потеряется в цикле переходов между сообщениями, почтой и лентой новостей – здесь все обсуждения собираются в одном месте ***(Facebook запустил приложение для группового общения Facebook Groups // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-prilozhenie-dlja-gruppovogo-obschenija-facebook-groups-42167/). – 2014. – 19.11).***

***

Сервіс мікроблогів Twitter оголосив про запуск функції пошуку за всіма публічними повідомленнями-твітів, які користувачі написали за вісім років існування сервісу, пише Корреспондент.net (http://ua.korrespondent.net/business/companies/3445573-Twitter-zapustyt-poshuk-za-povidomlenniamy-tvitiv).

Досі ькористувачі могли зайти на сайт search.twitter.com для пошуку твітів з яких-небудь тем або про якісь події. Однак для пошуку певного повідомлення або твіта за конкретну дату доводилося користуватися сторонніми інструментами – наприклад, Topsy.

«Більш ніж за вісім років з моменту публікації першого твіту, сотні мільярдів повідомлень фіксували повсякденні справи користувачів і великі історичні події. Наш пошуковий рух зарекомендував себе в пошуку повідомлень про термінові новини і важливі події в реальному часі. Однак наша довгострокова мета – дати можливість людям шукати по всіх твітах, що були коли-небудь опубліковані», – ідеться в повідомленні Twitter.

На сторінці пошукового сервісу можна задати ключові слова чи фрази, хештеги, мову, включаючи російську, акаунти і згадки акаунтів, конкретні місця і дати публікацій, а також емоційний настрій повідомлення (позитивне, негативне, питальне).

Сервіс пояснює, що вже підтримує індексацію повідомлень в реальному часі, яка покриває твіти приблизно за тиждень. Однак повна індексація зажадає набагато більше ресурсів, оскільки обсяг індексованих повідомлень зростає приблизно на кілька мільярдів твітів на тиждень.

Пошук по базі об’ємом близько половини трильйона документів стане доступний користувачам Twitter в наступні кілька днів. Функція буде реалізована в веб-версії Twitter, а також в додатках для iOS і Android ***(Twitter запустить пошук за повідомленнями-твітів // Корреспондент.net (http://ua.korrespondent.net/business/companies/3445573-Twitter-zapustyt-poshuk-za-povidomlenniamy-tvitiv). – 2014. – 19.11).***

***

На пресс-конференции в Сан-Франциско глава технологического подразделения Pinterest М. Лопп представил некоторые демографические данные, характеризующие аудиторию социальной сети. Эта встреча была

проведена накануне мероприятия, посвящённому знакомству с технологической командой Pinterest.

В мае 2014 г. агентство RJMetrics опубликовало результаты исследования, согласно которым женщины составляют бóльшую часть аудитории Pinterest – около 80 %. По словам М. Лоппа, в настоящее время соотношение между мужчинами и женщинами среди пользователей социальной сети изменилось.

За последний год Pinterest удвоил количество активных пользователей мужского пола. Мужчины составляют одну треть всех новых подписчиков социального сервиса, и этот показатель среди них выше, чем среди женщин.

На появляющихся рынках, таких как Индия, Корея и Япония, мужчины и женщины представлены в аудитории социальной сети примерно поровну.

Бóльшая часть выступления М. Лоппа была сосредоточена на улучшениях поискового продукта компании – Guided Search и других технических деталях, показывающих, как социальная сеть обрабатывает более 120 тыс. запросов в секунду.

Напомним, что согласно данным исследования Pew Internet, опубликованным в конце декабря 2013 г., Pinterest является третьей по популярности социальной сетью у жителей США. Её использует 21 % взрослых интернет-пользователей США. Кроме того, этот социальный ресурс был признан аналитиками отрасли одним из самых «женских». Что же касается мужчин, использующих Pinterest, – то, как правило, это учащиеся высших учебных заведений или дипломированные специалисты с доходом выше среднего.

В конце октября 2014 г. Shareaholic представил отчёт о трафике социальных медиа за третий квартал 2014 г.. По его данным, Pinterest догоняет Facebook по количеству перенаправленного на другие сайты трафика. Он приобрёл огромную популярность среди американских женщин, но еще не достиг масштабов своих конкурентов. Имея 70 млн пользователей, Pinterest надежно закрепил свои позиции на втором месте списка социальных источников реферального трафика ***(Pinterest удвоил количество пользователей-мужчин в 2014 году // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_udvoil_kolichestvo_polzovateley_muzhchin_v_2014_godu). – 2014. – 20.11).***

***

В сети появились сообщения о том, что Facebook запустил аналог Foursquare. Facebook Places (Каталог мест) – это своего рода локальный поиск по сайту, который может стать достойным дополнением для некоторых местных поисковых и туристических сайтов.

Поиск осуществляется по названию города или другому топониму.

Однако он отвечает не на все запросы. Например, запрос «Лучшие суши в Лондоне» не дает никаких результатов. Также нельзя искать

страницы отдельных компаний/организаций, даже если они точно представлены в социальной сети.

Определившись с локацией, пользователи могут выбрать нужное место из списка стандартных категорий: «Рестораны», «Гостиницы», «Бары», «Кафе», «Достопримечательности», «Искусство и развлечения», «Кинотеатры» и др.

В каждой категории, соответственно, представлены страницы компаний, однако о том, по какому принципу они ранжируются, пока ничего неизвестно.

В каждой категории есть дополнительная форма поиска, позволяющая пользователю переместиться в интересующее его место.

Со стороны Facebook это большой шаг в направлении локального поиска, который необходим соцсети для удовлетворения потребностей пользователей и привлечения владельцев бизнеса.

Последним, кстати, стоит озаботиться созданием и развитием страниц компании в Facebook, так как Facebook Places (Каталог мест) имеет все шансы стать эффективным рекламным каналом ***(Facebook нашел альтернативу Foursquare // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_nashel_alternativu_foursquare). – 2014. – 20.11).***

***

Команда Facebook представила своим пользователям новый функционал по созданию видео – «Скажи спасибо». Теперь каждый желающий может записать персональную видеооткрытку для своих друзей на Facebook.

Для того чтобы создать видео «Скажи спасибо», нужно перейти по ссылке и выбрать имя друга. Facebook автоматически запишет превью видео. У пользователя будет возможность выбрать из четырех различных тем и добавить те фотографии и посты, которые связаны с общей историей отношений.

После редактирования, созданным видео можно поделиться, и оно появится в Хронике. Если ваши друзья будут отмечены в видео, то это благодарственное послание появится также и в их Timeline.

Число видео «Скажи спасибо», которые может создать один пользователь, не ограничено – поэтому можно записать видео для друзей, родственников, коллег и просто знакомых.

В самое ближайшее время функция «Скажи спасибо» будет доступна во всем мире на стационарных и мобильных устройствах ***(Facebook запускает новый функционал по созданию видео – «Скажи спасибо» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_zapuskaet_novyy_funktsional_po_sozdaniyu_video_skazhi_spasibo). – 2014. – 20.11).***

***

По данным российских чиновников социальная сеть «ВКонтакте» может завершить легализацию контента уже в начале 2015 г., сообщает «ЛІГАБізнесІнформ».

В частности, заместитель руководителя Роскомнадзора М. Ксензов поведал журналистам о том, что в настоящее время «ВКонтакте» вплотную проводит переговоры с крупными правообладателями цифрового контента. Чиновник ожидает, что уже в начале следующего года с ними будет достигнуто соответствующее соглашение.

Также М. Ксензов отметил, что ресурсы типа магазина Apple App Store игнорируют эти процессы, блокируя «ВКонтакте».

«Таким образом, мы видим условия недобросовестной конкуренции. Сейчас "ВКонтакте" хотят сделать так, чтобы пользователи сервиса не заметили изменений, чтобы они для них были максимально комфортны», – подчеркнул чиновник.

Напомним, вступивший в силу 1 августа 2013 г. «антипиратский закон» предусматривает, что правообладатели могут подать иск в суд против любого интернет-ресурса, где будет обнаружен нелегальный контент. На основании решения суда может быть подана жалоба в Роскомнадзор, и если в течение трех дней нелегальный контент не будет удален, провайдер обязан будет заблокировать разместивший его сайт ***(«ВКонтакте» удалит пиратский контент к 2015 году // InternetUA (http://internetua.com/vkontakte--udalit-piratskii-kontent-k-2015-godu). – 2014. – 21.11).***

***

За год с июля 2013 по июль 2014 число украинских Twitter-аккаунтов резко возросло, а их активность увеличилась.

Вероятнее всего, это связано с бурной общественно-политической жизнью в стране – Евромайданом и последующими событиями.

В январе и июле 2014 г. в украинском Twitter дважды происходило резкое увеличение числа пользователей. Первый раз, очевидно, связан с Евромайданом. Второй – с авиакатастрофой в Донецкой области. Половина всех регистраций в июле 2014 г. пришлись на день крушения «Боинга» и следующий день. Всего же в июле 2014 г. появилось около 100 тыс. новых украинских аккаунтов – это больше, чем за первые шесть лет существования сервиса с 2006 по 2012 гг. В итоге на конец июля 2014 г. Поиск по блогам Яндекса проиндексировал почти 600 тыс. украинских аккаунтов Twitter.

Поначалу Евромайдан не сильно повлиял на активность украинских пользователей. Зато в феврале этого года количество публикуемых сообщений резко возросло – среднее число твитов в день увеличилось с 80 тыс. до 180 тыс. записей. А самым активным по числу публикаций в день оказался июль. За 18 и 17 июля – два дня с самым большим числом твитов – в украинских аккаунтах появилось почти миллион сообщений.

С началом Евромайдана доля твитов на украинском языке возросла вдвое – с 6 до 12 %, а 18–22 февраля сообщений на украинском языке было более четверти от всех твитов с украинских аккаунтов.

До 21 ноября средняя длина твита на украинском составляла около 90 символов, а после – более 100. В то же время длина твитов на русском практически не изменилась – около 80 символов в среднем твите.

Самым распространенным хештегом с начала Евромайдана до конца июля 2014 г. в украинском Twitter оставался #євромайдан. Если суммировать все упоминания хештегов с разными вариантами написания слова «Евромайдан» на украинском, русском и английском языках (#євромайдан, #евромайдан, #euromaidan и др.), то с ноября 2013 по июль 2014 г. в украинском Twitter их употребили более 700 тыс. раз.

Многие из часто упоминаемых хештегов в украинском Twitter появились или набрали популярность в период Евромайдана и последовавших за ним событий. Большинство этих тегов выходили на пиковые значения упоминаемости в одни и те же дни: 18–22 февраля, в начале и середине марта, в середине апреля, в конце мая, а также в начале июля 2014 г. ***(Яндекс изучил, как изменился украинский Твиттер за год // ITnews (http://itnews.com.ua/news/75055-yandeks-izuchil-kak-izmenilsya-ukrainskij-tvitter-za-god). – 2014. – 21.11).***

***

В привычных нам соцсетях на смену «обновлению статуса» давно пришли фотографии. Селфи – это просто, быстро и не требует расшифровки, это новая цифровая мода. Однако израильский стартап Ku решил снова придать вес словам и сделать обновления статуса в соцсетях более креативными.

Название Ku взято из окончания слова «хокку» – короткого японского стихотворения, которое имеет определенную слоговую структуру (5-7-5). Помимо краткости, хокку славятся глубиной своего содержания. На первый взгляд они кажутся невероятно простыми, но на деле все иначе.

Самое сложное при креативном написании текстов – это сесть над листом бумаги или за клавиатурой. Ku – приложение для iOS, которое призвано упростить составление статусов, с его помощью каждый пользователь сможет сочинить некое подобие стиха.

Не стоит думать, что с использованием Ku у всех из-под пальцев будут выходить отточенные философские хокку. Программа создана для того, чтобы делать из бытовых статусов нечто более глубокое, не столь заштампованное.

В Instagram пользователям предлагается украсить свои фото с помощью квадратных рамок, наложения фильтров и т. п., а приложение Ku предлагает наводящие вопросы, которые должны вдохновить на сочинительство.

Они очень обыденны, например, «как вы пообедали?» или «что вы делали прошлым вечером?», но рутинность вопросов только к лучшему, поскольку это дает пользователям простую отправную точку и так легче преодолеть писательский блок и развить свою мысль.

Как только пользователь составит свое квазихокку (квази – потому что строгих правил написания нет, нужно только уложиться в 3 строчки), то приложение предложит дополнить его дудлом или фотографией.

Также к постам можно прикреплять хэштеги, что поможет людям быстро находить контент одной тематики или хокку (если вы решите придерживаться традиционной формы написания). Статусами можно делиться в сети Ku, где другие пользователи будут их комментировать, лайкать и распространять в других соцсетях.

Ku – это красиво сделанное приложение, которому, впрочем, вряд ли удастся свергнуть господство фотостатусов в социальных сетях. Для написания чего-либо требуется больше усилий, чем для того, чтоб щелкнуть затвором, но с помощью Ku можно переосмыслить суть текстовых постов и слегка отвлечься от повальной моды на селфи ***(Ku – социальная сеть для создания креативных статусов // NewsOne (http://newsone.ws/technology/ku-sotsialnaya-set-dlya-sozdaniya-kreativnykh-statusov-20-11-2014). – 2014. – 20.11).***

***

На днях пользователи Google+ получили возможность отслеживать количество упоминаний их профиля другими участниками социальной сети.

Функция доступна в отдельной вкладке «Упоминания» на странице профиля и постепенно запускается для всех стран мира.

Ранее ознакомиться со статистикой упоминаний можно было, лишь кликнув по кнопке уведомлений в верхнем правом углу страницы профиля. Там же можно было увидеть статистику отметок +1, личных сообщений и любых взаимодействий с контентом профиля.

Вкладка «Упоминания» позволяет получить прицельную статистику упоминаний профиля в Google+. Функционал позволит маркетологам находить пользователей, наиболее активно вовлечённых в обсуждение контента, публикуемого владельцем страницы.

Владельцы публичных страниц также могут отслеживать упоминания в выпадающем меню вкладки Stream.

В апреле 2014 г. в Google+ появилась метрика Views («Просмотры»). Она показывает количество просмотров другими пользователями профиля, публикаций, фото и видео с учётом перепостов и переходов пользователей на страницы контента ***(Пользователи Google+ могут отслеживать количество упоминаний профиля // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/polzovateli_google_mogut_otslezhivat_kolichestvo_upominaniy_profilya). – 2014. – 24.11).***

***

Украинские пользователи смотрят на YouTube более 4,4 млн часов видео в день, 25 % из которых приходится на просмотры с мобильных устройств и планшетов. Такую статистику озвучил Ю. Хазанов, менеджер по партнерским программам YouTube в Восточной Европе. Об этом со ссылкой на delo.ua пишет Marketing Media Review (http://mmr.ua/news/id/majdan-i-vojna-na-vostoke-uvelichili-interes-k-ukrainskomu-kontentu-na-youtube-na-37-42266/).

За год количество часов украинского контента, который смотрят украинцы каждый месяц возросло на 37 %, с октября 2013 по октябрь 2014 г. Рекордсменом по количеству часов, показанных в прямом эфире на YouTube, за всю историю сервиса стало Громадське ТВ. Сегодня этот канал имеет имеет 307 подписчиков и 126 млн просмотров.

«Ежемесячные просмотры украинских партнеров возросли на 28 % с октября 2013 г. по октябрь 2014. А с начала года доходы украинских партнеров увеличились на 22 % и составляют несколько миллионов долларов», – сообщил Ю. Хазанов.

По его словам, более 1 млн человек сегодня зарабатывает на YouTube. Не отстают здесь и украинцы. К примеру четыре канала о вязании студии SHERU Sheruknittingcom на YouTube за полтора года существования получили 167 тыс. подписчиков и 25 млн просмотров на русском языке и 100 тыс. подписчиков и 15 млн просмотров на английском. Команда из семи человек выкладывают по одному ролику ежедневно и сегодня имеют около 600 роликов на русском языке и в два раза больше на английском. Один ролик может быть длительность от 3 до 30 мин. По ее словам топовые ролики приносят до 500 дол. в месяц.

«Мы ждем когда YouTube запустится в Китае и Африке. Так как китайцы очень активные и любят делать что-то руками, особенно вязать. По количеству просмотров у нас лидирует США, потом Латинская Америка и Алжир», – говорит Е. Ругальная, одна из основательниц студии SHERU.

Чтобы адаптировать сервис для бизнеса YouTube запускает услугу инфо карты. С помощью нее можно переходить с видео непосредственно на сайт, что призвано увеличивать заходы.

«Мы уже тестируем эту услугу с несколькими партнерами в США, в следующем году она будет доступна по всему миру. С ее помощью можно увеличить количество заходов от 2 % до 20 % в зависимости от нишевости канала», – говорит Ю. Хазанов.

Кроме этого YouTube в следующем году предоставит пользователем платную услугу просмотра видео без рекламы, в США она уже доступна за 10 дол., и «фанатские субтитры», когда подписчики канала могут сами переводить ролики на разные языки и тем самым увеличивать их просмотры и доступность в разных регионах мира.

На сегодняшний день топ-канал в мире – это канал шведского геймера Ф. Чельберга PIE DIE PEW с 13 546 706 просмотрами.

Сегодня YouTube имеет более 1 млрд уникальных пользователей по всему миру. Ежемесячное время просмотра растет на 50 % из года в год, 40 % его уже традиционно приходится на мобильные устройства. На сегодняшний день ежеминутно загружается 300 часов видео, тогда как год назад этот показатель был около 100 часов.

YouTube доступен в 73 странах на 61 языке. В следующем году ресурс планирует открыть еще семь стран ***(Майдан и война на востоке увеличили интерес к украинскому контенту на YouTube на 37 % // Marketing Media Review (http://mmr.ua/news/id/majdan-i-vojna-na-vostoke-uvelichili-interes-k-ukrainskomu-kontentu-na-youtube-na-37-42266/). – 2014. – 25.11).***

***

Компания LinkedIn объявила о том, что сервис SlideShare обогатился новым способом увеличить видимость и охват для пользователей социальной сети для профессионалов.

Теперь с помощью одного клика они смогут загрузить презентацию, инфографику или видео в свой профайл в LinkedIn.

LinkedIn будет спрашивать новых пользователей SlideShare, хотят ли они опубликовать свой контент в социальной сети. Тот же вопрос будет задаваться и существующим пользователям.

«В LinkedIn вы можете наглядно продемонстрировать ваш профессиональный опыт, публикуя визуальный контент, такой как презентации и видео», – сказал представитель компании Д. Луф. «Теперь вы можете делиться контентом в Slideshare с помощью одного клика, расширяя свою представленность, как специалиста, и охват аудитории».

«Все знают старую поговорку: “Лучше один раз увидеть”. Это особенно важно в отношении презентаций, где изображения – фактор, оказывающий влияние», – добавил он.

Согласно данным компании, ежемесячно сервис SlideShare используют 70 млн пользователей ***(LinkedIn упростила шеринг контента SlideShare // ProstoWeb (ttp://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_uprostila_shering_kontenta_slideshare). – 2014. – 25.11).***

***

Компания Abbyy полностью пересмотрела концепцию своего продукта Lingvo, презентовав и запустив бета-версию социальной сети LingvoLive. Сервис адресован переводчикам и пользователям, нуждающимся в переводе, и расположен по адресу lingvolive.ru.

Lingvo, исторически первый продукт Abbyy, представляет собой обширный сборник словарей (до 224 словарей на 19 языках) и представлен на большинстве существующих программных платформ.

Как рассказал на анонсе нового сервиса основатель и глава Abbyy Д. Ян, до сих пор «продукты для разных платформ и форум переводчиков были разрозненны, что не доставляло удовлетворения». Решением проблемы стала разработка единой платформы, позволяющей синхронизировать все продукты для различных устройств и операционных систем и обладающей свойствами социальной сети.

Число пользователей словарей Lingvo в компании оценивается в 8 млн человек, не считая тех, кто прибегает к ним на страницах «Яндекса» и других сервисов.

Все сообщество делится на четыре главных типа пользователей: тех, кому нужен перевод, тех, кто хочет изучать языки и профессионалов в обеих областях – перевода и обучения. Все эти люди пользуются Lingvo, и компания решила «дать им место, где они могут общаться и решать свои задачи», – говорит Д. Ян.

В отличие от классического словарного сервиса Lingvo, предоставляющего доступ к 224 словарям на 19 языках, LingvoLive дает возможность пользоваться 130 словарями для 14 языков, причем все они бесплатны. Представитель Abbyy А. Большаков сообщил CNews, что недостающие языки и словари будут появляться в доступе по мере получения прав на их использование в онлайн бесплатно, либо по мере ввода платного доступа к ним.

Кроме того, пользователи получают возможность принимать участие в создании «живого», «народного» словаря, отражающего актуальные изменения языка.

Сервис пока доступен в двух видах: в веб-интерфейсе и как приложение для устройств на iOS, которое сейчас проходит аппрув у цензоров App Store. Как говорят в Abbyy, эти платформы наиболее популярны у пользователей компании.

Существующие приложения будут продолжать работать и поддерживаться, однако, выпуска их новых версий в планах Abbyy нет. Компания собирается постепенно перевести аудиторию на приложения LingvoLive.

В планах компании выпуск клиентских программ для Android, Windows Phone и для десктопных Windows и OS X. Мобильные клиенты LingvoLive, как рассказал CNews представитель Abbyy, «будут постепенно обрастать теми функциями, какие имели место в мобильных клиентах классического Lingvo».

Сроков появления клиентов для новых операционных систем в компании не называют, говоря, что приоритетной задачей будет поддержка офлайн-доступа в имеющихся LingvoLive-приложениях.

Социальная функциональность сервиса заключается в том, что пользователи смогут запрашивать мелкие подсказки или заказывать переводы текстов. Для целенаправленного общения заказчиков и исполнителей на сайте выделен специальный раздел, названный

«Маркетплейс». Там же, по замыслу идеологов LingvoLive, пользователи смогут знакомиться с интересными преподавателями. У компаний, специализирующихся на обучении языкам, в перспективе появится возможность заводить бизнес-профили.

Отдельным способом монетизации сервиса станет реклама, от которой, впрочем, на первых порах пользователи будут избавлены ***(Abbyy превращает свой знаменитый продукт Lingvo в социальную сеть // Media бізнес (http://www.mediabusiness.com.ua/content/view/41511/118/lang,ru/). – 2014. – 25.11).***

***

Сервис Tumblr, принадлежащий корпорации Yahoo, стал самой быстрорастущей социальной сетью: активная пользовательская база Tumblr за последние полгода возросла на 120 %, сообщает TechCrunch со ссылкой на исследование компании Global Web Index. Об этом сообщает gazeta.ru

Если говорить о числе зарегистрированных пользователей, лидером среди соцсетей стал Pinterest – число его пользователей за 6 месяцев увеличилось на 57 %, а число активных пользователей возросло на 111 %.

Instagram, LinkedIn, Twitter, YouTube и даже Google Plus обогнали по скорости роста пользователей Facebook, самую популярную соцсеть в мире: количество аккаунтов на Facebook за 6 месяцев увеличилось на 6 %, а количество активных пользователей – всего на 2 % ***(Tumblr стала самой быстрорастущей социальной сетью // Media бізнес (http://www.mediabusiness.com.ua/content/view/41524/118/lang,ru/). – 2014. – 26.11).***

***

Издание Mashable составило подборку из 10 растущих социальных сетей, в которых, по мнению редакции, стоит зарегистрироваться тем, кому надоели Facebook и Twitter.

1. Secret

Secret – сервис для публикации анонимных сообщений. Он был запущен в 2013 г. Пользователи социальной сети могут анонимно комментировать «секреты» других людей. Все записи, которые видны в ленте, поступают от друзей пользователя в Facebook, «ВКонтакте» и из телефонной книжки – без указания, кто именно опубликовал тот или иной «секрет».

Проект вызвал большой резонанс как в Соединенных Штатах, так и в России. Дело дошло до того, что главному редактору издания TechCrunch А. Тсотсис пришлось публично опровергать появившуюся в Secret информацию о том, что она покидает свой пост.

2. Shots

Приложение появилось в App Stope в конце 2013 г. Изначально социальная сеть назвалась Shots of Me, но позже имя сократили. В Shots

отсутствует какая-либо функциональность, позволяющая подтрунивать над другими, потому что создатели задумывали социальную сеть полностью свободной от негатива.

Сервис имеет две основных функции: пользователи могут выкладывать собственные селфи и лайкать селфи других или переписываться с друзьями в чате. Возможность комментирования фотографий отсутствует. Учетную запись можно сделать закрытой с помощью настроек конфиденциальности.

3. Snapchat

Snapchat – сервис для обмена самоуничтожающимися фотографиями. Любой снимок, посланный друзьям с помощью Snapchat, автоматически удаляется через заданный пользователем промежуток времени (не превышающий 10 с).

Социальная сеть была запущена в 2011 г. По неофициальным данным, в настоящее время количество её пользователей превышает 27 млн. В 2013 г. сооснователь Snapchat Э. Шпигель отверг предложение М. Цукерберга о приобретении сервиса Facebook за 3 млрд дол. По словам Э. Шпигеля, он был уверен, что мессенджер поднимется в цене – и не ошибся. Осенью 2014 г. оценка рыночной стоимости Snapchat достигла 10 млрд дол.

4. WeChat

WeChat – приложение от китайского гиганта Tencent. Его можно использовать как текстовый мессенджер, а можно – как социальную сеть. WeChat позволяет обмениваться сообщениями с друзьями, загружать фотографии (и применять к ним различные фильтры в стиле Instagram), совершать бесплатные звонки и искать людей поблизости – словом, представляет собой смесь почти всех популярных соцсетей.

Первый релиз приложения был выпущен в январе 2011 г.

5. We Heart It

We Heart It – социальная сеть, основанная на фотографиях. Издание Mashable считает, что сервис напоминает Pinterest, только появился We Heart It раньше. Пользователь может загружать и сохранять понравившиеся снимки, искать фотографии по ключевым словам, отмечать своих друзей на изображениях.

6. Tinder

Приложение, предназначенное для поиска свиданий вслепую через Интернет. Принцип работы сервиса таков: пользователь просматривает фотографии других людей, находящихся в радиусе 160 км от него, и, если кто-то из них ему приглянулся, лайкает его фотографию. Если оказывается, что симпатия взаимная, то пара может начать общаться с помощью Tinder.

Ранее в приложении не было возможности просмотреть отклонённые заявки, но 5 ноября 2014 г. стало известно, что скоро такая функция в Tinder появится. Воспользоваться ей можно будет за деньги. Кроме того, создатели Tinder собираются ввести «Паспорт» – кнопку, которая позволит искать собеседников за пределами радиуса в 160 км.

7. Medium

Платформа для ведения блогов, разработанная создателями сервиса микроблогов Twitter. Сервис собирает похожие публикации и предлагает их пользователю, которому они могут быть интересны. «Вкусы» каждого блогера Medium определяет по его собственным записям, лайкам и комментариям.

Если пользователь хочет высказаться по теме конкретной статьи, он может прокомментировать её, написать автору развернутый ответ (собственную запись в блоге) либо отправить свой комментарий ему на почту.

8. Vine

Vine – это сервис, позволяющий записывать короткие видеоролики и делиться ими с друзьями. Компания была выкуплена Twitter ещё до официального релиза первого приложения. Видео, снятое при помощи Vine, не может быть длиннее 10 с.

9. Bubblews

Bubblews – социальная сеть, которая платит своим пользователям за действия, совершаемые на сайте. Она не имеет мобильного приложения – доступна только веб-версия. Для того, чтобы зарабатывать деньги с помощью Bubblews, нужно писать тексты на английском языке.

Оплачиваются лайки, дислайки, комментарии к записям и просмотры страницы автора другими пользователями. За день можно публиковать не более 10 текстов. Каждые заработанные 50 долларов авторы могут выводить на свой счёт PayPal.

10. Whisper

Whisper – предшественник приложения Secret. С помощью сервиса пользователь получает возможность анонимно публиковать фотографии с подписями, а также комментировать публикации других – публично или в частном порядке. Если пользователь хочет пообщаться с автором какой-либо записи лично, он может это сделать с помощью чата – оба собеседника при этом сохраняют конфиденциальность.

Социальная сеть не обязывает пользователей включать службы геолокации, если они хотят сохранить полную анонимность. Однако в октябре 2014 г. журналисты издания The Guardian выяснили, что Whisper отслеживает своих пользователей, даже если у тех отключено определение местоположения ***(Кто, если не Facebook: 10 быстрорастущих социальных сетей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kto_esli_ne_facebook_10_bystrorastuschih_sotsialnyh_setey). – 2014. – 28.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

У сервісі мікроблогів Twitter зявилася сторінка MaydanDenZaDnem, яка день за днем відтворює події на Майдані річної давнини.

Публікації супроводжуються фактами, фотозвітами та відеороликами, які з'явилися цього ж дня рівно рік тому.

Окрім того, в акаунті можна знайти цитування відомих осіб, народних депутатів та журналістів, що коментували події того часу. 21 листопада в Україні відзначали першу річницю подій на Євромайдані, що розгорталися впродовж зими 2013–2014 рр. ***(В твітері з'явилася сторінка, що день за днем відтворює події Майдану // UkrainianWatcher (http://watcher.com.ua/2014/11/27/v-tviteri-zyavylasya-storinka-scho-den-za-dnem-vidtvoryuye-podiyi-maydanu/). – 2014. – 27.11).***

***

Соцмережі – чудове місце для політика не тільки щоб агітувати, але й неформально спілкуватися зі своїми виборцями. Журналіст «20 хвилин» вирішив промоніторити сторінки вінницьких нардепів на предмет активності в мережі.

О. Домбровський, народний депутат від 11 округу. Політик має свою сторінку в Facebook та «ВКонтакте». Проте у «ВКонтакте» політик не дуже активний, останній запис на його сторінці у цій соцмережі був зроблений 7 вересня 2013 р. А от у Facebook політик активний.

О. Порошенко, нардеп від 12 округу. Має свою сторінку на Facebook, на яку майже не заходить. Останній запис зроблений 28 травня цього року, О. Порошенко оновив фото. Перед цим молодший Порошенко виставив фото, де він разом з батьком голосує на президентських виборах, які відбувались в травні цього року.

І. Мельничук балотувався по 14 округу на Вінниччині. Нардеп був активним у Facebook протягом усієї виборчої кампанії та продовжує бути активним і досі.

На сторінці нардепа від 16 округу Ю. Македона багато записів. Політика вітають з обранням у Верховну Раду, проте він відповідає, що рано, адже ще йдуть суди. Варто зазначити, що нардеп бере участь в обговореннях під записами на свої сторінці.

Нардеп від 18 округу Р. Демчак теж активний користувач Facebook. Постить новини. Теж бере участь в обговореннях під записами на свої сторінці.

Варто також сказати, що на Facebook є сторінка, присвячена екс-меру Вінниці, а нині народному депутатові України В. Гройсману. Записи на ній

постійно додаються, а люди їх коментують. Проте сам політик участі у них не бере.

Також, в рамках експерименту кожному нардепу було відіслано повідомлення, щоб перевірити, як швидко той на нього відповість. Перші відповіді були вже через 20 хв. Це означає, що тепер кожний виборець може поспілкуватися з політиками в соцмережі та дізнатися відповіді, які його так хвилюють. Відповіли всі, крім В. Гройсмана ***(Не можете достукатись у двері нардепів? Пишіть їм в соцмережах // 20 хвилин (http://vn.20minut.ua/Polityka/ne-mozhete-dostukatis-u-dveri-nardepiv-pishit-yim-v-socmerezhah-10424266.html). – 2014. – 17.11).***

***

Після того, як стало відомо, що президент Чехії М. Земан запросив В. Путіна до Праги, чехи розпочали протест проти цього у соцмережах.

Як повідомляє газета «День», через кілька годин після повідомлення про запрошення, у соціальній мережі Facebook з'явилася спільнота «Ми не хочемо Путіна у Празі».

В описі спільноти її організатори пишуть, що не згодні із рішенням президента.

«Ми не згодні з рішенням Земана запросити до Праги президента РФ Володимира Путіна. З урахуванням ситуації, що склалася в Україні, вважаємо це неприйнятним», – ідеться у тексті.

За добу сторінку вподобало понад 5 тис. користувачів ***(Чехи у соцмережах висловлюються проти візиту Путіна до Праги // MediaSapiens (http://osvita.mediasapiens.ua/web/social/chekhi_u_sotsmerezhakh_vislovlyuyutsya_proti_vizitu_putina_do_pragi/). – 2014. – 19.11).***

***

Небайдужі українці вирішили привітати затриманого кримського активіста з ювілеєм

Ще кілька місяців тому український активіст О. Кольченко не міг уявити, що святкуватиме своє двадцятип'ятиріччя в Лефортовому СІЗО. Нині ж, доки активного учасника протестів проти анексії Криму російська влада продовжує утримувати за ґратами, у соціальних мережах стартувала інформаційна кампанія «Привітай із днем народження кримського політв'язня Олександра Кольченка». Таку ініціативу спільними зусиллями організували ініціативна група «Комітет солідарності», Центр «Соціальна дія», проект «Без кордонів», Центр громадянських свобод і «Євромайдан-SOS». Громадські активісти пропонують користувачам соціальних мереж відправити на підтримку українця вітальні листівки. В «Євромайдан-SOS» «УМ» зазначили, що О. Кольченку, якого тримають у в'язниці для залякування кримчан, така моральна підтримка наразі дуже необхідна.

За словами організаторів акції, суть флешмобу дуже проста. Потрібно обрати фотографію з краєвидами Криму та розмістити її на своїй сторінці в соціальній мережі Facebook, «ВКонтакте» або Instagram разом із побажаннями для Олександра та хештегом #freeKolchenko ***(Капнік О. З Днем народження, Сашко! // Україна молода (http://www.umoloda.kiev.ua/number/2566/116/90565/). – 2014. – 21.11).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Руководители социальной сети Facebook заявили, что с 2015 г. изменят формулу, по которой рассчитывается выдача рекламных материалов в ленте новостей, сообщила газета The Wall Street Journal, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-sokratit-kolichestvo-reklamy-v-novostjah-42124/)

Изменения коснутся сообщений, которые по своему характеру похожи на рекламу или промо-материалы. При этом количество платной рекламы в выдаче останется прежним.

По словам вице-президента соцсети по глобальному маркетингу К. Эверсон, изменения направлены на то, чтобы сделать ленту новостей более «личной, актуальной и полезной».

Ранее компаниям предлагалось бесплатно создавать аккаунты, новости которых будут видеть подписчики. Однако компании жаловались на небольшой охват аудитории. В руководстве соцсети сказали, что наиболее качественный контент промо-аккаунтов может быть виден не только подписчикам, а для отсечения «лишних» сообщений был разработан специальный алгоритм ***(Facebook сократит количество рекламы в новостях // Marketing Media Review (http://mmr.ua/news/id/facebook-sokratit-kolichestvo-reklamy-v-novostjah-42124/). – 2014. – 17.11).***

***

Більше половини американських спеціалістів із набору персоналу проглядають профілі кандидатів на вакансії у соціальних мережах.

Про це пише Mashable із посиланням на результати цьогорічного опитування про соціальний рекрутинг – The 2014 Social Recruiting Survey, проведеного компанією Jobvite.

Mashable зазначає, що, враховуючи конкуренцію серед хедхантерів, все більшої популярності набуває рекрутинг у соціальних медіа.

Згідно з дослідженням, рекрутери та компанії все активніше використовують соціальні мережі під час відбору кадрів. Якщо 2010 р. ішлося про 82 %, то у 2012 р. – вже 92 %. Цього року цей показник зріс до 93 %.

Нині 55 % спеціалістів із набору персоналу переглядають профілі кандидатів у соціальних мережах. Метою цього є виявити, ким людина є поза інтерв'ю та резюме ***(55 % рекрутерів переглядають профілі кандидатів у соцмережах // MediaSapiens (ttp://osvita.mediasapiens.ua/web/social/55_rekruteriv_pereglyadayut_profili_kandidativ_u_sotsmerezhakh/). – 2014. – 17.11).***

***

Спустя год после дебютного размещения рекламной кампании в сети Instagram, Майкл Корс запускает там же свой новый проект #instaKors для покупки одежды, аксессуаров и обуви прямо в приложении, пишет Marketing Media Review (http://mmr.ua/news/id/proekt-majkla-korsa-instakors-pozvolit-pokupat-veschi-v-instagram-42140/).

Идея использовать соцсети в качестве дополнительной торговой площадки накануне рождественского бума почему-то пришла в голову только Майклу Корсу. Последний проект марки, именуемый #instaKors, призван упростить до нельзя покупку продуктов Michael Kors.

Что для этого нужно? Во-первых, зарегистрироваться на официальном сайте компании, привязав данные к своему аккаунту Instagram и электронной почте. Во-вторых: зайти в приложение и поставить like на приглянувшуюся модель сумки, клатча, часов, пары обуви и других товаров, помеченных хэштегом #instaKors. В-третьих, проверить почтовый ящик, куда в кратчайшие сроки должно прийти письмо с прямыми ссылками для приобретения приглянувшейся продукции ***(Проект Майкла Корса #instaKors позволит покупать вещи в Instagram // Marketing Media Review (http://mmr.ua/news/id/proekt-majkla-korsa-instakors-pozvolit-pokupat-veschi-v-instagram-42140/). – 2014. – 17.11).***

***

Маркетинговый Партнер Facebook компания SocialCode утверждает, что проактивный подход к таргетингу покупателей на праздники может принести рекламодателям более значительный доход.

Специалисты SocialCode обнаружили, что CPM (цена за тысячу показов) рекламы в ленте новостей неуклонно растет со своего минимума в конце октября – начале ноября до пика в «Черную пятницу» для десктопов и «Кибер-понедельника» для мобильных устройств.

Согласно SocialCode, рекламодатели должны начать размещать свои сообщения как можно скорее, чтобы воспользоваться более низкой стоимостью тысячи показов.

Согласно Experian, в 2005 г. потребители могли получить большие скидки всего два дня в году: в «Черную пятницу» и в день после Рождества. В настоящее время бренды начинают акции раньше, чем когда-либо. Потребители реагируют на это, начиная сезон праздничных покупок задолго

до Дня благодарения. По данным ФНС, более четырех из десяти опрошенных начали сезон праздничных покупок до Хэллоуина.

Это дает возможность рекламодателям воспользоваться более низкими ценами за тысячу показов перед ростом конкуренции и всплеском цены.

Мобильный сегмент является критическим компонентом праздничного шопинга, так как потребители, рекламодатели и ритейлеры подключаются через исследовательские, рекламные и коммерческие операции. По данным исследования, представленного Facebook в течение Рекламной Недели 2014, 65 % взрослых покупателей пользуются мобильными устройствами, совершая покупки в магазине. Исследования также показывают, что в этому году рекордное количество потребителей будет использовать мобильный телефон, чтобы исследовать продукты и цены накануне приобретений. Внутренние данные Facebook показывают, что из 100 % американских пользователей, которые выразили заинтересованность в мобильной рекламе Facebook, более 32 % осуществят конверсию на десктопах в течение 28 дней.

Стоимость тысячи показов рекламы в мобильной ленте Facebook в 4-м квартале 2013 г. показывала пики в «Черную пятницу» и «Кибер-понедельник», окруженные более низкими показателями. Таким образом, бренды могут повысить эффективность рекламы с помощью более усиленных показов накануне и после основных дней покупок ***(Праздничные рекламные кампании Facebook: время старта // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/prazdnichnye_reklamnye_kampanii_facebook_vremya_starta). – 2014. – 17.11).***

***

Однажды специалисты из Buffer собрались и решили проверить, какой же из многочисленных маркетинговых ходов и советов будет работать в Facebook лучше всего. Были рассмотрены следующие варианты, пишет Marketing Media Review (http://mmr.ua/news/id/sovety-po-marketingu-v-facebook-chemu-verit-42171/):

Не публикуйте посты в часы пик.

Выкладывайте посты чаще, не менее 6 раз в день.

Публикуйте посты 1 раз в день, не чаще.

Задавайте своим подписчикам вопросы, чтобы повысить вовлеченность.

Экспериментируйте с манерой постинга.

Размещайте только ссылки.

Добавляйте к ссылкам разные картинки.

На проверку каждого совета была отведена неделя. И вот что из этого получилось.

Совет 1: не публикуйте посты в час пик

Каждый раз заходя в Facebook, пользователь видит приблизительно 1500 различных постов от друзей, интересных страниц и пользователей, на

которых он подписан. Большинство этих постов публикуется днем между пиковыми 8 часами утра и 6 вечера.

Различные специалисты, основываясь на данных исследований, советуют не публиковать свои посты в часы пик, чтобы не потеряться среди тысяч других постов.

Как показывает исследование 5800 страниц в Facebook и 1,5 млн постов, нужно отказаться от постинга в самые популярные часы в пользу постинга в самое «эффективное» время суток.

Стратегия была испытана на странице Buffer в Facebook. Посты публиковались в 7 утра и 11 вечера.

Результаты: едва заметное увеличение вовлеченности в целом, сильнее всего проявилось в 11 вечера. Количество кликов и охват остались примерно такими же, как и до применения данной стратегии, и возросли всего на 6 % и 10 % соответственно.

Совет 2: выкладывайте посты чаще, не менее 6 раз в день

Что такое идеальная частота постинга для Facebook? Специалисты из Buffer рассмотрели этот вопрос со всех сторон, и вот к чему они пришли.

Изначально посты публиковались 3 раза в день. Увеличение частоты публикаций, предположительно, должно было увеличить количество кликов и вовлеченность в течение дня. Одним слово, больше постов – и всего остального станет больше.

Для постинга, который проводился только по будням, было выбрано следующее время:

5:00
8:00
11:00
11:50
13:07
16:00

Результаты: небольшое снижение всех показателей. Количество кликов осталось таким же, а охват упал на 20 %.

Совет 3: публикуйте посты не чаще 1 раза в день

Советы бросали команду Buffer из крайности в крайность: часто публиковать посты теперь было нежелательно, и рекомендовалось ограничиться одним постом в день.

Этот совет был дан специалистами из Social Bakers. В своем исследовании они утверждают, что от 5 до 10 постов в неделю вполне достаточно для успешной брендовой страницы в Facebook. Соответственно, в день постов должно быть 1–2. Решено было публиковать по одному посту каждый день в 9 утра.

Результаты: почти в точности повторяются показатели предыдущего эксперимента. Количество кликов было немногим меньше, чем при постинге постов 6 раз в день. Охват сократился на 25 %.

Совет 4: задавайте своим подписчикам вопросы, чтобы повысить вовлеченность

Какие посты популярнее всего в Facebook? Для тех, кто не знал: содержащие вопрос, то есть, обсуждения.

Самая наиболее часто рекомендуемая маркетинговая стратегия в соцсети – это стратегия общения со своими подписчиками, вовлечение их в беседу. Предполагается, что чем больше разговоров и обсуждений провоцируют ваши посты, тем больше людей будет охвачено при публикации следующего поста.

В течение нескольких месяцев SMM-специалист Buffer публиковал различные вопросы в аккаунте компании. Вопросы размещались 5 раз в неделю и провоцировали активные дискуссии.

Результаты: резкое снижение всех показателей. Совет оказался самым провальным из всех. Число кликов упало на 50 %, а охват – на 40 %. В среднем, количество людей, видевших посты, снизилось на 250 человек.

Для сравнения: типичный вопросительный пост (без ссылки) провоцировал небольшое увеличение количества охваченных пользователей, и в среднем его комментировали 5–7 человек.

Совет 5: экспериментируйте с манерой постинга

Делать посты можно по-разному. Известен по крайней мере 71 способ, как можно это сделать, и команда Buffer решила узнать, есть ли смысл верить разрекламированным советам.

Были испробованы следующие способы:

Пост без текста, со ссылкой

Несколько строк текста

Подпись (каждый пост подписан именем специалиста, который его разместил)

Суперкороткий пост

Очень длинный пост

Размещать посты без текста с прикрепленной ссылкой – это ход, который взяли на вооружение многие бренды. Вместо текста с описанием сути поста, желание перейти по ссылке у пользователей вызывают заголовок, анонс и картинка.

Результаты: количество кликов сократилось на 10 %. Что касается нескольких строк текста, то этот способ не принес особенной пользы и добавил лишь 3–4 клика. Использование подписи добавило в среднем 8–10 кликов каждому посту.

Суперкороткие и очень длинные посты продемонстрировали одинаковый результат, немного увеличив количество кликов.

Совет 6: размещайте только ссылки

Алгоритм ранжирования постов в новостной ленте Facebook уделяет особое внимание типу публикаций, размещаемых брендами. Приоритет имеют посты со ссылками, так как они ранжируются выше, чем просто фотографии с прикрепленными в заголовке ссылками.

Результаты: большое увеличение охваченных пользователей, примерно на 70 %. Количество кликов увеличилось на 10 %.

Совет 7: публикуйте разные картинки к ссылкам

Когда пользователь расшаривает какую-то ссылку в Facebook, пост обычно публикуется с картинкой, которая вытягивается с сайта, где размещен материал. Специалисты из Buffer проверили, действительно ли картинки-ссылки так эффективны, а также выяснили, какие типы картинок, покажут лучшие результаты в соцсети. В своих публикациях они пользуются двумя типами изображений: архивными фотографиями, которые работают фоном для заголовков, а также картинками-тизерами, которые прикрепляются к постам в соцсетях.

Результаты: совет оказался самым действенным из всех, показав хороший результат для картинок-тизеров. Охват увеличился на треть от предыдущего количества охваченных пользователей, а количество кликов возросло на 85 %.

Какие советы реально работают?

Основываясь на приобретенном в ходе проведения экспериментов опыте, команда Buffer считает особенно действенными следующие советы:

Размещение ссылок

Расшаривание по вечерам

Создание картинок-тизеров для постов

Конечно, стоит помнить, что если эксперимент проведет другая компания, то и результаты могут оказаться совершенно иными. Так что если захотите выработать идеальную маркетинговую стратегию для Facebook, то ее придется разрабатывать методом проб и ошибок ***(Советы по маркетингу в Facebook: чему верить? // Marketing Media Review (http://mmr.ua/news/id/sovety-po-marketingu-v-facebook-chemu-verit-42171/). – 2014. – 19.11).***

***

Когда дело касается измерения результатов, главный вопрос, который мы ставим перед собой: «Помогают ли они принимать решения?» Аналитика вашей SMM-активности – это зыбучие пески. Да, лайки тешат самолюбие и – если повезет – вдохновляют на эксперименты, но они не подскажут куда идти дальше (и уж точно не приведут новых клиентов). В этой статье я хочу разобраться, на какие метрики стоит обращать внимание в первую очередь. Интересно, что они могут рассказать внимательному аналитику?

Социальная активность – работа с полной занятостью, без поблажек и выходных, считает А. Керя. Это марафон 24 часа 7 дней в неделю. Впрочем, оценка социального маркетинга проста и адаптивна: вы можете углубиться в аналитику так глубоко, как пожелаете, но даже беглый взгляд на главные метрики позволит сформулировать те направления, которые требуют оптимизации или, наоборот, уже сегодня дают хорошие результаты в виде лидов или положительного информационного шума.

Давайте придерживаться следующего плана из блога компании Buffer. И пусть вас не смущает, что он прост: все вращается вокруг метрик, которые мы постараемся определить чуть позже.

– Экспресс-аудит профилей в социальных медиа

– Определите все официальные и неофициальные странички вашей компании в соцсетях.

– Оцените качество наполнения каждой страницы: графика, информация, плотность и качество сообщений.

– Очертите главные цели вашего бизнеса и сравните сегодняшнюю активность по достижению этих целей с результатами годичной давности.

– Оценка активности лидеров вашего сегмента

– Найдите 4–8 лидеров мнений, чья работа в социальных медиа приносит хорошие результаты.

– Сравните графику и брендинг на их страницах.

– Оцените ключевые метрики конкурентов.

Далее необходимо составить рабочий план улучшений ваших показателей. Если же вы поймете, что необходимо сместить фокус на другие метрики, не стоит бездумно копировать их у конкурентов. Чтобы расставить все точки на i, разберемся, какими метриками оперирует толковый SMM.

15 главных метрик социального маркетинга

Конверсии (conversions) – количество людей, которые совершили желаемое действие. Заплатили за продукт, оставили заявку, заполнили форму на сайте и т. п.

Лиды (leads) – пользователи, которые могут быть «конвертированы» в клиентов. Эта метрика охватывает всех людей, заинтересованных в вашем предложении.

Вовлечение пользователей (engagement) – общее количество лайков, шеров и комментариев на странице в социальной сети.

Охват (reach) – количество ваших подписчиков.

Показы (impressions) – объем аудитории, которая видит ваши сообщения. В идеале, это все ваши подписчики плюс те, кто видит ваши посты, когда подписчики шерят их для своей аудитории.

Воронки продаж (funnels) – путь, который проходит ваш пользователь для того, чтобы превратиться в клиента.

Посещения vs. уникальные посетители (visits/unique visits). Посещения – общее количество заходов на вашу страницу, вне зависимости от того, был ли пользователь у вас раньше или нет. Уникальные посетители – это количество пользователей, которые пришли к вам единожды или многократно.

Показатель отказов (bounce rate) – процент людей, которые оказались на сайте, но не перешли на следующую его страницу и вскоре покинули сайт.

Показатель выходов (exit rate) – процент людей, которые покинули ваш сайт с конкретной страницы. Возможно, что перед этим они посетили еще несколько ваших страниц.

Время, проведенное на сайте (time on site) – время, которое пользователь провел на сайте перед тем, как закрыл окно браузера.

Показатель роста аудитории (audience growth rate) – сравнение вашей аудитории с показателями недельной, месячной, годичной давности.

Средний показатель вовлечения (average engagement rate) – показатели популярности конкретного сообщения в сравнении с общим количеством ваших подписчиков.

Процентная доля ответивших (response rates) – процент людей, ответивших на ваше сообщение. Чтобы рассчитать процентную долю ответивших, общее количество ваших подписчиков (охват) следует разделить на количество пользователей, которые показали определенный уровень взаимодействия.

Входящие ссылки (inbound links) – количество сайтов, на которых размещены активные ссылки на ваш ресурс или конкретную страницу.

Я не сомневаюсь, что вы без заминки ответите на вопрос о бизнес-целях вашей компании. Но вот незадача: вы уверены в глобальной стратегии вашей компании/сайта/блога, но с опаской смотрите на социальные сети. Я вас понимаю: порой сложно определить, насколько этот канал работает и, что еще важнее, найти ту манеру коммуникации с подписчиками, которая сработает в вашем конкретном случае. Как показывает практика, она может существенно отличаться от языка, на котором вы общаетесь с клиентами тет-а-тет или даже на страницах своих сайтов.

Хотя даже беглый взгляд на эти 15 метрик должен существенно облегчить ваш поиск. Соотнесите глобальные цели вашего бизнеса с теми метриками (и – что не менее важно – с механикой их расчета), которые кажутся вам подходящими. Оцените работу конкурентов с помощью инструментов. На этом теория заканчивается.

Если с конверсией все и так ясно – это абсолют любой маркетинговой активности – то на вовлечении пользователей нужно остановиться подробнее. В этом нам поможет А. Кошик. Полагаю, этот маркетолог не нуждается в представлениях. Еще в 2011 г. он опубликовал методологию оценки вовлечения пользователей во всех социальных медиа. По сути, относительный уровень вовлечения пользователей по А. Кошику – это самоценная метрика, которая состоит из четырех составляющих:

– количества коммуникаций (комментариев);

– средний показатель усиления поста (пользователи делятся вашим сообщением со своими подписчиками);

– показатель, который выражает одобрение аудитории (лайки, добавление в избранное, +1, «мне нравится» и т. д.);

– экономическая ценность (сумма краткосрочной и долгосрочной выручки; это следствие вашей активности).

Среди прочих, Moz также используют этот метод для оценки эффективности социального маркетинга, и вот как они объясняют его суть.

Итак, у вас есть все эти метрики, но что именно значат конкретные цифры? Как можно соотнести показатель конверсии на Facebook с этим же показателем в Twitter? Именно тут вступает относительная метрика, предложенная А. Кошиком: мы можем получить средний уровень вовлечения для каждой социальной сети по отдельности (учитывая специфику каждой площадки) – и затем сравнить данные, чтобы увидеть общую картину.

Такой подход позволит оценить фидбэк пользователей во всех социальных сетях. Даже больше – определить качество каждого SMM-канала:

– насколько эффективна ваша стратегия;

какие каналы взаимодействия с потенциальными клиентами стоит сделать более или менее приоритетными;

– насколько оправдана активность в конкретной соцсети в принципе (быть может, там попросту нет вашей аудитории);

– окупаются ли ваши инвестиции на SMM – или вы ведете свои страницы на автомате, «потому что так делают все».

И уже после этого в ход идет Google Analytics с подробными отчетами активности пользователя-из-соцсети на вашем сайте. Как результат – вы видите всю воронку продаж: от первого ретвита до того волшебного момента, когда человек решил стать вашим клиентом ***(SMM-метрики: как измерить эффективность бренда в социальных сетях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/smm_metriki_kak_izmerit_effektivnost_brenda_v_sotsialnyh_setyah). – 2014. – 19.11).***

***

Социальная сеть Facebook продолжает сокращать органический охват сообщений сообществ брендов, стимулируя тем самым рост цен на платную рекламу. Об этом пишет oborot.ru.

По мнению Facebook, бренды публикуют слишком много сообщений, которые являются «чрезмерно рекламными». Такой подход соцсети не только повысит расценки на платное размещение, но и ожесточит конкуренцию среди рекламодателей.

Facebook собирается ограничить и без того невысокий органический охват, однако это коснется не всех сообщений, а лишь тех, которые, по мнению социальной сети, являются наименее креативными. В частности, речь идет о сообщениях, которые предлагают что-либо купить, на что-то подписаться, поучаствовать в лотерее или конкурсе. Проще говоря, под запрет попадут те механики, которые активно используются интернет-магазинами для продвижения.

Брендированные сообщения оценивать будет тот же фильтр, который сейчас оценивает рекламу. В частности, система будет анализировать отзывы пользователей, а также их активность по отношению к продвигаемому контенту. Например, если большое количество пользователей пометит пост

как рекламу или спам, то это послужит сигналом к тому, чтобы свернуть его публикацию, сообщает Yahoo.

В Facebook уверяют, что к столь радикальному решению их подтолкнули результаты опроса пользователей. В соцсети утверждают, что пользователи жаловались на огромное количество рекламных сообщений в ленте. При этом компания не дает никакой информации о количестве опрошенных человек, в каких странах проводилось исследование и т. д.

«Данная мера – это шаг по наполнению ленты новостей пользователей качественным контентом. Она направлена на то, чтобы не растерять аудиторию соцсети», – уверены в Facebook. Там также напомнили о том, что ранее была запущена возможность отключать сообщения конкретных страниц или друзей, которые слишком часто публикуют рекламу.

Стоит отметить, что подобное решение полностью вписывается в политику Facebook последнего времени. Так, например, ранее Facebook сократил количество рекламных мест, что привело к росту цен на размещение в третьем квартале на 274 %, в то же время физический объем рекламы уменьшился на 56 % ***(Facebook продолжает взвинчивать цену на рекламу // Media бізнес (http://www.mediabusiness.com.ua/content/view/41424/118/lang,ru/). – 2014. – 18.11).***

***

Совершая покупки в Интернете, люди руководствуются мнением других пользователей и охотнее покупают товары в магазинах, которые собрали больше лайков в социальные сетях вроде Facebook, пишет Marketing Media Review (http://mmr.ua/news/id/kak-lajki-v-facebook-zastavljajut-sovershat-pokupki-42178/).

Интернет-шопинг покоряет города и страны: оборот торговли в сети в этом году достигнет 600 млрд дол. и удвоится к 2018 г. Новые технологии меняют поведение покупателей и наши мотивы: в сети нельзя пощупать ткань платья или проверить на прочность сумку, но можно узнать, как эти товары понравились тем, кто их уже приобрел.

Отзывы пользователей на страничках магазинов и производителей в социальных сетях становятся чуть ли не главным двигателем онлайн-торговли, уверены немецкие ученые из Johannes Gutenberg-University Mainz, которые изучили, как люди делают покупки в Интернете.

Лайк в помощь

В сети оценки, рекомендации и мнения других пользователей играют особенно важную роль. Рекомендации лежат в основе различных сервисов вроде Airbnb: пользователи оценивают людей и услуги, которые они предлагают. Да и в крупнейшей социальной сети Facebook кнопка Like играет ключевую роль.

Социальные сети и различные интернет-сервисы аккумулируют информацию о собственных клиентах и их предпочтениях и постоянно

спрашивают их, как им понравились приобретенные товары, и почему они решили купить именно их. Выясняется, что люди в сети больше доверяют чужим рекомендациям и мнениям, чем любой рекламе.

Немецкие ученые решили доказать, насколько важны лайки для интернет-магазинов. Их основной вывод довольно прост: если вы хотите увеличить продажи, добавьте на страницу продукта окошко с отметками пользователей социальных сетей и соберите как можно больше лайков. Это позволит привлечь покупателей, особенно тех, кто хочет купить что-нибудь для собственного удовольствия и развлечения.

Эксперимент в магазине игрушек

Немецкие ученые, чтобы установить связь между рекомендациями пользователей и покупками онлайн, провели простой эксперимент. В основе эксперимента лежат отметки Like, которые ставят пользователи социальных сетей. Обычно они отмечают, что им нравится товар, который устраивает их по качеству. Это простой и удобный способ оценить товар.

В эксперименте участвовал популярный в Германии интернет-магазин игрушек и настольных игр. Дизайн магазина похож на Amazon. На странице товара можно найти информацию о нем, цену, способ доставки и фотографии товаров. Кроме того, на сайте есть отдельное окошко для лайков, которые набрал товар.

Продукты оценивали пользователи социальной сети OSN, популярной в Германии. Ею владеют хозяева магазина игрушек. Пользователи могут оценивать товары и оставлять рецензии на них. Сеть работает по принципу Facebook: на странице товара пользователю показывают количество отметок «мне нравится» и фотографии пользователей, оценивших товар.

В эксперименте принимали участие пользователи, которые впервые посетили страницу магазина. Половине этих людей показывали отметки «мне нравится» и рецензии, другой – нет. Последние стали контрольной группой. Распределялись пользователи на группы случайно.

В магазине представлено порядка 9,5 тысяч товаров, который набирали от 0 до 477 отметок «Like». Медианное значение – 7 отметок. Цена на товар колеблется в пределах от 79 центов до 480 евро.

Лайки увеличивают продажи

Эксперимент длился 23 дня в феврале 2013. За этот период сайт посетили почти 73 тыс. новых пользователей, которые просмотрели более 112 тыс. продуктов. 791 пользователь заказал хотя бы один товар. Вместе они потратили чуть больше 26 тыс. евро.

Поведение представителей подопытной и контрольной группы различалось. Люди, которым показывали отметки Like, чаще покупали товары и просматривали больше страниц. Они купили товаров почти на 14 тыс. евро – это на 13 % больше, чем сумма, потраченная представителями контрольной группы. Контрольная группа потратила менее 13 тыс. евро.

Шопинг: нужда или развлечение

Всех покупателей можно разделить на две группы. Первая – те, кто пришли за заранее выбранным товаров. Вторая – те, кто просто хочет купить что-нибудь, они занимаются шоппингом для развлечения. Обычно первая группа делает покупки в рабочие часы: у них мало времени на развлечения и они пришли за конкретным товаром. Вторая группа «ходит за покупками» в Интернет вечером и по выходным, когда у многих есть свободное время – они делают покупки для собственного удовольствия.

Вечером и в выходные эффект от оценок пользователей особенно заметен: отметки Like увеличивают расходы на одного посетителя на 26 %, или 9 евроцентов. Подобные покупатели чаще переходят со страницы на страницу и больше просматривают товаров. Таким образом, мнение пользователей наиболее важно для тех, кто покупает ради развлечения ***(Как лайки в Facebook заставляют совершать покупки // Marketing Media Review (http://mmr.ua/news/id/kak-lajki-v-facebook-zastavljajut-sovershat-pokupki-42178/). – 2014. – 19.11).***

***

О. Ларина, эксперт в области интернет-маркетинга, о том, как превратить подписчиков в Facebook в потенциальных клиентов (http://mmr.ua/news/id/kak-predprinimateljam-vesti-profil-kompanii-v-facebook-42196/).

В эффективном продвижении бизнеса на Facebook можно выделить два основных момента: контентная стратегия и вовлечение подписчиков.

Контентная стратегия

Начнем с контента. Я рекомендую выделить четыре основных направления: отраслевой, персоналии, брендированный и развлекательный. По данным репорта Wave 6 и 7, основной целью присутствия украинцев в социальных сетях является развлечение. Логично, что люди хотят переключиться и отвлечься от сложных рабочих задач, поэтому не стоит делать основой своей контентной стратегии аналитические материалы с графиками и таблицами. Рекомендую выделять на развлекательный контент 20 % из 100 % всего контента страницы. Какой это будет контент – каждая компания решает сама. Мотиваторы, книги, фильмы, яркие картинки, вдохновляющие цитаты – это должно быть то, что радует и вдохновляет вашу целевую аудиторию (ЦА).

Брендированный контент также занимает 20 %. Здесь необходимо быть осторожным, потому что Facebook постоянно ужесточает алгоритм формирования ленты новостей. Задача алгоритма – демонстрировать пользователю наиболее релевантный контент, поэтому бизнес конкурирует за внимание пользователя не только с другими бизнес-страницами, но и с его френдами. Здесь важно не переборщить с call to action и айдентикой бренда. Это скорее отталкивает пользователя.

Персоналии – это люди. Причем не только эксперты внутри компании и рядовые сотрудники, но и ваши лояльные клиенты, адвокаты бренда и

лидеры мнений. Чем больше на странице живых и разных людей – тем выше уровень доверия к ней. Принцип социального доказательства отлично работает в социальных сетях, а чужой клиентский опыт по-прежнему является наиболее весомым аргументов при принятии решения о покупке. И я рекомендую выделять на это 30 %.

Отраслевой контент посвящен рынку в целом. Вы можете публиковать обзоры, рейтинги и инфографики. Давать рекомендации, советы и пояснения. Здесь вы наглядно демонстрируете экспертность своей компании в выбранных вами вопросах. Все, что облегчает жизнь пользователю, очень ценится – поэтому смело отдаем отраслевому контенту 30 %. Образовывайте своих клиентов, помогайте им, и они с благодарностью к вам вернутся.

Теперь про время и частоту. Универсальных рецептов здесь нет и быть не может – все зависит от бизнеса и ЦА. Эксперты говорят, что жизненный цикл поста на Facebook в среднем составляет 5 часов. Прибавьте сюда высокую информационную конкуренцию и привычку пользователя просматривать ленту новостей по диагонали. Считаю, что лучше сделать один емкий и интересный пост в день и направить свои усилия на его продвижение, чем сделать три средних и ждать охвата.

Вовлечение подписчиков

Одна из главных целей присутствия бизнеса в социальных сетях – это лидогенерация. Как превратить подписчиков в потенциальных клиентов – один из главных вопросов. Конкурсы «нажми лайк и выиграй айпад» уже практически полностью дискредитировали себя. Это может быстро помочь увеличить охват, но вряд ли огромное количество соревнующихся ботов – ваша цель. Однако конкурсы были и остаются прекрасным инструментом вовлечения. Здесь есть два главных правила – интеграция приза в деятельность бренда и проведение конкурса по правилам. Чтобы оградить себя от возможных претензий, я рекомендую использовать специальные приложения и конструкторы. Вы защищены от накруток, а пользователи получают прозрачный и понятный механизм участия.

Запрос на обратную связь также ощутимо повышает вовлечение подписчиков. Если вы готовы слушать, слышать и меняться – пользователи с радостью поделятся своим мнением и рекомендациями. Безусловно, вы можете столкнуться с негативом, однако конструктивный диалог – наиболее ценное, что может получить и компания, и ее клиенты.

Правильная работа с лидерами мнений может очень благоприятно сказаться на продвижении бизнеса. Если вы точно выбрали интересующих вас персон и договорились о взаимовыгодном сотрудничестве – охват, лиды и конверсия не заставят себя ждать. Благо, в Украине становится все больше подобных примеров.

В качестве итога приведу три основные стадии продвижения бизнеса в социальных сетях. Сначала бизнес становится интересным – пользователи привыкают к интересному контенту, возвращаются снова и снова, читают, комментируют, репостят и рекомендуют другим. Потом бизнес становится

полезным: пользователи находят ответы на интересующие вопросы, оптимизируют важные для себя процессы, взаимодействия становится еще больше. И наконец – бизнес становится необходимым. Именно здесь и начинается конверсия ***(Как предпринимателям вести профиль компании в Facebook // Marketing Media Review (http://mmr.ua/news/id/kak-predprinimateljam-vesti-profil-kompanii-v-facebook-42196/). – 2014. – 20.11).***

***

Важный маркетинговый партнер Facebook, платформа SHIFT, полностью интегрировалась с рекламной платформой Atlas. Это значит, что теперь клиенты получили возможность управлять рекламными кампаниями прямо из интерфейса SHIFT, ключевая статистика по кампаниями будет заимствоваться из Atlas.

«Рекламный инвентарь не должен ограничиваться только размещением на таких площадках, как: Facebook, Twitter и LinkedIn. Сегодня мы обслуживаем объявления, которые размещаются как веб, так и в мобильной среде. И эта реклама не должна быть ограничена одними только показами внутри приложений, разработанных для Facebook», – комментирует Д. Бороу, CEO SHIFT.

Сегодня в компании SHIFT работает более 100 сотрудников, а клиентами маркетинговой платформы являются такие бренды, как: AT&T, American Express и Unilever.

«Именно так должно выглядеть новое поколение рекламных платформ. Мы таргетируем рекламу на конкретных людей, не на cookie. За счёт этого мы способны достигать рекламным сообщением пользователей любых устройств: вне зависимости от того, проверяют они ленты на Facebook или в Twitter, или же взаимодействуют с игровым приложением Angry Birds. Это огромный шаг вперед для рекламодателей», – добавляет Д. Бороу.

29 сентября 2014 г. глава Atlas, принадлежащей компании Facebook, Э. Джонсон официально объявил о запуске новой рекламной платформы – Atlas. Разработчики перестроили сервис для соответствия актуальным маркетинговым реалиям: увеличению охвата пользователей различных устройств и установлению связи между онлайн-показами и оффлайн-покупками.

People-based маркетинг, который предоставляет Atlas, решает эти проблемы. Он помогает маркетологам достигать людей через различные устройства и платформы. С его помощью можно легко решить проблему эффективности рекламы на различных устройствах за счёт настройки таргетинга и измерения производительности. Теперь Atlas также может подключить онлайн-кампании к оффлайн-продажам, в конечном счете, подтверждая реальное влияние цифровых кампаний на управление поэтапным охватом и новыми продажами ***(Платформа SHIFT, маркетинговый партнер Facebook, интегрировалась с Atlas // ProstoWeb***

(http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/platforma_shift_marketingovyy_partner_facebook_integrirovalas_s_atlas). – 2014. – 20.11).

***

Агентство маркетинговых исследований Forrester опубликовало отчет «Стратегии работы с аудиторией, которые еще работают», согласно которому Facebook и Twitter потеряли свою ценность в качестве площадок для SMM.

В отчёте сказано, что крупные социальные сети уже практически бесполезно использовать в качестве площадок для работы с аудиторией и привлечения внимания к бренду, сообщает издание The Wall Street Journal.

Специалисты Forrester полагают, что компании попусту тратят время, усилия и деньги в Facebook и Twitter. Исследование показало, что сообщения известных брендов в соцсетях достигают только 2 % адресатов. Эффективность записей еще ниже: не более 0,07 % подписчиков обращают на них внимания.

«Прекратите использовать Facebook и Twitter как площадки для пиара», – написал в блоге компании Н. Эллиотт, вице-президент и главный аналитик Forrester.

Согласно записи блога, Facebook с января 2014 г. сужает охват неоплаченных записей, чтобы побудить маркетологов платить. Неоплаченные записи исчезают из ленты новостей, платные остаются, что сильно озадачивает всех, кто занимается рекламой в соцсетях.

«Сейчас ясно, что ни Facebook, ни Twitter не позволяют выстроить отношения с потребителем, которых так жаждут маркетологи, – написал Н. Эллиотт. До сих пор большинство брендов использует эти сайты как главные площадки для налаживания контакта с аудиторией. Это трата финансов и человеческих ресурсов, которая не окупается. Для специалистов по маркетингу настало время переходить на сайты, которые способны принести реальную пользу».

Маркетологов, которые ищут способ заинтересовать покупателя, вице-президент Forrester призывает перестать уделять столько внимания сетевым гигантам вроде Facebook и Twitter. В особенности Twitter, так как он сильно ограничивает возможности по коммуникации, порождая множество нелепых ситуаций.

Выбор площадки, в которую стоит вкладывать деньги, зависит от направления работы компании. Указывая на сайт Sony об игровой приставке PlayStation 4 GreatnessAwaits.com, привлекший 4,5 млн посетителей, главный аналитик Forrester предсказывает, что в 2015 г. серьезным прорывом в маркетинге станут небольшие «брендовые комьюнити». По мнению Н. Эллиотта, если ваш продукт или услуга действительно интересует покупателей, они самостоятельно найдут вас.

Кроме того, специалист Forrester призывает не забывать о рассылках.

«Письма рассылки достигают адресата в 90 % случаев, в то время как посты в Facebook – только в 2 %. При этом никто не заглядывает вам через плечо, указывая, что вы можете писать в своём сообщении, а что – нет. Если вы выбираете между новым адресатом в списке рассылки и новым другом в Facebook, всегда выбирайте первое», – посоветовал Н. Эллиотт ***(Деньги на рекламу в Facebook и Twitter уходят впустую // ООО «Состав.ру» (http://sostav.ua/publication/dengi-na-reklamu-v-facebook-i-twitter-ukhodyat-vpustuyu-64726.html). – 2014. – 21.11).***

***

Крупнейшая в мире социальная сеть Facebook дает избранным брендам эксклюзивный доступ к информации, полученной от 1,3 млрд пользователей. Благодаря комментариям и прочим видам социальной активности, крупнейшие рекламодатели узнают, что потребители действительно думают о них, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-pozvoljaet-elitnym-brendam-uvidet-mnenie-polzovatelej-o-nih-42258/)

Бренды и их маркетинговые команды получили возможность глубоко погрузиться в Facebook и измерить общественное мнение благодаря маркетинговой программе под названием Grapevine (Виноградная лоза). Будет ли бренд приглашен в программу, зависит от его финансового состояния. «Рекламодатели, которые тратят миллионы долларов на рекламные кампании и полмиллиона за одно объявление, – вот кто имеет доступ», – сообщил неназванный источник. С Grapevine работают те же бренды, которым Facebook помогает индивидуальными маркетинговыми семинарами.

В Facebook заявляют, что социальная сеть не обменивается информацией с рекламодателями, которые могли бы идентифицировать отдельного пользователя, поэтому все маркетинговые отчеты являются анонимными.

Инструмент похож на то, что Twitter делает со своим «пожарным шлангом» твитов, просеивая поток информации для отслеживания общественного мнения.

Grapevine в конечном итоге может стать гигантской фокус-группой для брендов, позволяя им точно узнать, что пользователи думают о них и их продукции. Поток общественного мнения будет ключевым компонентом для брендов при планировании их праздничных кампаний не только в Интернете, но и на телевидении.

Facebook уже имеет аналогичную программу для анализа настроений, открытую для некоторых медиа-партнеров вроде BuzzFeed, которые использовали ее для оценки отношения общественности к выборам ***(Facebook позволяет элитным брендам увидеть мнение пользователей о них // Marketing Media Review (http://mmr.ua/news/id/facebook-pozvoljaet-elitnym-brendam-uvidet-mnenie-polzovatelej-o-nih-42258/). – 2014. – 25.11).***

***

Специалисты Socialbakers изучили репрезентативную выборку в 1 млн твитов от брендов, проанализировав уровень вовлечения пользователей. Анализировались записи, опубликованные с 3 по 9 ноября 2014 г., пишет Marketing Media Review (http://mmr.ua/news/id/tvity-s-izobrazhenijami-i-tekstom-samye-populjarnye-42237/).

Анализ ТОП-10 выдачи Twitter показал, что наиболее популярные и эффективные в плане взаимодействия с пользователями твиты, содержат прикрепленные изображения.

Постов с фотографиями оказалось 47 %. Специалисты Socialbakers советуют регулярно прикреплять к твитам изображения, если эффект от этого столь ощутим. Говоря о текстовых твитах можно отметить, что причиной их популярности может стать использование их компаниями при поддержке клиентов на социальных платформах.

Коммуникационный потенциал Twitter делает его удобной платформой для взаимодействия пользователей и доступа к свежему и актуальному контенту. Возможности Twitter можно использовать для увеличения количества перепостов, если вы раскручиваете бренд и повышаете информированность пользователей о нем ***(Твиты с изображениями и текстом – самые популярне // Marketing Media Review (http://mmr.ua/news/id/tvity-s-izobrazhenijami-i-tekstom-samye-populjarnye-42237/). – 2014. – 24.11).***

***

Сервис микроблогов Twitter в скором времени начнет собирать информацию о приложениях, которые пользователь загрузил на мобильное устройство. Об этом говорится на странице техподдержки Twitter.

«Чтобы обеспечить большую персонализацию Twitter, мы будем собирать и периодически обновлять список приложений, установленных на вашем мобильном устройстве, дабы аккуратнее подбирать потенциально интересный вам контент», – говорится в сообщении Twitter.

Функция будет включена по умолчанию, однако пользователь может отключить ее в настройках. Кроме того, если пользователь Twitter ранее уже отказался от таргетинга рекламы по интересам на iOS или Android-устройстве, нововведение его не коснется.

Бизнес-модель Twitter практически полностью зависит от таргетированной мобильной рекламы. Кроме того, Twitter не так давно начал показывать пользователям твиты от аккаунтов, на которые они не подписаны, но которые могут быть потенциально интересны для них.

Twitter подчеркнул, что собираться будут исключительно данные о скачанных приложениях, другая информация на смартфонах и планшетах использоваться не будет ***(Twitter начнет отслеживать скачиваемые пользователем приложения // InternetUA (http://internetua.com/Twitter-nacsnet-otslejivat-skacsivaemie-polzovatelem-prilojeniya). – 2014. – 27.11).***

***

Сервис микроблоггинга Twitter тестирует новое предложение для рекламодателей под названием Twitter Offers, которое позволяет им демонстрировать рекламу, связанную с платежными картами, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-testiruet-novoe-predlozhenie-dlja-reklamodatelej-twitter-offers-42297/).

Когда пользователи Twitter видят Twitter Offer в хронике, они могут добавить его к своей кредитной или дебетовой карте и выкупить в режиме реального времени, используя свою платежную карту в магазине, который предложил сделку.

«С Twitter Offers рекламодатели смогут соотносить оплату непосредственно со своей кампанией в Twitter, так что они могут эффективно измерить ROI своих предложений, даже если выкуп происходит оффлайн», – говорит менеджер по продукту Т. Джейн. – «Кроме того, мы делаем его легким для продавцов, потому что они могут использовать свои существующие платежные сети, нет никаких изменений в процессе приобретения, не нужны обучение работников, установка нового оборудования или программного обеспечения. Используя надежные таргетинговые возможности Twitter, рекламодатели могут адаптировать свои акции и кампании к нужной аудитории, оптимизируя представление».

Twitter будет шифровать и хранить платежную информацию пользователей, чтобы было удобнее пользоваться следующими предложениями. При этом пользователь может удалить информацию в любое время.

В настоящее время Twitter тестирует Offers с несколькими брендами на территории США.

Это предложение является следующим шагом после внедрения кнопки «Купить», которую можно использовать с выбранными брендами.

Twitter начал показывать отдельным пользователям в твитах кнопку Buy Now («Купить сейчас») в июне текущего года. Она размещалась в «Продвигающих твитах» от интернет-магазина Fancy в мобильной версии сервиса. На тот момент кнопка была нерабочей.

О том, что Twitter совместно с платёжным стартапом Stripe готовится к запуску покупок непосредственно из твитов, стало известно в конце августа 2014 г.

А уже в сентябре сервис микроблоггинга приступил к тестированию кнопки «Купить» в твитах партнёров сервиса, которая позволяет приобретать товары, не покидая социальной сети. На тот момент нововведение могли видеть только небольшой процент пользователей в США ***(Twitter тестирует новое предложение для рекламодателей Twitter Offers // Marketing Media Review (http://mmr.ua/news/id/twitter-testiruet-novoe-predlozhenie-dlja-reklamodatelej-twitter-offers-42297/). – 2014. – 27.11).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Датские исследователи обнаружили, что использование Интернета усугубляет социальное неравенство.

В то время как более образованные и финансово обеспеченные люди используют сеть для саморазвития и обогащения, другие пользуется Интернетом в основном для общения и развлечений, что приводит к своеобразному расслоению пользователей Всемирной паутины и появлению «информационной элиты».

Цифровое неравенство – это отсутствие равного доступа населения к услугам современных коммуникаций. То есть ситуация, когда часть общества, к примеру, имеет доступ Интернету, а другая часть – нет, что автоматически ставит пользователей сети в более выгодное положение, усугубляя социальное неравенство.

Как выяснили датские ученые из Университета Твенте, в странах, где доступ к Интернету уже практически повсеместен, социальное неравенство проявляет себя с новой, довольно неожиданной стороны.

Речь идет о том, как люди пользуются Всемирной паутиной. Изначально всем казалось, что из-за того, что доступ к полезной информации стал мгновенным, а налаживать контакты стало легче, чем когда-либо, Интернет снизит социальное неравенство.

Судя по результатам нового исследования, все оказалось ровно наоборот. Испытуемых, среди которых были представители самых различных социальных групп Дании, спрашивали, для чего они чаще всего используют сеть. Предложено было 7 типов активностей – поиск информации, чтение новостей, саморазвитие, онлайн-покупки и продажи, общение, проведение досуга, а также компьютерные игры.

Выяснилось, что люди с высшим образованием и высоким уровнем дохода чаще используют Интернет для саморазвития и улучшения своего социального статуса, чем группы с более низким уровнем дохода или не столь впечатляющим образованием, которые используют Всемирную паутину в основном для общения, сетевой коммерции, проведения досуга и компьютерных игр.

Также ученые обнаружили, что более образованные участники опроса демонстрировали более высокий уровень владения компьютером – другими словами, они лучше знали, как и где находить нужную информацию, в сравнении с теми, кто был менее образован.

С годами эта тенденция только растет, отмечают ученые. За 2010–2013 гг. хорошо образованные люди стали чаще использовать Интернет для

саморазвития (сюда относятся онлайн-курсы, чтение большого количества новостей и поиск полезной информации), в то время как менее образованные респонденты все больше склонны пользоваться сетью в развлекательных целях.

Появляется ситуация, в которой Интернет, призванный устранить социальное неравенство, лишь усугубляет его и приводит к появлению «информационных плит», которые по своим характеристикам – образованию, уровню дохода – поразительно напоминают классические социальные элиты. Этот тренд, отмечают ученые, требует дальнейших исследований ***(Среди пользователей Интернета определились «информационные элиты» // InternetUA (http://internetua.com/sredi-polzovatelei-interneta-opredelilis--informacionnie-eliti). – 2014. – 20.11).***

***

Исследователи Мадридского университета, Испания, определили способ быстрого и дешёвого отслеживания уровня безработицы в стране. Простой анализ использования сервиса микроблогов Twitter пользователями без труда определяет уровень их занятости, пишет Блог Imena.UA (http://www.imena.ua/blog/twitter-workers/).

Индикаторами уровня пользовательской занятости исследователи называют время публикации записей в сети микроблогов, их частоту, а также, содержание. Трудоустроенные люди чаще упоминают работу, публикуют записи, в основном, по утрам, и делают больше опечаток.

В свою очередь, безработные пользователи пишут медленнее, соответственно, грамотнее и реже поминают какую-то трудовую деятельность.

Кроме того, последние заметно интересуются отвлечёнными темами, вплоть до светских слухов, и пишут в Twitter равномерно на протяжении всего дня, особенно активизируясь по вечерам.

По словам исследователей, подтверждения данным закономерностям им удалось отыскать пока что только на территории Испании. Учитывая культурологические особенности, данные могут оказаться неприменимы для оценки ситуации в других странах.

Тем не менее, открытие позволит властям существенно снизить затраты на аналитику. Анализ записей в Twitter может оказаться беспрецедентно оперативным методом отслеживания динамики уровня безработицы в Испании ***(Записи в Twitter позволяют отслеживать уровень безработицы // Блог Imena.UA (http://www.imena.ua/blog/twitter-workers/). – 2014. – 25.11).***

Маніпулятивні технології

Рунет: репрессии и манипуляции

«Интернет возник как спецпроект ЦРУ». Эта фраза вызывает улыбку, хотя и звучит немного тревожно сейчас, когда паранойя выходит на международный уровень, а откровения Э. Сноудена надолго подпортили имидж США. Но кто же ее произнес? Нет, вовсе не представитель туманной касты сторонников теории заговора, а никто иной как В. Путин, самый влиятельный человек на планете по мнению Forbes, пишет «The Kiev Times» (http://thekievtimes.ua/society/408369-runet-repressii-i-manipulyacii.html).

Он считает, что Интернет появился как проект ЦРУ (то есть заклятого врага отставного офицера КГБ) и «так и развивается». Согласитесь, это навевает не самые приятные мысли. Правда то или нет, но Google и Facebook уже пустили слишком глубокие корни, чтобы от них можно было избавиться при возникновении малейших подозрений, особенно со стороны В. Путина. Кроме того это заставляет задуматься о том, как российские власти воспринимают и используют Интернет.

Зло повсюду

Россия превратилась в настоящую поборницу свободы и прав человека, приняв у себя Э. Сноудена, и категорически не приемлет ни малейших посягательств на свой суверенитет. А что насчет суверенитета других? Ответом на этот вопрос может послужить нынешнее кровопролитие на востоке Украины…

Суверенитетом не поступаются, а американские веб-сайты находятся под пристальным надзором. Замаскированные агентства ЦРУ еще находятся в зоне терпимости, но их видимость ограничена. У всех сайтов с миллионами пользователей по всему миру есть свой российский аналог. «Яндекс», «Рамблер», «ВКонтакте», LiveJornal – все это ни о чем вам не говорит? Но ведь это настоящие столпы рунета… Относительно закрытое сообщество, которое связано со многими другими бывшими странами-сателлитами русским языком и пока еще неохотно говорит по-английски.

Twitter и прочие MySpace – карлики в российском сетевом пространстве и находятся под пристальным надзором спецслужб. А что насчет российских сайтов, они свободны? Нет, они подчиняются воле Кремля. Как бы это не раздражало блогеров, чьи права урезаются законами о безопасности Интернета и его пользователей.

Роскомнадзор обязал всех успешных блогеров (успешность приравнивается как минимум к 3000 посетителей) пройти регистрацию. А если выпущенная информация слишком сильно отдает оппозиционным душком, то вас закроют и, поминай, как звали. В Amnesty International забили тревогу еще в мае этого года. Но призыв к открытой демонстрации против властей воспринимается не лучшим образом, даже как что-то противозаконное. С тех пор паровой каток закона пришел в движение, но оценить нанесенный им ущерб весьма непросто. Ну да, ведь информация теперь… под контролем.

Президент Human Rights Watch Х. Уильямсон был совершенно прав, когда говорил, что «этот закон призван поставить перед блогерами те же

ограничения, что и перед СМИ, не предоставив им такой же защиты и привилегий. Это новый этап в бесконечном подавлении свободы слова в России».

В российском представлении Интернет совершенно определенно представляет собой некий американский объект. Но раз обойтись без него сегодня уже невозможно, им нужно пользоваться по самим установленным правилам. Поэтому в стране принимаются все более ограничительные законы, но российские сайты могут получить широкую свободу для маневра, если докажут свою ненависть к «гринго».

Один из самых раздражающих моментов – это полное отсутствие уважения к интеллектуальной собственности. Интернет превращается в неправовую зону, и вам не нужно быть гениальным хакером, чтобы воспользоваться падающей на вашу голову манной. Тысячи сайтов с разным успехом предлагают скачать или посмотреть программы со всего мира.

Стриминг? Скачивание фильмов и музыки? Да ведь это все делают! Только вот подобные нелегальные вещи стали в России настоящим бизнесом, а пиратские сайты процветают. Таких ресурсов существует бесконечное множество. Причем относится это даже к RuTube и «ВКонтакте».

Последствия тому более чем ощутимы, потому что на 97% стриминговых сайтов (как в России, так и других странах) обитают вредоносные программы. Один неосторожный клик, и подключенный компьютер сольет всю информацию о своем владельце. Хакеры не нарадуются, а постоянных предупреждений оказывается все равно недостаточно для того, чтобы уберечь людей от ловушек сетевых пиратов.

RuTube, то есть российский YouTube, априори вообще доступен лишь для тех, кто хоть что-то смыслит в кириллице. Но он уже прославился как центр для всего видеотрафика и в частности тех видео, которым больше не находится места в сети. На российской платформе весело и радостно чередуется друг с другом как легальный, так и нелегальный контент. Ответный удар начинает набирать обороты.

Российский Facebook, «ВКонтакте» не то что попался с поличным, а даже не пытался скрываться. «ВКонтакте» не просто является эрзацем всемирно известного сайта (та же структура, дизайн и функционал), но и предлагает пользователям бесплатно смотреть любое оказавшее там видео. А их там насчитываются многие тысячи на всех языках.

Достигший отметки в 230 млн пользователей «ВКонтакте» оказался под прицелом американцев, которые не преминули наклеить на него ярлык «пиратский сайт». Директор «ВКонтакте» категорически не согласен с выдвинутыми обвинениями и клятвенно заверяет всех в приверженности защите авторских прав, хотя в то же время подчеркивает, что контролировать весь выложенный пользователями контент было бы просто безумием. Иначе говоря, ничего не видел, ничего не знаю.

Кибервойна

Нежелание считаться с правилами получает отражение и на другом, еще более неприглядном уровне. У российского государства есть своя дорожная карта, и когда какая-либо страна оказывается под прицелом, с грохотом пушек соседствуют сетевые атаки. Те бывшие советские республики, которые, по мнению Москвы, «неправильно» себя повели, знают об этом не понаслышке.

После сноса военного мемориала в Таллинне россияне выразили недовольство широкомасштабными кибератаками на все самые используемые в Эстонии сайты. Волны DDoS-атак буквально парализовали инфраструктуру страны в 2007 г. Это стало своего рода генеральной репетицией перед нападением на Грузию год спустя. Танки начали операции после территориального спора при не такой масштабной, но чрезвычайно эффективной поддержке армии кремлевских хакеров.

Россияне стали экспертами по помехам в сети. Они всегда славились как прекрасные шахматисты, а сегодня превратились в виртуозов клавиатуры. Украинцы вот уже год регулярно испытывают это на собственном опыте, и никто не может сказать, где остановится эта маленькая игра с большими последствиями. Интернет безграничен, что прекрасно сочетается с российскими амбициями. Добро пожаловать на Дикий Восток ***(Рунет: репрессии и манипуляции // «The Kiev Times» (http://thekievtimes.ua/society/408369-runet-repressii-i-manipulyacii.html). – 2014. – 23.11).***

***

На Луганщине СБУ пресекла попытку террористов через соцсети втянуть подростков в диверсионную деятельность. Об этом сообщила пресс-служба УСБУ в Луганской области.

В Луганской области в ходе проведения мероприятий по противодействию проявлениям терроризма и сепаратизма в социально-ориентированных интернет-ресурсах Службой безопасности Украины прекращено функционирование группы террористической направленности в социальной сети «ВКонтакте».

Группа «Сопротивление Северодонецк Лисичанск Рубежное» привлекла внимание сотрудников СБУ, поскольку на ее странице публиковались материалы, содержащие призывы к совершению террористических актов, диверсий, убийства военнослужащих ВС Украины, проведение акций гражданского неповиновения, нацеленных на поддержку террористических организаций «ЛНР» и «ДНР».

«Администрация группы распространяла информацию о методах ведения диверсионной работы, организации партизанской войны, соблюдения требований конспирации и тому подобное. Одновременно целью группы было привлечение лиц для проведения диверсионной и террористической деятельности на территории региона. В конце октября по указанному факту следователи СБУ начали уголовное производство по ч.1

ст. 258-3 Уголовного кодекса Украины (создание террористической группы или террористической организации)», – сообщает пресс-служба.

В ходе установления лиц, причастных к противоправной деятельности, правоохранители вышли на администратора этой группы. Им оказался студент из Северодонецка.

«Парень охотно рассказал, что эту группу он создал в сентябре 2014 г. под влиянием гражданина РФ, с которым познакомился через Интернет. Взрослый человек, действуя из анонимного аккаунта (его IP-адрес, как установили оперативники, зарегистрирована в Санкт-Петербурге), внушал подростковые антиукраинские идеи и побудил его проводить акции по дискредитации органов государственной власти и Вооруженных Сил, надругательства над государственными символами Украины. Под влиянием «незримого координатора» тинейджер распространял эти идеи среди сверстников, которые стали членами группы в соцсети. Конечной целью интернет-сообщества была организация дееспособной диверсионной группы. Впрочем, ее достижению помешали сотрудники СБУ, и этим, кстати, уберегли подростков от совершения тяжких преступлений», – далее рассказали в пресс-службе.

Сотрудники Службы безопасности отмечают, что интернет-пространство сегодня также является сферой военных действий, и целью противника является получение контроля над сознанием молодого поколения украинских. Поэтому оперативники спецслужбы советуют родителям детей и подростков «интересоваться, с кем и о чем они общаются в социальных сетях, чтобы несовершеннолетние не стали орудием в руках злоумышленников» ***(Шаповал В. «ВКонтакте» выявили группу, которая призывала подростков Луганщины к диверсиям и убийствам украинских солдат // IT Expert (http://itexpert.org.ua/rubrikator/item/39697-vkontakte-vyyavili-gruppu-kotoraya-prizyvala-podrostkov-luganshchiny-k-diversiyam-i-ubijstvam-ukrainskikh-soldat.html). – 2014. – 30.11).***

Зарубіжні спецслужби і технології «соціального контролю»

Как сообщает информагентство Associated Press, второй по величине в США провайдер сотовой связи AT&T Mobility больше не будет прикреплять уникальные идентификаторы (так называемые «супер-куки») абонентов мобильной связи к пакетам данных, которые отправляются со смартфонов, поскольку такая практика не позволяет скрыть личность пользователя при работе в Интернете.

«Супер-куки» (буквенно-символьные идентификаторы) передавались каждому веб-сайту, на который заходил пользователь. Это давало прекрасную возможность сторонним лицам, в том числе и рекламодателям, отследить активность абонентов в Интернете.

Что интересно, подобную практику использует и крупнейший в США мобильный оператор Verizon Wireless и отказываться от нее пока не намерен.

По словам представителя компании Д. Льюис, для корпоративных тарифов и государственных служащих такие «маячки» не применяются. В настоящее время нет свидетельств, что подобные идентификаторы используют альтернативные операторы Sprint и T-Mobile.

Коды слежения применяются мобильными компаниями для мониторинга активности абонентов и их девайсов. В то время как сами коды не содержат расширенной личной информации, они являются уникальными и передаются на веб-сайты вместе с персональными данными, такими как имя или номер мобильного телефона, которые пользователь может предоставить добровольно ***(AT&T отключил идентификаторы, позволяющие следить за активностью абонентов в Интернете // InternetUA (http://internetua.com/AT-T-otkluacsil-identifikatori--pozvolyauasxie-sledit-za-aktivnostua-abonentov-v-internete). – 2014. – 18.11).***

***

Исследователи Института информационных технологий в Дели, Индия, обнаружили, что 81 % пользователей анонимной сети Tor могут быть деанонимизированы с помощью инструмента NetFlow от компании Cisco, пишет Блог Imena.UA (http://www.imena.ua/blog/tor-traffic-analysis/).

Как известно, Tor-системы пытаются сохранить такие характеристики, как задержки между пакетами. Можно осуществлять атаки анализа трафика, определяя шаблоны трафика в различных точках сети, и связывая между собой несвязанные сетевые соединения.

Это позволит раскрыть личности большинства пользователей анонимной сети, – считают индийские учёные.

Данный способ анализа трафика базируется на создании и мониторинге изменений пользовательского трафика на стороне сервера и исследовании выходных данных путём статистической корреляции.

В лабораторных условиях учёным удалось достигнуть стопроцентной деанонимизации пользователей Tor, за пределами лаборатории это число составило 81,4 %.

Мониторинг сетей на уровне пакетов в таких масштабах является довольно сложной задачей. Однако, для осуществления атак анализа трафика злоумышленники потенциально могут использовать менее точные, но легкодоступные инструменты, например, NetFlow от Cisco.

Компания Mozilla готовится внедрить технологии, используемые в анонимной сети Tor во встроенную поисковую систему Firefox ***(Индийские учёные нашли способ раскрыть личности более 80 % пользователей Tor // Блог Imena.UA (http://www.imena.ua/blog/tor-traffic-analysis/). – 2014. – 19.11).***

***

Визнання «Правого Сектора» екстремістською організацією в Росії дозволить силовикам блокувати сайти, спільноти та акаунти в соціальних мережах, пише РБК.

Одразу три націоналістичні організації України – «Правий Сектор», «Українська національна асамблея» (УНА-УНСО) та «Тризуб» імені Степана Бандери – за вимогою Генпрокуратури були визнані російським Верховним Судом екстремістськими. Відтепер діяльність цих організацій на території федерації заборонена, а це означає, що правоохоронці можуть вживати всіх необхідних заходів для забезпечення дотримання закону.

За словами експертів, опитаних РБК, рішення суду змусить також кожну згадку про «Правий Сектор» у ЗМІ уточнювати приналежність цієї організації до списку екстремістських. В іншому випадку може повторитись ситуація, яка виникла у березні 2014 р., коли вся редакція Lenta.ru звільнилась в знак протесту проти цензури ***(«Правий Сектор» в Росії заборонили з метою блокування популярних груп у «ВКонтакте» // UkrainianWatcher (http://watcher.com.ua/2014/11/18/pravyy-sektor-v-rosiyi-zaboronyly-z-metoyu-blokuvannya-populyarnyh-hrup-u-vkontakte/). – 2014. – 18.11).***

***

Apple и американское правительство уже давно увлечены «гонкой вооружений» в сфере технологий шифрования и информационной безопасности, особенно в отношении iOS-устройств. Тем не менее, по данным издания Wall Street Journal, Министерство юстиции США активно предпринимает попытки перенести эту риторику в более удобную для себя плоскость.

Так, в ходе официальной встречи, состоявшейся в прошлом месяце, один из представителей ведомства заявил руководителям Apple, что в перспективе компания может стать одной из сторон, несущих криминальную ответственность за инциденты, связанные с похищением и убийством детей.

Вместе с тем, логика рассуждений правоохранителя построена на одних лишь предположениях. По его словам, однажды преступники – возможно похитители детей – воспользуются технологиями шифрования (в iMessage, FaceTime) и устройствами Apple, чтобы избежать обнаружения силовыми структурами. При этом неспособность правоохранительных органов получить доступ к устройству подозреваемых может обернуться убийством заложника.

Представитель Apple, в свою очередь, раскритиковал Министерство юстиции за нарушение права граждан на неприкосновенность частной жизни и подчеркнул, что в описанной чиновником ситуации правоохранители могут сохранить жизнь ребенка, воспользовавшись другими источниками информации о преступниках, в том числе данными из сетей мобильной связи.

Он также отметил, что репутация Apple и без того пострадала из-за раскрывшихся в прошлом году фактов слежки за мирным населением со стороны АНБ США. Среди прочего, общественности стало известно, что разведывательное ведомство тайно получало доступ к iOS-устройствам американцев при помощи бэкдора.

Реакцией производителя на ситуацию стала реализация улучшенных технологий шифрования данных, а также создание веб-страницы с подробным описанием политики Apple в отношении вопросов неприкосновенности частной жизни ***(Технологии шифрования Apple могут стать причиной гибели детей // InternetUA (http://internetua.com/tehnologii-shifrovaniya-Apple-mogut-stat-pricsinoi-gibeli-detei). – 2014. – 21.11).***

***

З 1 січня 2015 р. соціальна мережа Facebook запроваджує нову політику, що дозволяє передавати дані третім особам без спеціального дозволу.

Згідно з повідомленням компанії, ті, хто продовжить користуватися соцмережею та її сервісами після 1 січня, погодяться з нововведеннями за замовчуванням, повідомляє «КоммерсантЪ».

Уточнюється, що Facebook буде ділитися інформацією з рекламними та аналітичними компаніями, операторами зв'язку та іншими постачальниками послуг, а також власниками інтернет-сайтів і додатків для мобільних пристроїв.

Соцмережа також передасть дані користувача держорганам, якщо визнає, що їх запит юридично обґрунтований.

Перелік персональних даних містить активність людей в соцмережі: опубліковані пости, листування з іншими користувачам, дані про місцезнаходження людини, особисті дані при реєстрації самого користувача та осіб, які спілкуються з ним ***(З 1 січня Facebook зможе передавати інформацію про користувачів без їхнього дозволу // LB.ua (http://ukr.lb.ua/news/2014/11/26/287360_1_yanvarya_facebook_smozhet_peredavat.html). – 2014. – 26.11).***

***

Эксперты выявили версию FinFisher, замаскированную под менеджер закладок. Вредоносное приложение удалось обнаружить благодаря инструменту Detekt от международной правозащитной организации Amnesty International.

Как сообщает издание The Register, уже в первую неделю после релиза сканера вредоносных приложений Detekt от правозащитников Amnesty International, инструмент выявил неизвестную ранее модификацию FinFisher. В рамках атаки разработчики вируса замаскировали его под легитимный менеджер закладок.

Напомним, что Detekt был представлен широкой общественности 20 ноября и в настоящее время доступен для пользователей Windows. Программа сканирует компьютер на наличие правительственного шпионского ПО.

Интересно, что анонимный пользователь инструмента загрузил обнаруженную им модификацию FinFisher на Virus Total, что позволило проанализировать вредонос более детально. Как выяснилось, менеджер закладок содержал сертификат Comodo с подписью Jagdeependra, вместо подписи оригинального разработчика Outertech.

Оригинальная версия FinFisher была разработана компанией Gamma Group International. Шпионский инструмент был неоднократно и легально продан правоохранительных органам ряда стран. Среди прочего, FinFisher был куплен полицией Австралии, Бельгии, Сингапура, и Италии ***(Эксперты выявили версию FinFisher, замаскированную под менеджер закладок // InternetUA (http://internetua.com/eksperti-viyavili-versiua-FinFisher--zamaskirovannuua-pod-menedjer-zakladok). – 2014. – 27.11).***

***

Інтернет-користувачі повідомляли про масове блокування соціальних медіа та онлайн-месенджерів 27 листопада у Казахстані. Як повідомляє TJournal.ru, недоступними на території країни виявилися «ВКонтакте», Facebook, Twitter, месенджери WhatsApp та Viber.

Про блокування повідомляли користувачі кількох інтернет-провайдерів. Користувалися вони при цьому проксі-серверами.

Крім цього, про ситуацію написало новинне видання TengriNews. Водночас отримати офіційного коментаря від одного із найбільших провайдерів у Казахстані «Казахтелеком» редакції не вдалося. TJournal.ru не отримав пояснень і від інших компаній: «Білайн Казахстан» та KCell.

Сервіси запрацювали у звичному режимі ближче до півночі.

Один із користувачів розповів, що після розблокування сайтів звернувся до служби підтримки його провайдера 2Day Telecom. Там йому відповіли, що ніякого блокування не відбувалося ***(У Казахстані на декілька годин блокували доступ до популярних соцмереж // MediaSapiens (http://osvita.mediasapiens.ua/web/social/u_kazakhstani_na_dekilka_godin_blokuvali_dostup_do_populyarnikh_sotsmerezh/). – 2014. – 28.11).***

Проблема захисту даних. DDOS та вірусні атаки

Неактивные IP-адреса могут использоваться для рассылки спама и осуществления DDoS-атак

Хакеры используют лазейки в регистре маршрутизации Интернета для захвата адресного пространства и рассылки спама. Как заявляет Б. Кребс, подобные действия могут использоваться, в том числе, для осуществления

DDoS-атак. Аналогичное мнение также высказал исследователь Cisco Д. Шульц.

Эксперты обратили внимание на болгарского интернет-провайдера Mega Spred, который обменивался информацией по протоколу BGP с соседними маршрутизаторами. В результате злоумышленникам удалось анонсировать пространство IP-адресов, принадлежащим ирландскому хостинг-провайдеру.

BGP-анонс был признан легитимным вышестоящим провайдером и анонсирован на другие маршрутизаторы в сети Интернет. Таким образом, Mega Spred стал «владельцем» автономных систем адресов, которые использовал для рассылки спама.

Д. Шульц заявил, что преступники все чаще прибегают к анонсированию BGP-префиксов для неиспользованного адресного пространства IP, «захватывая» адреса в своих собственных целях. Эксперт утверждает, что в дальнейшем они могут использоваться не только для рассылки спама, но и для осуществления DDoS-атак и похищения интернет-трафика у легитимных владельцев сетей.

Для того чтобы остановить подобную преступность, потребуется строгая фильтрация BGP-трафика в сетях. Вышестоящие провайдеры не должны разрешать нижестоящим сетям анонсировать BGP-префиксы для IP-блоков, которые они не контролируют. К сожалению, пока не будут предприняты более строгие меры фильтрации, подобные инциденты будут продолжаться ***(Неактивные IP-адреса могут использоваться для рассылки спама и осуществления DDoS-атак // InternetUA (http://internetua.com/neaktivnie-IP-adresa-mogut-ispolzovatsya-dlya-rassilki-spama-i-osusxestvleniya-DDoS-atak). – 2014. – 17.11).***

***

В Windows обнаружена новая опасная уязвимост

Обновление, исправляющее критическую уязвимость в SChannel, стало вызывать проблемы со стабильностью некоторых процессов в Windows. Об этом сообщает издание ZDNet. По их словам, четыре новых шифра TLS, добавленных в исправлении, могут привести к разрыву всех соединений через TLS 1.2 и зависанию некоторых процессов.

На прошлой неделе Microsoft выпустила бюллетень безопасности MS14-065, исправляющий критическую уязвимость в SChannel – реализации шифрования SSL/TLS в ОС Windows. Специалисты компании утверждали, что брешь в данном компоненте позволяла осуществить удаленное выполнение кода, в связи с чем бюллетень получил статус критического.

Вскоре после установки обновления пользователи столкнулись с серьезными затруднениями. Если TLS 1.2 был включен по умолчанию, и TLS-переговоры завершаются с ошибкой, все соединения через данный протокол разрываются, а процессы и службы, использующие TLS, зависают. В некоторых случаях в журнале системных событий появляется запись

происшествия с идентификатором 36887: «Неисправимая ошибка со стороны удаленной конечной точки. Код ошибки определен протоколом TLS как 40».

Для того чтобы исправить ошибки, возникающие после установки данного обновления, требуется удалить новые шифры для TLS, используя редактор реестра системы ***(В Windows обнаружена новая опасная уязвимость // InternetUA (http://internetua.com/v-Windows-obnarujena-novaya-opasnaya-uyazvimost). – 2014. – 18.11).***

***

Согласно результатам исследования мобильных угроз, проведенного Kaspersky Lab совместно с Интерполом, за период с августа 2013 г. по июль 2014 г. 60 % атак, предотвращенных защитными продуктами компании на Android-устройствах, были нацелены на кражу денег пользователей. Атакам мошенников в большинстве случаев были подвержены пользователи в России и Украине, Испании, Великобритании, Вьетнаме, Малайзии, Германии, Индии и Франции.

По всему миру за исследуемый период более чем 588 тыс. пользователей Android столкнулись с банковскими и SMS-троянцами. Это в 6 раз превышает показатель за предыдущий аналогичный период.

В целом 57 % всех зарегистрированных инцидентов были связаны с семейством SMS-троянцев, которые отправляют короткие платные сообщения на премиум-номера без ведома владельца. Большинство подобных случаев (64,4 %) затронули российских пользователей. Также подобные атаки были отмечены в Казахстане (5,7 %), на Украине (3,3 %), в Испании (3,2 %), Великобритании (2,4 %), Малайзии (2,3 %), Германии (2 %), Индии (1,6 %) и Франции (1,3 %).

При этом в 2 % случаев SMS-троянцы действовали в паре с банковскими зловредами – такой подход позволяет украсть данные банковских карт, а также реквизиты доступа к системам онлайн-банкинга. В рейтинге по числу инцидентов с мобильными банковскими троянцами Украина заняла третью строчку – на ее долю пришлось около 2 % атак. При этом за 12 месяцев число подобных зловредов возросло в 14 раз. Новые версии были получены с помощью незначительных изменений в оригинальном коде, которые могут помешать обнаружению вредоносной программы защитным средством.

«Одно заражение банковским троянцем может предоставить мошенникам доступ ко всем финансовым средствам жертвы, тогда как в случае с SMS-троянцами нужны десятки или даже сотни успешных атак, чтобы получить ощутимую выгоду. Вдобавок к этому далеко не все пользователи прибегают к помощи приложений для мобильного банкинга – именно этим объясняется разница в количестве инцидентов, связанных с этими типами вредоносных программ», – поясняет Р. Унучек, старший антивирусный эксперт Kaspersky Lab.

«В течение нескольких последних лет мы были свидетелями роста числа мобильных угроз, которые становились все сложнее и опаснее – настолько, что теперь уже могут быть нацелены на конкретные компании. В условиях экспоненциально растущего мобильного рынка мы видим, как злоумышленники пытаются освоить новые способы атак с целью получения контроля над персональными устройствами», – отметил М. Оберои, начальник отела киберинноваций и распространения информации ***(60 % мобильных угроз для Android нацелены на кражу денег пользователей // ITnews (http://itnews.com.ua/news/74978-60-mobilnykh-ugroz-dlya-android-natseleny-na-krazhu-deneg-polzovatelej). – 2014. – 17.11).***

***

Хакер, известный в сети Интернет под ником Chainfire, сообщил на своей странице в Google+ о том, что ему удалось получить администраторские привилегии к системным файлам Android 5.0 Lollipop. Он успешно взломал все модели Nexus (4, 5, 7, 9 и 10) и в ближайшее время выпустит инструменты для их рутирования.

Ранее он предупреждал, что Google внесла изменения в схему защиты файлов в Android, и она может воспрепятствовать взлому. К счастью для любителей ставить кастомные прошивки и получать root-доступ, эта схема по-прежнему легко ломается. Скорее всего, смартфоны и планшеты LG, Samsung, HTC, Sony и других производителей защищены ничуть не лучше, чем устройства Nexus ***(Хакеру удалось получить root-доступ на устройствах Nexus с Android Lollipop // InternetUA (http://internetua.com/hakeru-udalos-polucsit-root-dostup-na-ustroistvah-Nexus-c-Android-Lollipop). – 2014. – 18.11).***

***

В августе этого года известные хакеры К. Нол и Я. Лелл из консалтинговой компании SR Labs сообщили о «фундаментальной уязвимости устройств USB». В октябре они опубликовали код программы для взлома компьютера по USB и с тех пор проверили сотни различных устройств разных производителей на наличие бага.

Были проверены все USB-контроллеры от 8 крупнейших мировых производителей: Phison, Alcor, Renesas, ASmedia, Genesys Logic, FTDI, Cypress и Microchip. Результаты проверки неоднозначные. Хорошая новость в том, что около половины устройств не подвержена уязвимости. Плохая новость: вы не можете сказать, какая конкретно половина.

Буквально каждая модель флешки, веб-камеры, концентратора или адаптера для флеш-карт поставляется с разной начинкой, в зависимости от партии. В одной партии может быть уязвимый контроллер, а в другой – уже нет. Модель контроллера не обозначена на упаковке. Узнать её можно только после вскрытия прибора. Приходится использовать устройство вслепую.

О результатах исследования авторы рассказали на конференции по безопасности PacSec, которая прошла на прошлой неделе в Токио (слайды, pdf).

Есть несколько интересных фактов, достойных отдельного упоминания. Например, уязвимости подвержены абсолютно все USB-флешки с контроллерами производства тайваньской фирмы Phison. Все чипы ASmedia, напротив, защищены от бага. У другой тайваньской компании Genesys уязвимы контроллеры USB 3.0, но безопасны контроллеры USB 2.0. В общем ситуация совершенно непредсказуемая.

Программа BadUSB устанавливается в прошивку периферийного устройства и полностью берёт под контроль компьютер при подключении к нему по USB. На компьютере жертвы BadUSB творит что угодно, в том числе видоизменяет файлы, которые устанавливаются в системе, и перенаправляет интернет-трафик на произвольные адреса, изменив DNS-записи. Зловред всегда может выдать себя за клавиатуру и ввести произвольные команды.

Установленная на компьютере программа может изменить прошивку по USB, а та, в свою очередь, может установить зловреда в системе. Из-за такого двустороннего взаимодействия ни одному устройству и компьютеру больше нельзя доверять. Вы не только должны ограничить свой ПК от посторонней периферии, но и сами не можете безопасно вставить чистую флэшку в посторонний ПК.

Поскольку код находится в прошивке, его довольно трудно обнаружить и удалить. Самая действенная защита – вообще запретить подключение к компьютеру новых USB-устройств: флешек, мышек, клавиатур, смартфонов и других приборов. А в будущем производители обязаны будут чётко указывать, какие конкретно микросхемы установлены в их устройствах. Как вариант, можно использовать криптографическую проверку обновлений прошивки ***(В каких USB-контроллерах есть фатальная уязвимость BadUSB // InternetUA (http://internetua.com/v-kakih-USB-kontrollerah-est-fatalnaya-uyazvimost-BadUSB). – 2014. – 18.11).***

***

Вредоносный выходной узел Tor, расположенный на территории РФ, может быть связан с создателями бэкдора MiniDuke. Согласно данным ИБ-экспертов из F-Secure, используемый вирус не является версией MiniDuke. Наоборот, он представляет собой новое вредоносное ПО, в связи с чем и получил название OnionDuke.

Когда пользователь пытается скачать программу через вредоносный выходной узел Tor, то вместо желаемого продукта на компьютер устанавливается «адаптер». Последний устанавливает и оригинальную программу, и вредоносную. Как уверяют специалисты, используя отдельный «адаптер» вирусописатели могут обойти любую проверку целостности, которая может быть встроена в ПО.

Помимо записи всех файлов оригинального исполняемого модуля, OnionDuke также запускает инсталляцию вредоносной части скачанного файла. После этого вирус пытается связаться с подконтрольными злоумышленникам URL-адресами. Несмотря на то, что ресурсы выглядят подлинными, они скомпрометированы. В случае успешного соединения с URL-адресами вирус скачивает дополнительные вредоносные компоненты на инфицированный компьютер.

Осуществив данную атаку, вирусописатели могут похитить важную информацию, в том числе учетные данные, сведения об ОС/ПО и пр.

По словам ИБ-экспертов, о том, что вредоносная кампания связана с MiniDuke, свидетельствует попытка вируса связаться с доменом, зарегистрированным в 2011 г. владельцем ресурсов, задействованных в атаках с MiniDuke ***(Замечен новый вирус от создателей вредоноса MiniDuke // InternetUA (http://internetua.com/zamecsen-novii-virus-ot-sozdatelei-vredonosa-MiniDuke). – 2014. – 18.11).***

***

Специалисты ESET раскрыли детали масштабной киберкампании хакерской группы Sednit. Не менее 10 лет злоумышленники атакуют защищенные корпоративные сети правительственных учреждений Восточной Европы.

Ранее группа осуществляла распространение вредоносных программ путем компрометации легитимных сайтов, принадлежащих финансовым учреждениям Восточной Европы. Для этого злоумышленники использовали набор эксплойтов для удаленной установки вредоносного ПО.

Недавно специалисты ESET выяснили, что хакеры осуществляют также атаки закрытых сетей с применением вредоносного ПО, которое распространяется через USB-накопители. Программа позволяет получать файлы и другие конфиденциальные данные с компьютеров, изолированных от Интернета. Антивирусные продукты ESET NOD32 детектируют ее как Win32/USBStealer.

Для кражи данных с компьютера жертвы Win32/USBStealer использует многоступенчатый подход:

– Злоумышленники удаленно устанавливают Win32/USBStealer на компьютер человека, имеющего доступ к закрытой сети (компьютер A). При этом исполняемый файл маскируется под легитимное российское ПО USB Disk Security. Вредоносная программа отслеживает подключение USB-накопителя и мгновенно выполняет заражение.

– Пользователь подключает инфицированный USB-накопитель к изолированному компьютеру защищенной сети (компьютер B). После заражения вредоносная программа получает список файлов для передачи злоумышленникам.

– USB-накопитель возвращается в компьютер B со списком доступных файлов.

– Пользователь снова подключает USB-накопитель к компьютеру B, и вредоносная программа копирует на него нужные файлы.

– При новом подключении накопителя к компьютеру A Win32/USBStealer отправит на удаленный сервер скопированные файлы ***(Хакеры группы Sednit крадут данные с изолированных от Интернета компьютеров // InternetUA (http://internetua.com/hakeri-gruppi-Sednit-kradut-dannie-s-izolirovannih-ot-interneta-kompuaterov). – 2014. – 19.11).***

***

Німецькі спецслужби констатують, що в країні стають частішими кібератаки на ресурси уряду ФРН із закордону.

Як пише dw.de, найбільшу загрозу для Берліна становлять хакери, що діють із Китаю та Росії. Про це 18 листопада заявив голова Федерального відомства із охорони конституції Х.-Г. Масен.

Він пояснив, що останнім часом почастішали напади іноземних спецслужб на мережеві ресурси німецьких підприємств та ІТ-інфраструктуру уряду. За словами чиновника, щодня відбувається близько 3 тис. хакерських атак. При цьому більшість із них не спричиняють суттєвої шкоди. Проблемними є приблизно 5 мережевих проникнень щодня. Їх здійснюють спецслужби, зокрема Росії та Китаю.

Німецьке спеціалізоване відомство з безпеки у сфері інформаційної техніки зіштовхується із труднощами у виявленні іноземних кібератак. Х.-Г. Масен зауважив, що особливо добре підготовані атаки на урядові структури Німеччини відбуваються переважно перед великими міжнародними подіями, як-от зустріч G20 ***(Німецький уряд все частіше піддається кібератакам // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/nimetskiy_uryad_vse_chastishe_piddaetsya_kiberatakam/). – 2014. – 19.11).***

***

Во вторник, 18 ноября, Microsoft выпустила бюллетень безопасности MS14-068, который должен был появиться неделей ранее. Бюллетень MS14-068, обозначенный как критический, исправляет обнаруженную в частном порядке брешь в контроллере домена Kerberos KDC.

Уязвимость позволяет злоумышленнику выполнять произвольный код на любом устройстве домена с правами администратора. Для того чтобы иметь возможность эксплуатировать эту брешь, злоумышленнику необходимо пройти аутентификацию с использованием подлинных доменных учетных записей. Уязвимый компонент доступен только удаленным пользователям, обладающим стандартными учетными записями с идентификационными данными для всего домена.

Данное обновление безопасности исправляет уязвимости в поддерживаемых версиях Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 и Windows Server 2012 R2.

Также апдейт предназначен для обеспечения безопасности всех поддерживаемых версий Windows Vista, Windows 7, Windows 8 и Windows 8.1 по принципу глубоко эшелонированной защиты.

Обновление исправляет уязвимость путем изменения процесса подтверждения подписи в Windows-версиях Kerberos ***(Microsoft устранила брешь в Kerberos DC // InternetUA (http://internetua.com/Microsoft-ustranila-bresh-v-Kerberos-DC). – 2014. – 19.11).***

***

Команда российских исследователей безопасности SCADA StrangeLove обнаружила уязвимости в миллионах SIM-карт абонентов сотовой связи по всему миру и отдельные бреши в распространенных модемных платформах 4G, сообщает портал The Register. В совокупности эти уязвимости позволяют злоумышленникам отправлять созданные SMS-сообщения с целью получения доступа к критическим системам и установки вредоносного ПО на подключенные компьютеры.

«Уязвимости в современных SIM-картах позволяют преступникам заполучить важную информацию, которой достаточно для того, чтобы сымитировать личность жертвы, клонировать телефон в сети или расшифровать трафик посредством двух специально созданных SMS-сообщений», – отметил один из исследователей С. Гордейчик.

Также злоумышленники могут осуществить масштабную DoS-атаку посредством ввода неверных PIN- и PUK-кодов в таргетируемые SIM-карты.

Специалистам SCADA StrangeLove удалось получить удаленный доступ и установить вредоносные приложения на модем 4G, изменить пароли на портале управления маршрутизатором и даже получить доступ к внутренней системе телекоммуникационной компании.

По словам С. Гордейчика, усовершенствованные атаки позволяют злоумышленникам удаленно выполнить перепрограммирование модемов 4G, иногда через SMS-сообщения, заставляя их действовать как устройство ввода-вывода и накопитель для имитации нажатия клавиш, перегрузки подключенного ноубука и установки буткитов.

Данные атаки специалисты SCADA StrangeLove представили на конференциях по безопасности PacSec и ZeroNights ***(Исследователи обнаружили уязвимости в миллионах SIM-карт // InternetUA (http://internetua.com/issledovateli-obnarujili-uyazvimosti-v-millionah-SIM-kart). – 2014. – 20.11).***

***

Аналитики отмечают, что киберпреступники могут сконцентрироваться на предметах «Интернета вещей».

На территории США находится наибольшее количество C&C-серверов. Об этом сообщается в квартальном отчете IBM X-Force. Специалисты

компании также выяснили, что наибольшее количество инфицирований зафиксировано в Литве и странах Восточной Европы.

В отчете также указывается, что предметы «Интернета вещей» оказывают все большее влияние на человечество. Как и в случае с облачными или мобильными технологиями, «Интернет вещей» может упростить и улучшить жизнь человечества, но при этом он может стать желанной целью для киберпреступников.

Что касается актуальных киберугроз, то наибольшее количество вредоносных ссылок в настоящее время рассылается с территории США (~43 %). На втором месте находится Китай (~11 %), сразу после него расположилась Германия (8,3 %). Отметим, что теперь с Поднебесной рассылается почти в два раза больше ссылок – в 2013 г. эксперты X-Force подсчитали, что Китай рассылал 6,2 % всех вредоносных ссылок.

В отчете также указано, что в отдельно взятых странах уменьшается количество инфицированных C&C-серверов. Аналитики предполагают, что хакеры пытаются децентрализовать свою архитектуру и расположить C&C-серверы во все страны мира. Количество атак непрестанно увеличивается – в отчете IBM Cyber Security Intelligence Index указано, что среднестатистическая компания в 2013 г. столкнулась с 91 млн киберугроз, что на 12 % больше показателя 2012 г. ***(Количество вредоносного ПО растет, но C&C-серверов становится все меньше // InternetUA (http://internetua.com/kolicsestvo-vredonosnogo-po-rastet--no-C-C-serverov-stanovitsya-vse-menshe). – 2014. – 19.11).***

***

Согласно проведенному специалистами Kaspersky Lab исследованию киберугроз, обнаруженных в третьем квартале, Украина стала третьей в рейтинге стран, пользователи которых подвергались наибольшему риску онлайн-заражений.

При этом 33 % всех веб-атак, заблокированных продуктами компании, проводились с использованием вредоносных веб-ресурсов, расположенных в США. Украина также вошла в топ-5 стран, жители которых пользователи подвергались наибольшему риску заражения через Интернет (40,70 %).

Среди положительных тенденций можно отметить уменьшение числа атак компьютеров финансовыми зловредами – этот показатель снизился на 25 % по сравнению с предыдущим отчетным периодом. Первое место по количеству таких инцидентов продолжает занимать Бразилия, за ней – Россия и Германия.

Одновременно с уменьшением этого показателя наблюдается повышение интереса к денежным средствам владельцев мобильных устройств. Так, в третьем квартале эксперты Kaspersky Lab обнаружили свыше 7 тыс. новых мобильных банковских троянцев – это приблизительно в 3,5 раза больше, чем в во втором. Растет и количество атакованных стран:

если в прошлом квартале инциденты были зафиксированы в 31 стране, то в этом – в 70.

Что касается атак через уязвимости, 47 % попыток использования «дыр» в безопасности пришлось на эксплойты для браузеров – в первую очередь Internet Explorer, эксплойт для которого присутствует почти в каждом эксплойт-паке. Второе место занимают Java-уязвимости – их доля составила 28 %.

«Атаки компьютеров с помощью богатого арсенала вредоносных программ очень частое явление, однако мы призываем пользователей обратить внимание на относительно новый тренд среди злоумышленников – заражение мобильных устройств банковскими троянцами, темп роста числа которых постоянно увеличивается. Со своей стороны, мы рекомендуем использовать надежное комплексное защитное решение класса Internet Security для всех устройств, которое позволит не идти на компромисс в вопросе безопасности и обеспечит высокий уровень защиты всем девайсам пользователя – как стационарным, так и мобильным», – комментирует В. Чебышев, руководитель группы исследования угроз для мобильных платформ Kaspersky Lab ***(40 % украинских пользователей подвергаются риску заражения через Интернет // ITnews (http://itnews.com.ua/news/75036-40-ukrainskikh-polzovatelej-podvergayutsya-risku-zarazheniya-cherez-internet). – 2014. – 20.11).***

***

BitTorrent Sync не пригоден для обмена конфиденциальными даннями

BitTorrent Sync, сервис для синхронизации и резервного копирования файлов, чрезвычайно популярен среди пользователей Интернета, что объясняется простотой в установке и эксплуатации этого ПО. К тому же, как утверждают разработчики, сервис был создан с учетом требований по безопасности и конфиденциальности. Именно с этой точки зрения участники конференции Hackito Ergo Sum решили исследовать популярное ПО с закрытыми исходными кодами.

В подробном отчете Hackito дано описание поверхности атаки, указаны векторы потенциальных атак, а также упомянуты некоторые внушающие тревогу недоработки в области безопасности и криптозащиты. К числу последних эксперты относят то обстоятельство, что инфрастуктура Sync зависит от других инфрастуктур и ресурсов, надежность которых может вызывать сомнение. Если Amazon станет жертвой хакерской атаки, безопасность всей архитектуры BTsync окажется скомпрометированной, считают аналитики.

Эксперты также удивлены тем, что на сервер GetSync.com в массовом порядке поступают незакодированные хэши. Такая ситуация недопустима, тем более что речь идет об обмене ссылками. Исследователи также считают, что за время существования файлообменника парадигма обмена претерпела изменения и теперь содержит уязвимость, коды которой могли быть

получены компанией BitTorrent Inc и/или разработчиками от следственных органов, руководствующихся так называемыми письмами национальной безопасности (NSL).

Исследователи не исключают утечек сетевых адресов клиентов, а также существования различных уязвимостей у клиентов сервиса. Все изложенное дает экспертам основания не рекомендовать сервис для обмена конфиденциальной информацией ***(BitTorrent Sync не пригоден для обмена конфиденциальными даннями // InternetUA (http://internetua.com/BitTorrent-Sync-ne-prigoden-dlya-obmena-konfidencialnimi-dannimi). – 2014. – 19.11).***

***

На официальных форумах развлекательной игровой платформы Steam появились сообщения о вредоносном файле .SCR, который распространяется через чат. Подписчики сервиса получали уведомления с безобидным на вид файлом изображения. Исследователи из ИБ-компании Malwarebytes проанализировали атаку и обнаружили, что в большинстве случаев киберпреступники распространяли вредоносный файл под видом некоего виртуального объекта, который им якобы требовалось обменять.

По словам специалиста ИБ-компании Panda Security Б. Блэйза, помимо вышеуказанной уловки, преступники также использовали сообщения с простым текстом «посмотри на мою фотографию».

Для того чтобы замаскировать ссылку, указывающую на вредоносный файл, мошенники использовали сервис сокращения URL Bit.ly. Данная ссылка вела на страницу Google Drive, на которой содержался файл .SCR с именем IMG_211102014_17274511.scr.

Как поясняет исследователь, обычно для загрузки файла .SCR необходимо приложение Google Drive Viewer, однако в этом случае к ссылке была добавлена строка «&confirm=no_antivirus», что позволяло загружать его автоматически. Файл похищал учетную запись жертвы и использовал ее для дальнейшего распространения вредоносной ссылки. По словам Б. Блэйза, вредоносный файл не передавал загруженные данные с инфицированного устройства на удаленный сервер.

Для удаления вредоносной программы необходимо осуществить выход из сервиса Steam и удалить процесс, связанный с вредоносным файлом из Диспетчера задач (процесс обычно называется temp.exe, wrrrrrrrrrrr.exe, vv.exe или случайным именем 340943.exe). Далее необходимо просканировать устройство на вирусы и изменить пароль учетной записи в Steam ***(Злоумышленники распространяют вредоносный файл .SCR через Steam Chat // InternetUA (http://internetua.com/zloumishlenniki-rasprostranyauat-vredonosnii-fail--SCR-cserez-Steam-Chat). – 2014. – 19.11).***

***

Хакеры продолжают эксплуатировать уязвимость ShellShock в командной оболочке Bash, позволяющую удаленному пользователю выполнять произвольные команды на целевой системе.

Как сообщает издание Net-Security, эксперт компании Trend Micro Р. Иносенсио предупреждает о появлении новой версии вредоноса Bashlite, первоначально предназначавшегося для осуществления DDoS-атак путем эксплуатации бреши ShellShock. Теперь вредоносное ПО пригодно для выполнения атак на расположенные в одной сети компьютеры и другие устройства, в которых реализована система BusyBox.

BusyBox – это набор UNIX-утилит, представляющий собой один исполняемый файл, который был разработан специально для встраиваемых систем с ограниченными ресурсами, например, роутеров.

Оригинальная версия вредоноса отслеживала такие устройства в сети, но не компрометировала их. Новая версия внедряется в целевое устройство путем брут-форс атаки с применением наиболее распространенных логинов и паролей. Инфицировав устройство, вредоносное ПО загружает и использует два скрипта оболочки и таким образом приобретает полный удаленный контроль над системой BusyBox.

Для решения проблемы достаточно установить обновления, исправляющие ShellShock, либо отключить удаленную оболочку. Эффективной может оказаться полная замена логинов и паролей на всех сетевых устройствах ***(Уязвимость ShellShock позволяет атаковать устройства с BusyBox // InternetUA (http://internetua.com/uyazvimost-ShellShock-pozvolyaet-atakovat-ustroistva-s-BusyBox). – 2014. – 19.11).***

***

Исследователи компании Seculert обнаружили новую версию трояна Matsnu (также известную как Trustezeb), алгоритм генерации доменных имен (domain generation algorithm, DGA) которой использует довольно любопытную технику для обхода средств защиты безопасности.

DGA-алгоритм Matsnu генерирует 24-символьные доменные имена, основанные на комбинации существительных и глаголов (существительное – глагол – существительное – глагол). Используемые слова могут быть введены злоумышленником или взяты из предопределенного списка, содержащего 878 существительных и 444 глагола.

По словам технического директора и сооснователя Seculert А. Раффа, используя данный метод, злоумышленники пытаются обойти фонетические алгоритмы машины, которые отслеживают бессмысленные доменные имена, например, ldfjdiehwslgoeh.com.

DGA-алгоритм является реконфигурабельным, поскольку позволяет киберпреступникам установить количество ежедневно генерируемых доменных имен и время, через которое ранее сгенерированное доменное имя может быть использовано повторно.

После инфицирования машины, троян соединяется с C&C-сервером посредством отправки HTTP-запроса. По команде C&C-сервера вредонос собирает информацию о системе, в том числе имени пользователя, имени компьютера в сети, версии операционной системы, о центральном и графическом процессорах, виртуальных машинах, а также языках, драйверах и установленных средствах защиты безопасности.

Кроме того, по инструкции C&C-сервера троян может выполнять различные действия. Например, самоудалиться, самомодифицироваться, обновить предопределенный список доменных имен или загрузить файлы. Как пояснили специалисты Seculert, коммуникации между инфицированным компьютером и командным сервером обфусцированы, а все пересылаемые данные сжаты и зашифрованы.

По словам экспертов, Matsnu использует новый алгоритм с июня 2014 г. Наибольшее количество инфицирований этим трояном было зафиксировано в Германии (89 %). Немного меньше – в Австрии и Польше ***(Новая версия трояна Matsnu использует реконфигурируемый алгоритм генерации доменных имен // InternetUA (http://internetua.com/novaya-versiya-troyana-Matsnu-ispolzuet-rekonfiguriruemii-algoritm-generacii-domennih-imen). – 2014. – 20.11).***

***

Исследователи Trend Micro обнаружили киберпреступную кампанию, в рамках которой злоумышленники использовали рекламные сети и набор эксплоитов Flashpack для распространения разнообразного вредоносного ПО, включая Zeus, Dofoil и Cryptowall. Как сообщают специалисты компании в блоге фирмы, Flashpack использует бесплатные рекламные объявления для распространения вредоносов. Эксперты проследили за несколькими ссылками, используемыми набором эксплоитов, и установили, что в большинстве случаев по ним переходили пользователи из Северной Америки.

Одним из вредоносов, распространяемых киберпреступниками, оказался троян TROJ_DOFOIL, очень часто заражавший ПК пользователей в октябре этого года. По данным Trend Micro, 41 % всех заражений этим вирусом произошли в азиатско-тихоокеанском регионе, еще 27 % – в Северной Америке и 17 % – в регионе EMEA (Европа, Ближний Восток и Африка).

Когда пользователь заходит на веб-сайт, на котором размещена вредоносная реклама, через серию редиректов он попадает на ресурс, использующий набор эксплоитов Flashpack. С его помощью на устройство жертвы загружается троян Dofoil.

Вместе с этим было обнаружено, что через SWF-файлы, эксплуатирующие уязвимость в Flash Player, на компьютеры пострадавших загружается вымогательское ПО CryptoWall. Adobe исправила брешь еще в апреле этого года.

В Trend Micro объяснили, что распространение киберугроз наподобие Dofoil и CryptoWall с помощью вредоносной рекламы представляет серьезную угрозу для бесплатных приложений со встроенной рекламой ***(Набор эксплоитов Flashpack использует рекламные сети для распространения вредоносного ПО // InternetUA (http://internetua.com/nabor-eksploitov-Flashpack-ispolzuet-reklamnie-seti-dlya-rasprostraneniya-vredonosnogo-po). – 2014. – 20.11).***

***

Служба Безопасности Украины фиксирует очередную волну хакерских атак на компьютеры государственных органов власти Украины. Об этом на своей странице в Facebook написал советник главы СБУ М. Лубкивский.

«Преступники пытаются сломать информационные сети и почтовые серверы государственных учреждений. Под видом официальных писем направляются электронные сообщения с вложенным в него вредоносным программным обеспечением, которое рекомендуется установить», – написал советник.

По его словам, участились случаи так называемых fishing, то есть рассылки фейковых писем с вредоносными вложениями.

В СБУ призвали руководителей госучреждений, а также сотрудников IT усилить меры безопасности, проверять достоверность подозрительных писем и материалов, поступающих на электронную почту ***(СБУ фиксирует волну хакерских атак на сервера госорганов Украины // InternetUA (http://internetua.com/sbu-fiksiruet-volnu-hakerskih-atak-na-servera-gosorganov-ukraini). – 2014. – 21.11).***

***

Эксперты компании «Доктор Веб» предупредили о новом трояне для Linux-систем Linux.BackDoor.Fgt.1, который используется для осуществления DDoS-атак. Вредоносное ПО способно отправлять злоумышленникам IP- и MAC-адрес инфицированного устройства, а также осуществлять атаки на заданные узлы с применением техники DNS-усиления, UDP-флуда, а также путем переполнения пакетами SYN.

После запуска на зараженной системе троян проверяет подключение к Интернету, обращаясь к одному из серверов Google. После успешного соединения вредонос определяет IP- и MAC-адрес инфицированного устройства, пытается связаться с C&C-сервером и передает на него данные о версии вредоносного ПО. Примечательно, что адрес этого сервера встроен в тело самого трояна. После этого вредонос ожидает дальнейших команд. Получив от сервера команду PING, он отправляет в ответ PONG и продолжает свою активность. Завершается работа трояна после получения команды DUP.

Благодаря специальной функции, за один цикл, запущенный злоумышленниками, вредоносное ПО осуществляет сканирование 256

удаленных случайных IP-адресов. При этом адреса, использующиеся для адресации внутри локальных сетей, игнорируются.

Эксперты отмечают, что на подконтрольном злоумышленникам сервере хранится множество исполняемых файлов трояна, скомпилированных для разных версий и дистрибутивов Linux, в том числе для встраиваемых систем с архитектурой MIPS и SPARC-серверов. Это значит, что Linux.BackDoor.Fgt.1 способен заражать не только подключенные к Интернету серверы и рабочие станции на базе Linux, но и такие устройства, как маршрутизаторы ***(Эксперты обнаружили новый троян для Linux-систем // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/11/21/linux-trn.html). – 2014. – 21.11).***

***

Kaspersky Lab обнаружила, что вредоносная платформа Regin оказалась первым зловредом, способным проникать в сотовые сети стандарта GSM и вести слежку за пользователями мобильной связи.

Эта платформа использовалась в кибератаках по меньшей мере в 13 странах. В зоне риска оказались телекоммуникационные операторы, правительства, финансовые учреждения, исследовательские организации, а также лица, занимающиеся сложными математическими и криптографическими исследованиями.

Первые следы активности Regin были замечены экспертами Kaspersky Lab еще весной 2012 г. На протяжении последних трех лет образцы этого вредоносного ПО периодически встречались, но не имели прямой связи между собой. Вместе с тем специалисты Kaspersky Lab получили в свое распоряжение ряд образцов Regin в ходе расследования кибератак на правительственные учреждения и телекоммуникационные компании – и именно это позволило получить достаточно данных для глубокого исследования вредоносной платформы.

Анализ зловреда показал, что платформа Regin включает в себя множество вредоносных инструментов и модулей, способных полностью заражать сети организаций и удаленно контролировать их на всех возможных уровнях. При этом для контроля скомпрометированных корпоративных сетей злоумышленники используют довольно нетривиальный способ.

Изучив процесс передачи данных из зараженных организаций в пределах одной страны, эксперты Kaspersky Lab установили, что лишь в одной из скомпрометированных сетей была установлена связь с сервером атакующих, расположенным в другой стране. В то же время все зараженные сети в одном государстве могли коммуницировать друг с другом, обмениваясь информацией. Таким образом, преступники аккумулировали все нужные им данные на серверах лишь одной жертвы. Именно эта техническая особенность платформы Regin и позволяла киберпреступникам действовать незаметно столь долгое время.

Однако наиболее интересной функцией вредоносной платформы Regin является реализованная в ней возможность атаковать GSM-сети. Согласно информации, полученной экспертами Kaspersky Lab из контроллера базовой станции GSM, злоумышленники способны извлекать регистрационные данные для контроля GSM-ячеек в рамках сотовой сети телекоммуникационного оператора. Таким образом, они могут узнавать, какие звонки обрабатываются в конкретной ячейке сети, имеют возможность перенаправлять звонки в другие ячейки или активировать соседние, а также осуществлять другие вредоносные действия. В настоящее время функции контроля GSM-сетей не присутствуют ни в одном другом известном вредоносном ПО.

«Способность проникать в GSM-сети, пожалуй, самый необычный и интересный аспект во всей вредоносной активности Regin. В современном мире мы слишком зависимы от мобильной связи, однако для ее реализации сегодня используются устаревшие коммуникационные протоколы, которые не способны в достаточной мере обеспечить безопасность конечного пользователя. С другой стороны, все GSM-сети имеют механизмы, которые позволяют правоохранительным органам отслеживать подозрительные инциденты, и именно эта техническая возможность дает шанс злоумышленникам проникать в сеть и осуществлять вредоносные действия», – рассказывает К. Райю, руководитель центра глобальных исследований и анализа угроз Kaspersky Lab ***(Kaspersky Lab выявила угрозу GSM-сетям // ITnews (http://itnews.com.ua/news/75095-kaspersky-lab-vyyavila-ugrozu-gsm-setyam). – 2014. – 24.11).***

***

Издание The New Yok Times, ссылаясь на данные компании Lookout, сообщает, что с января 2013 г. около 4,5 млн американских Android-пользователей установили на свои смартфоны приложения, заражённые достаточно опасным вирусом NotCompatible. Lookout уверяет, что вирус NotCompatible установил новый уровень сложности среди всех мобильных вредоносных программ. Для заражения смартфонов хакеры использовали самые различные методы, например, рассылку спама с предложением установить антивирус или советами по похудению. Lookout сообщает, что злоумышленники заражали с помощью спама более 20 тыс. устройств в день.

Специалистам не удалось установить, что именно делает вирус NotCompatible. Он не выполняет никаких действий относительно аппарата пользователя или его данных. Считается, что хакеры задались целью заразить как можно больше мобильных устройств, чтобы создать таким образом сеть, которую можно было впоследствии использовать в различных незаконных целях.

Хакеры арендовали несколько ботнетов для людей, которые использовали их на различных сайтах или целевых аккаунтах в WordPress,

чтобы взломать их. Пользователи заражённых смартфонов замечали увеличенное потребление батареи, но при этом не видели причины этого.

Lookout сообщила, что заражённые вирусом NotCompatible устройства способны «общаться» с другими инфицированными устройствами. Также хакеры нашли способ организовать зашифрованную связь между своим командным центром и заражёнными смартфонами, что усложняет их определение. Компания Lookout уверяет, что её антивирус способен определить и заблокировать NotCompatible, когда тот попробует попасть на ваш смартфон.

Google также подтвердила, что некоторые Android-устройства заражены вредоносными программами, но их число невероятно мало в сравнении с количеством активных пользователей.

Мы же напомним, что установка приложений только из официального магазина приложений значительно уменьшает шанс «подхватить» какой-либо вирус ***(4,5 миллиона Android-смартфонов заражены вирусом NotCompatible // InternetUA (http://internetua.com/4-5-milliona-Android-smartfonov-zarajeni-virusom-NotCompatible). – 2014. – 25.11).***

***

По данным специалистов ИБ-компании Black Lotus, в 2015 г. Вьетнам, Индия и Индонезия станут основными источниками DDoS-атак благодаря увеличению количества взломов мобильных телефонов. Согласно квартальному отчету, охватывающему период с 1 июля по 29 сентября 2014 г., по угрозе безопасности Вьетнам занимает пятую позицию после Китая, США, России и Германии.

Как отмечают специалисты, в то время как Вьетнам, Индия и Индонезия не обладают широкой полосой пропускания, необходимой для осуществления масштабных DDoS-атак, наличие большого количества скомпрометированных устройств, в частности смартфонов, делает эти страны отличными площадками для создания новых ботнетов.

Сооснователь Black Lotus Ш. Мэрк прогнозирует, что в следующем году число DDoS-атак уменьшится. При этом крупным корпорациям они не нанесут масштабного ущерба, но могут причинить немало беспокойства небольшим предприятиям.

Эксперты компании проанализировали атаки, совершенные в период с 1 июля по 29 сентября текущего года и выяснили, что по сравнению с 2013 г. их мощность снизилась на 96 %. Также уменьшилось и количество инцидентов с 462 621 в первом квартале этого года до 201 721 в третьем ***(В следующем году значительное количество DDoS-атак будут осуществляться из Азии // InternetUA (http://internetua.com/v-sleduuasxem-godu-znacsitelnoe-kolicsestvo-DDoS-atak-budut-osusxestvlyatsya-iz-azii). – 2014. – 25.11).***

***

Неизвестные хакеры взломали выложенное в Play Маркете приложение Back up & restore, предназначенное для резервного копирования и восстановления данных на устройствах Sony. Его издателем стал некий Н. Канудо, а в описании указано, что оно захвачено группой HeArT HaCkEr. Ситуацию осложняет тот факт, что оно было предустановлено на некоторые устройства Sony, а значит является системным и обычными средствами его удалить невозможно. Отозвать предоставленные ему разрешения тоже нельзя.

Каким образом хакеры завладели этим приложением, пока непонятно. Возможно, был скомпрометирован аккаунт Sony в Play Маркете. Вероятно, скоро компания обратится в Google и либо уберет это приложение, либо заменит его на настоящее. До этого момента владельцам устройств Sony рекомендуется не запускать это приложение, а по возможности – удалить его (например, с использованием root-прав и Titanium Backup).

За последнее время это уже второй случай, когда пользователи устройств Sony подвергаются опасности. В конце октября был взломан сервис MyXperia, и некоторым операторам пришлось заблокировать IP-адреса, на которые утекали украденные пользовательские данные ***(Хакеры завладели фирменным приложением Sony в Play Маркете // InternetUA (http://internetua.com/hakeri-zavladeli-firmennim-prilojeniem-Sony-v-Play-markete). – 2014. – 25.11).***

***

Новый тип MitM-атаки под названием DoubleDirect «обучен» перенаправлять мобильный трафик с таких крупных ресурсов, как Google, Facebook и Twitter, на устройство, подконтрольное злоумышленнику. Заполучив контроль над трафиком жертвы, преступник может без проблем узнать регистрационные данные пользователя на различных сайтах, а также отправлять вредоносное программное обеспечение на конкретное мобильное устройство.

Новый вид угрозы был обнаружен специалистами из компании Zimperium, которая занимается вопросами безопасности. DoubleDirect использует протокол ICMP, необходимый для передачи сообщений об ошибках и других ситуациях, возникших при передаче данных. Представители компании Zimperium сообщили, что мобильные устройства на базе iOS (включая версию 8.1.1) и Android (Lollipop тоже подходит) и OS X (включая Yosemite) подвержены MitM-атаке, тогда как владельцев настольных систем Windows и Linux эти проблемы не затрагивают ***(Злоумышленники перенаправляют мобильный трафик с Google, Facebook и Twitter // InternetUA (http://internetua.com/zloumishlenniki-perenapravlyauat-mobilnii-trafik-s-Google--Facebook-i-Twitter). – 2014. – 25.11).***

***

Аналитики компании «Доктор Веб» исследовали новый троян, инфицирующий смартфоны и планшеты на базе операционной системы Android. Вредонос похищает персональные сведения владельцев устройств, а также денежные средства с банковских счетов и со счетов мобильных телефонов жертв.

Троян распространяется под видом системного обновления различных популярных программ. После установки фальшивого ПО, вредоносная программа размещает свой ярлык на экране мобильного устройства. При этом он может соседствовать с ярлыком легитимного приложения, если оно уже инсталлировано. Таким образом, жертва по ошибке может запустить подложную программу вместо настоящего ПО. Стоит отметить, что в функционале вредоносной программы предусмотрена автоматическая загрузка при каждом включении операционной системы, и даже если владелец мобильного устройства не активирует вредоносное приложение, запуск трояна все равно произойдет.

После запуска вредонос запрашивает у пользователя доступ к функциям администратора мобильного устройства, что в некоторой мере позволяет трояну усложнить его удаление.

По существу, вредонос способен использовать два варианта атаки. Первый сценарий используется в случае, если пользователь запускает одно из интересующих преступников приложений. Тогда троян отображает поверх интерфейса программы фишинговое диалоговое окно с полями для ввода персональной информации (логин, пароль, номер мобильного телефона, данные кредитной карты). Все добытые таким образом сведения передаются на удаленный сервер злоумышленников.

Второй сценарий атаки не зависит от действий пользователя. В этом случае вредонос получает указания от злоумышленников, поступающие с C&C-сервера. К примеру, троян может выполнять USSD-запрос, перехватывать и отправлять SMS-сообщения, передавать на сервер мошенников данные об установленных приложениях и т. д. ***(Android-троян похищает финансы и конфиденциальные данные владельцев мобильных устройств // InternetUA (http://internetua.com/Android-troyan-pohisxaet-finansi-i-konfidencialnie-dannie-vladelcev-mobilnih-ustroistv). – 2014. – 27.11).***

***

В новом докладе ирландской консалтинговой компании Experian указано, что один из шести владельцев смартфонов по всему миру, уже стал жертвой киберпреступников. Эксперты отмечают, что ситуация может ухудшиться, поскольку уровень защиты мобильных устройств слишком слабый, чтобы противостоять хакерским атакам. Так, около 60 % смартфонов и 50 % планшетов в мире нуждаются в дополнительных сервисах безопасности.

Стремительный рост спроса на мобильный банкинг, а также использование мобильных телефонов для совершения транзакций,

провоцирует интерес киберпреступников к этим устройствам и представляет огромные риски как для обычных пользователей, так и для предпринимателей.

На сегодняшний день в мире насчитывается около 5 млрд устройств, подключенных к сети Интернет. Они обслуживают 1 млрд банковских счетов онлайн, а также стимулируют глобальный рынок электронной коммерции размером 13 трлн дол.

В докладе указано, что хакеры могут ограничиться фишинговыми сообщениями для того, чтобы получить платежные реквизиты жертвы. Также киберпреступники могут контролировать и перехватывать веб-страницы, которые посещает пользователь, просматривая данные, которые пользователь вводит в соответствующие поля при совершении покупки.

Результаты отчета продемонстрировали, что владельцы смартфонов мало осведомлены о рисках, связанных с киберпреступностью. Главной целью мошенников по-прежнему остаются Android-устройства ***(60 % смартфонов в мире подвержены хакерским атакам // InternetUA (http://internetua.com/60--smartfonov-v-mire-podverjeni-hakerskim-atakam). – 2014. – 26.11).***

***

Как пишет британская The Guardian, электронные сигареты могут приносить пользу курильщикам, однако несут потенциальную угрозу их компьютерам. Обзор этой статьи приводит портал InoPressa.

В статье сообщается, что большинство электронных сигарет заряжается от USB-разъема персонального компьютера или ноутбука. В случае подключения к этому разъему дешевая электронная сигарета, произведенная неизвестно кем и как, получает доступ к электронному устройству. Таким образом, на компьютер может попасть вредоносное ПО.

В качестве подтверждения этого тезиса издание приводит историю, опубликованную пользователем популярного портала Reddit под ником Jrockilla.

По его словам, компьютер одного топ-менеджера некоей крупной компании был заражен вредоносным ПО, источник которого долгое время не удавалось установить. Однако в итоге оказалось, что в зарядное устройство электронной сигареты, сделанной в Китае, было жестко запрограммировано вредоносное ПО. Когда сигарета подключалась к USB-порту компьютера, вирус «звонил домой» и заражал систему.

Консультант по безопасности из компании Trend Micro Р. Фергюсон назвал этот случай вполне правдоподобным. «Вредоносное ПО с “конвейера” существует уже несколько лет: оно заражает фоторамки, MP3-плееры и т. д.», – отметил он.

По мнению Р. Фергюсона, предприятиям стоит отключать USB-порты либо принять меры, чтобы сотрудники пользовались только санкционированными устройствами. А рядовым пользователям следует

установить и обновить антивирусы и не связываться с устройствами сомнительного происхождения.

Отметим, что в конце июля специалисты в области компьютерной безопасности из немецкой компании SR Labs сообщили об обнаружении опасной уязвимости в стандартной USB-прошивке. Сообщалось, что экспертам удалось внедрить в нее скрытый от любых защитных программ вредоносный код, который позволяет получать доступ к файлам, хранящимся на жестком диске, перехватывать пароли, перенаправлять интернет-трафик и шпионить за пользователями. Также это ПО могло заражать другие USB-устройства, подключенные к компьютеру ***(Электронная сигарета может заразить компьютер опасным вирусом // InternetUA (http://internetua.com/elektronnaya-sigareta-mojet-zarazit-kompuater-opasnim-virusom). – 2014. – 26.11).***

***

Сирийская электронная армия (СЭА) атаковала сайты ведущих мировых СМИ, пишет The Guardian.

В частности, от действий хакеров также пострадали сайты британских газет Independent и Daily Telegraph, американской The New York Times, а также Evening Standard, The Chicago Tribune, The Guardian и La Repubblica.

Кроме того, пострадали сайты телекомпаний CNBC и CBC, журналов OK! и Forbe, Национальной хоккейной лиги, компаний Dell, Microsoft и Ferrari и международной организации ЮНИСЕФ. Сведения о взломанных сайтах продолжают поступать.

Взломанные сайты либо не открывались, либо на них выскакивало окно с информацией о том, что акция проведена СЭА.

Предположительно хакеры использовали уязвимость в сетях доставки и дистрибуции контента (CDN), чтобы получить доступ к сайтам. В газете Independent заявили, что взлом был осуществлен через сеть Gigya CDN, в результате часть читателей перенаправляли на сайт хакеров или показывали им сообщения используя запись DNS. В Daily Telegraph заявили, что к части сайта газеты был получен доступ третьей стороной, но информация о пользователях не была скомпрометирована.

Бывший агент ФБР, а ныне управляющий директор по борьбе с киберпреступностью компании Kroll Э. Хилберт заявил CNBC, что атака СЭА является пиар-ходом, призванным продемонстрировать ее возможности. Он подтвердил, что в основном речь шла о перенаправлении трафика на сайт, созданный хакерами, где они демонстрировали свою символику.

Сирийская электронная армия, как считается, состоит из сторонников Президента Сирии Б. Асада. Она неоднократно атаковала западные СМИ после начала гражданской войны в этой стране в 2011 г. На их счету также взломы аккаунтов в Twitter и Skype. Как правило действия хакеров из этой группировки носят пропагандистский характер и не наносят существенного ущерба ***(Сирийские хакеры сегодня атаковали сайты ведущих мировых***

СМИ, а также ряда компаний // InternetUA (http://internetua.com/siriiskie-hakeri-segodnya-atakovali-saiti-vedusxih-mirovih-smi--a-takje-ryada-kompanii). – 2014. – 27.11).

***

Представители автомобильной индустрии объединяют усилия для противодействия кибеугрозам.

Компьютерные системы автомобилей могут стать новым вектором кибератак. Понимая это, производители средств передвижения принимают меры по усилению киберзащиты транспортных средств от посягательств злоумышленников и террористов.

Выпускаемые сегодня автомобили подсоединены к Интернету и обеспечены сотовой связью, а это означает, что они уязвимы к хакерским атакам. Известные случаи удаленного управления автомобилем пока ограничиваются уровнем эксперимента. Однако автопроизводители объединяют усилия с тем, чтобы сделать электронные системы более защищенными.

Автомобильные концерны, в том числе Honda и Toyota, планируют создать структуру, одной из задач которой должно стать противодействие хакерским атакам, направленным на электронные системы автомобилей. Кроме того, участники проекта получат возможность обмениваться информацией, что позволит им своевременно вносить необходимые изменения в системы безопасности выпускаемых транспортных средств ***(Электронные системы автомобилей уязвимы к хакерским атакам // InternetUA (http://internetua.com/elektronnie-sistemi-avtomobilei-uyazvimi-k-hakerskim-atakam). – 2014. – 27.11).***

***

Группировка APT3, осуществившая серию глобальных атак нулевого дня, сейчас эксплуатирует не так давно исправленные уязвимости в Windows.

Компьютерные системы, на которых еще не установлено исправленное обновление опасной уязвимости, присутствовавшей во всех версиях Windows на протяжении последних 19-лет, могут быть подвержены точечным фишинговым атакам, предупреждают исследователи ИБ-компании FireEye.

По данным специалистов FireEye, талантливая хакерская группировка APT3, осуществившая серию глобальных атак нулевого дня, известную как Clandestine Fox, сейчас эксплуатирует не так давно исправленные уязвимости в Windows.

Злоумышленники осуществляли рассылку фишинговых электронных писем, нацеленных на две уязвимости (CVE-2014-6332 и CVE-2014-4113), обнаруженных в октябре и ноябре текущего года.

Первая уязвимость присутствовала во всех версиях Windows (начиная с Windows 95) и позволяла злоумышленнику удаленно получить контроль над целевой системой.

По словам экспертов, эксплуатация исправленной бреши является новым витком в деятельности группы, которая раньше была хорошо известна своими атаками, использующими уязвимости нулевого дня. В ходе своей последней кампании, известной как Operation Double Tap, злоумышленники рассылали жертвам фальшивые предложения от Playboy, содержавшие код эксплоита Metasploit. В случае успешного совершения атаки преступники удаленно получали контроль над ПК жертвы ***(Хакеры эксплуатируют исправленную уязвимость 19-летней давности // InternetUA (http://internetua.com/hakeri-ekspluatiruuat-ispravlennuua-uyazvimost-19-letnei-davnosti). – 2014. – 27.11).***

***

Украина оказалась на седьмом месте в списке мировых распространителей спама, сообщает корреспондент proIT.

Такие данные были представлены в отчете KasperskyLab. Анализ спама в третьем квартале 2014 г. показал, что на первом месте в рейтинге распространителей спама оказались США, откуда по всему миру было разослано почти 14 % вирусного контента. На втором месте находится Россия – ее доля составляет 6,1 %, на третьем Вьетнам, а Украина находится на седьмом месте с показателем в 3,41 %

В целом же в третьем квартале доля спама в почтовом траффике составила 66,9 %, что на 1,7 пункта меньше, чем в предыдущем. При этом количество фишинговых атак возросло на 19 %.

Сообщается также, что традиционно спамеры эксплуатировали громкие мировые события: к примеру, выход iPhone6 послужил причиной увеличения количества спама абсолютно разной направленности, как мошеннической, так и рекламной. События в Украине и лихорадка Эбола фигурировали в «нигерийских» письмах. Неудивительно, что на протяжении третьего квартала именно ситуация в Украине активно использовалась для обмана пользователей. В качестве авторов таких спам-сообщений мошенники указывали не только украинцев различных профессий, но также политиков и предпринимателей, предлагающих получателям денежные вознаграждения за помощь в переводе или инвестировании имеющихся у них крупных сумм денег ***(Украина оказалась на 7 месте в списке распространителей вирусного контента // proIT (http://proit.com.ua/news/internet/2014/11/28/143203.html). – 2014. – 28.11).***

***

Как защититься от кликджекинга?

Вы не можете их увидеть, их появление и поведение непредсказуемо, и они жадно охотятся за вашими кликами. Кликджекинг появился примерно в 2008 г., но о нем стали много говорить в последнее время из-за новой волны кликджекинговых атак на пользователей Facebook.

Что такое кликджекинг?

Это слово для кого-то может звучать как название нового модного танца стиля андеграунд, но это далеко не так. Кликджекинг происходит, когда интернет-мошенник размещает невидимую кнопку или другой элемент пользовательского интерфейса поверх другой, выглядящей совершенно невинно, кнопки на веб-странице или другого элемента интерфейса, используя прозрачный слой (который вы не можете видеть). Очень часто кликджекеры загружают доверенные сайты во фрейм и затем накладывают поверх невидимые кнопки.

Безопасная веб-страница может, например, содержать кнопку с надписью «Кликните здесь, чтобы посмотреть видео с очень милым и очаровательным пушистым котенком». Но скрытая поверх нее невидимая кнопка является ссылкой на что-то, на что бы вы никогда не кликнули, зная о ее действительном содержимом. Возможными действиями в результате кликджекинга могут быть:

– изменение настроек конфиденциальности вашего аккаунта на Facebook;

– добавление лайков кому-то или чему-то, неизвестному для вас (этот вид мошенничества еще называется «лайкджекинг»);

– добавление себя в подписчики (follower) кого-то, неизвестного вам, в Twitter;

– предоставление мошенникам доступа к вашему компьютеру (например, к микрофону или камере).

Как же уберечься от мошенничества?

Это довольно просто:

1. Обновите свой интернет-браузер и подключаемые плагины.

Пользуетесь ли вы Firefox, IE, Chrome или другими браузерами, вы всегда должны иметь самую последнюю их версию, которая имеет не только защиту от кликджекинга, но и другие улучшенные функции безопасности. Эта рекомендация касается также и подключаемых к браузеру плагинов, таких как Flash, устаревшие версии которых уязвимы для кликджекинговых атак.

2. Установите приложения для обнаружения и предотвращения кликджекинга.

Некоторые браузеры имеют встроенную защиту от кликджекинга, которая, к сожалению, обладает ограниченными возможностями. Однако существует ряд надежных приложений, предназначенных для обнаружения и защиты от кликджекинга. Их можно подключать к браузеру в качестве плагина. Некоторые из них даже бесплатны. Вот парочка наиболее распространенных и проверенных:

– NoScript – бесплатный противокликджекинговый плагин для Firefox;

– Comitari Web Protection Suite – Home LE (Limited Edition) – бесплатная версия приложения Comitari Web Protection Suite с ограниченным числом функций. Home LE включает защиту от кликджекинга.

Защита от кликджекинга – забота не только самих пользователей. Разработчики веб-сайтов и приложений также должны принимать превентивные меры. Для них существуют эффективные рекомендации по написанию кода, помогающего обнаружить и предотвратить кликджекинг ***(Как защититься от кликджекинга? // InternetUA (http://internetua.com/kak-zasxititsya-ot-klikdjekinga). – 2014. – 29.11).***

***

Хакеры из AnonGhostTeam атакуют пользователей, посещающих скомпрометированные веб-сайты.

Исследователи безопасности предупреждают о возникновении новой вредоносной кампании интернет-активистов, в рамках которой используются инструменты для удаленного выполнения кода на атакуемых системах. Инцидент выделяется на фоне аналогичных акций тем, что участники протеста зашли дальше привычной и менее опасной «порчи веб-сайтов».

Речь идет о кампании, организованной коллективом AnonGhostTeam, участники которого ранее уже атаковали государственные порталы и веб-сайты различных СМИ, сообщает исследователь К. Маннон в своем блоге. По его словам, ранее активисты проводили исключительно дефейс атакуемых ресурсов.

Тем не менее, с недавних пор AnonGhostTeam стала размещать на главных страницах скомпрометированных веб-сайтов ссылку на страницу lulz.htm с кодом JavaScript, который, в конечном счете, переадресовывает пользователя на сайт, содержащий набор эксплоитов Dokta Chef Exploit Kit (EK).

«Вероятно, это новая тактика группы – атаковать пользователей, посещающих скомпрометированные ресурсы», – предполагает К. Маннон.

Эксперт также отметил, что целью хакеров являются пользователи 32-разрядных операционных систем Windows с веб-обозревателем Internet Explorer ***(Хактивисты начали использовать инструменты для удаленного выполнения кода // InternetUA (http://internetua.com/haktivisti-nacsali-ispolzovat-instrumenti-dlya-udalennogo-vipolneniya-koda). – 2014. – 30.11).***

***

Нещодавно, для того щоб зберегти комп’ютер від вірусів достатньо було відімкнути його від мережі. Але досить скоро навіть такий захист буде не надійним, адже фахівцям вдалось розробити прототип вірусу, який зможе передаватись через динаміки та мікрофон.

Комп’ютерні фахівці М. Гаспач і М. Гетц встановили, що приховану акустичну мережу можна використовувати як передавач вірусу за допомогою пам’яті комп’ютерів. Дані досягають іншого комп’ютера, який під’єднаний до першого за допомогою зовнішньої мережі. Результатом випробування стали результати : данні передаються на відстань до 20 метрів на частоті 20 кГц зі швидкістю до 20 біт / с.

Дослідники заспокоюють користувачів, адже сьогодні ще рано боятись шкідливих програм, які матимуть змогу розповсюджуватись акустичним способом, але у найближчому майбутньому захистити свій комп'ютер буде набагато важче ніж на сьогоднішній день ***(Новий вірус вразить ваш комп'ютер за допомогою мікрофону або навушників // PINU (http://pinu.com.ua/novyny/it/30-11-14/noviy-virus-vrazit-vash-kompyuter-za-dopomogoyu-mikrofonu-abo-navushnikiv). – 2014. – 30.11).***