СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(15–28.12)

2014 № 24

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(15–28.12)
№ 24

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

Популярность Facebook среди подростков в США продолжила снижаться второй год подряд. Об этом пишет агентство Bloomberg со ссылкой на исследование компании Frank N. Magid Associates.

По данным исследования, около 88 % американских пользователей соцсетей в возрасте от 13 до 17 лет пользовались Facebook в 2014 г. Для сравнения – в прошлом году этот показатель составлял 94 %, в 2012 г. – 95 %.

Тинейджеры постепенно теряют интерес к Facebook, однако начинают обращать внимание на другие соцсети. Так, за последний год доля юных пользователей соцсетей, которые заходят в Twitter, возросла с 46 до 48 %.

Исследование за прошлый год серьезно обеспокоило инвесторов Facebook, причем топ-менеджеры соцсети сами признали, что подростки уже не столь активны в Facebook. Более взрослая пользовательская база Facebook создает больше возможностей для монетизации в краткосрочной перспективе, но если соцсетью перестанут интересоваться нынешние подростки, то в следующие 5–10 лет у инвесторов может возникнуть еще больше поводов для беспокойства.

Ряд других приложений Facebook также отличается более взрослой аудиторией. Около 55 % пользователей Facebook Messenger младше 37 лет, тогда как у мессенджеров Snapchat и Kik доля такой аудитории – 86 и 83 % соответственно.

Среди причин, по которым тинейджеры покидают Facebook, называется их восприятие безопасности соцсети. По данным опроса, только 9 % подростков назвали Facebook безопасной и внушающей доверие. Кроме того, молодежь оказалась недовольна и развлекательной функцией Facebook – веселой ее назвали лишь 18 % подростков по сравнению с 40 % у Pinterest и Instagram.

В то же время у Facebook есть скрытые резервы – по данным ряда исследований, популярность принадлежащих компании сервисов WhatsApp и Instagram среди подростков только растет ***(Популярность Facebook среди подростков снова упала в 2014 году // InternetUA (http://internetua.com/populyarnost-Facebook-sredi-podrostkov-snova-upala-v-2014-godu). – 2014. – 21.12).***

***

Социальная сеть Facebook объявила об обновлении функционала раздела «Популярное» (Trending), включая его доступность на мобильных устройствах и новые разделы для разных типов контента.

Разделы сделают контент Trending более структурированным. Ранее он представлял собой нагромождение новостей с разной степенью релевантности пользователю. Теперь популярные темы рассортированы по

следующим разделам: Articles, In the Story, Friends and Groups, Near the Scene и Live Feed.

В разделе Articles будут представлены новостные заметки на популярную тему от различных изданий.

In the Story покажет посты от людей, которые являются участниками конкретной истории.

Friends and Groups покажет, что об этой теме говорят друзья пользователя и участники групп, в которых он состоит. Это сделает популярные темы более релевантными пользователю на личностном уровне.

Near the Scene будет отображать посты людей, которые стоят у истоков обсуждаемых событий, предоставляя дополнительный слой географической релевантности.

Live Feed покажет ленту сообщений в режиме реального времени от людей во всём мире, подобно Twitter.

Под новыми разделами в «Популярном» останется лента, которая была ранее. Она отображает посты в Facebook, релевантные пользователю, ранжированные по вовлечённости, своевременности и другим факторам.

Что касается алгоритма определения популярных тем – он остался прежним.

Новый функционал будет доступен только для пользователей в США – в десктопной версии Facebook и в мобильном приложении для Android.

В будущем компания планирует запустить «Популярное» для пользователей в других странах и в приложении для iOS ***(Facebook обновил функционал раздела «Популярное» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_obnovil_funktsional_razdela_populyarnoe). – 2014. – 15.12).***

***

Популярная сеть для размещения фотографий и коротких видеороликов Instagram запустила пять новых фильтров для редактирования контента. Об этом «Ленте.ру» сообщили представители Instagram.

«Оригинальный набор фильтров Instagram был призван компенсировать низкое качество картинки, предоставляя человеку больше контроля над ощущениями от фотографии. Новые фильтры – менее броские и уловимые – используют более высокое качество снимков, но в то же время предоставляют простой способ запечатлеть настроение, тон и ощущения конкретного момента жизни», – говорят в Instagram.

Новые фильтры получили название Slumber, Crema, Ludwig, Aden и Perpetua. С их учетом пользователю доступен в Instagram набор из 25 фильтров с возможностью контролировать степень их применения.

Кроме того, Instagram также объявил о запуске трех новых функций: возможности публиковать видео в замедленном режиме (slo-mo), публикации комментариев в режиме реального времени без необходимости обновлять

ленту и функции корректировки перспективы кадра. Наконец, пользователь теперь может менять порядок фильтров в списке.

Глобальная аудитория Instagram насчитывает 300 млн пользователей в месяц ***(Фотосервис Instagram запустил пять новых фильтров // InternetUA (http://internetua.com/fotoservis-Instagram-zapustil-pyat-novih-filtrov). – 2014. – 16.12).***

***

Некоторые пользователи приложения Facebook для платформы Android заметили изменения при работе с программой. Крупнейшая социальная сеть, похоже, тестирует обновлённую версию пользовательского интерфейса, которая отличается более плоским внешним видом, обилием цветовых блоков и круговыми пиктограммами.

Вряд ли эти изменения можно назвать полноценным дизайном в соответствии с вещественными интерфейсом Google, представленным вместе с платформой Android 5.0 Lollipop. Однако Facebook явно желает, чтобы её основное мобильное приложение больше соответствовало общему стилю последней мобильной платформы Google.

Как обычно, изменения компания провела на стороне сервера. Другими словами, нет никакой специальной версии APK с обновлённым интерфейсом. Это, похоже, зависит просто от удачи – некоторые пользователи случайным образом получают изменения, а большинство – нет. Возможно, участники бета-тестирования имеют больше шансов получить возможность ознакомиться с обновлением ***(Facebook тестирует новый интерфейс для своего Android-приложения // InternetUA (http://internetua.com/Facebook-testiruet-novii-interfeis-dlya-svoego-Android-prilojeniya). – 2014. – 20.12).***

***

Компания Facebook представила дополнение к своему мобильному сервису для обмена сообщениями Messenger, которое позволяет накладывать значки-стикеры на фотографии перед их отправкой. Об этом говорится в блоге Facebook.

Значки-стикеры, с помощью которых пользователь может быстро описать свою эмоциональную реакцию, впервые появились на Facebook летом прошлого года. Пользователь может скачать различные тематические коллекции стикеров, помимо стандартного набора. В настоящее время они доступны в личных сообщениях, в приложении Messenger и в комментариях к записям на Facebook.

Однако чтобы воспользоваться наложением стикеров на фото, придется скачать отдельное бесплатное приложение Stickered. Программа доступна в магазине Google Play для Android-устройств, в ближайшее время ожидается выход iOS-версии.

По словам разработчиков, эта функция специально запускается в предпраздничный период, когда пользователи обмениваются большим

числом сообщений и фотографий. Среди других новогодних нововведений в Facebook Messenger ожидается специальная рамка для оформления фото, праздничные наборы стикеров и т. д.

В то же время Facebook внесла улучшения в работу самого мессенджера. Разработчики сообщили, что все версии Facebook Messenger теперь работают быстрее, а также в них появились анимированные оповещения о том, что сообщение отправляется, отправлено, доставлено или прочитано. В групповых чатах перемещение иконок с фотографиями участников беседы между этими стадиями позволит проследить, до кого дошло то или иное сообщение.

Аудитория Facebook Messenger насчитывает свыше 500 млн пользователей – ранее в этом году Facebook полностью перенесла в это приложение обмен сообщениями на мобильных устройствах ***(Facebook Messenger позволит накладывать стикеры на фотографи // InternetUA (http://internetua.com/Facebook-Messenger-pozvolit-nakladivat-stikeri-na-fotografii). – 2014. – 20.12).***

***

Facebook расширил возможности своих поисковых служб, чтобы облегчить пользователям ориентацию в огромном массиве данных, размещаемых в социальной сети. Теперь они могут найти в ленте нужный им пост, статью, фото или видео, когда-либо опубликованные их друзьями

В 2013 г. Facebook запустил бета-версию своего первого – семантического – поиска Graph Search. При запросах в Graph Search отображаются уникальные результаты, основанные на связях пользователей с людьми, местами и предметами, с учетом прав доступа к тем или иным материалам на Facebook. Порядок результатов поиска зависит от списка друзей, интересов и других связей пользователя.

По словам вице-президента Facebook по поисковым технологиям Т. Стоки, Facebook получил много отзывов о применении Graph Search. Основными пожеланиями пользователей были возможность использования поисковой опции в мобильном приложении Facebook, а также запуск поиска по постам. Сеть пошла им навстречу и внедрила новую поисковую службу.

Новая опция «позволит вам быстро найти видео вашего выпускного, статью, которые вы наметили для прочтения или фото с прошлогодней свадьбы ваших друзей», объясняет Т. Стоки. До запуска сеть тестировала новый сервис в течение девяти месяцев.

По данным Business Insider, результаты поиска по постам можно упорядочить по дате публикации, связи поста с другими постами, а также связям пользователя с другими пользователями.

Сами выводимые результаты отображаются не в хронологическом порядке, пишет Cnet.com. Чтобы найти нужный пост, необходимо промотать ленту вниз. Ввод имени автора публикации рядом с поисковым запросом

сузит результаты поиска. Чем короче поисковой запрос, тем больше шансов найти релевантный результат.

Первыми в результатах выводятся публикации друзей пользователя, после них – посты друзей друзей. Новая опция позволяет также искать информацию по публикациям людей, на новости которых пользователь подписан.

У поиска Facebook по публикациям нет временных ограничений, он позволяет найти посты, размещенные еще в 2006 г., примерно тогда сеть запустила новостные ленты пользователей.

Запуск нового сервиса потребовал огромной подготовительной работы. По словам генерального директора ресурса М. Цукерберга, компании пришлось проиндексировать информацию, которая по объему превосходит индексную базу данных любой поисковой системы. В январе 2014 г. М. Цукерберг говорил, что это более триллиона пользовательских статусов, неструктурированных публикаций, фото, а также иные данные, которые пользователи публиковали за 10 лет существования сети.

Искать по записям в Facebook умеет российский поисковик «Яндекс», соответствующая опция появилась в начале 2014 г. и доступна на сервисе «поиск по блогам». В «яндексовском» поиске по блогам на долю запросов по записям в Facebook приходится около 15 %, сказал РБК представитель поисковика. В основном же поиске «Яндекса» запросы, которые подразумевают поиск конкретной информации в Facebook, относительно редки ***(В Facebook появилась возможность поиска данных по постам // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_facebook_poyavilas_vozmozhnost_poiska_dannyh_po_postam). – 2014. – 19.12).***

***

Компания Facebook добавила в своё мобильное приложение функцию улучшения фотографий, создаваемых тут же, на мобильных устройствах.

Теперь все фотографии, отправленные в Facebook посредством мобильного приложения, будут проходить процедуру улучшения. Коррекции подвергнутся слишком светлые или затемнённые участки и общая чёткость снимков.

Функция улучшения фотографий активируется по умолчанию. После того как пользователь выберет фотографию, которую он хочет отправить в социальную сеть, на снимке появятся две кнопки.

В правом нижнем углу размещена кнопка кадрирования изображения, а в левом нижнем – кнопка улучшения. При необходимости, через специальный ползунок можно отрегулировать уровень вмешательства.

В настоящее время новая функция реализована лишь в приложении Facebook для iOS. Обновление версии приложения для Android произойдёт позже ***(Facebook будет автоматически улучшать фотографии***

пользователей на смартфоне // Блог Imena.UA (http://www.imena.ua/blog/facebook-better-photo/). – 2014. – 19.12).

***

По данным comScore (международный веб-ресурс статистики; учитывает данные измерений из 172 стран), в ноябре нынешнего года у сайта «Одноклассников» было больше посетителей, чем у «ВКонтакте». В эти данные не включены посещения с мобильных устройств – с учетом пользователей смартфонов и гаджетов «ВКонтакте» по-прежнему впереди, говорят эксперты (http://mmr.ua/news/id/comscore-odnoklassniki-obognali-vkontakte-42669/).

По информации comScore, в ноябре количество уникальных пользователей веб-версии сайта «Одноклассников» составило 61,1 млн, у «ВКонтакте» – 57,6 млн.

«За последние несколько месяцев команда проекта сделала много существенных доработок в области функциональности, дизайна и интерфейса. Что и послужило хорошим подспорьем для роста аудитории, – заявил “Известиям” директор по маркетингу и развитию бизнеса соцсети “Одноклассники” А. Исрапилов. – Сейчас мобильное направление для нас приоритетное, мы прилагаем большие усилия для улучшения приложений. Думаю, что рост и в этой области не заставит себя долго ждать».

«ВКонтакте» не согласились с результатами статистики.

«С тех пор как comScore поменял методику подсчета аудитории, их измерения стали настолько неточными, что мы перестали использовать их внутри компании, – говорит представитель “ВКонтакте” Г. Лобушкин. – Другие независимые метрики однозначно отдают лидерство “ВКонтакте”: LiveInternet, TNS, Alexa, Gemius, SimilarWeb и пр.».

Согласно статистике LiveInternet, в ноябре количество уникальных пользователей «ВКонтакте» (суммарно – с обычных компьютеров и с мобильных устройств) составило 65,3 млн человек, у «Одноклассников» – 44,9 млн. По мнению основателя LiveInternet Г. Клименко, в comScore оперируют «недостоверными данными».

«Данные comScore учитывают посетителей в возрасте 6+ с компьютеров. Сравнивать их со статистикой LiveInternet некорректно, – заявил представитель comScore С. Онищенко. – Мы определяем и удаляем из измерений “нечеловеческий трафик” (“боты” и т. п.). Существуют также другие особенности методологи».

По мнению гендиректора агентства «Социальные сети» Д. Терехова, пользователи «ВКонтакте» могут всё активнее использовать для входа в эту соцсеть мобильные устройства. А аудитория «Одноклассников» заходит на этот сайт более традиционным способом – с помощью компьютеров.

До 2008 г. социальная сеть «Одноклассники» была самой популярной в России. Но новое руководство компании во главе с Н. Шерманом активно занялось монетизацией различных сервисов. В частности, регистрация

нового пользователя в «Одноклассниках» стала платной. Тогда компания объяснила это возросшим количеством аккаунтов, распространяющих спам. После этого приток новых пользователей в соцсеть сильно уменьшился. Осенью 2008 г. «ВКонтакте» по посещаемости опередила «Одноклассников» – и с тех пор сохраняла первенство. Н. Шерман от комментариев по теме статьи отказался ***(Comscore: «Одноклассники» обогнали «ВКонтакте» // Marketing Media Review (http://mmr.ua/news/id/comscore-odnoklassniki-obognali-vkontakte-42669/). – 2014. – 23.12).***

***

Сервис микроблогов Twitter намерен заключить партнерское соглашение с Foursquare. Сотрудничество позволит Twitter значительно обогатить геолокационные функции и возможности сервиса.

Новые геолокационные функции будут запущены сервисом микроблогов уже в I квартале 2015 г.

Официально о заключении соглашения Twitter и Foursquare могут объявить уже в начале наступающего года. Одновременно сервис микроблогов активно развивает собственное подразделение геолокационных технологий, открывая новые вакансии.

После того как данные Foursquare интегрируют в Twitter, пользователи сервиса смогут добавлять в свои твиты географические метки, а системы аналитики сервиса смогут определять географические точки, из которых был написан каждый твит. Это положительно отразится на возможностях геотаргетинга и расширит возможности как для пользователей, так и для рекламодателей и создателей продвигающего контента. Предполагается, что владельцы Twitter-аккаунтов смогут оставлять твиты-чекины; рекламодатели – запускать рекламу для отдельных городов и районов; а создатели контента – публиковать твиты, содержащие информацию, актуальную для текущего местоположения пользователя.

Результаты экспериментов, проведённых командой аналитиков Twitter, показали: пользователи, которым транслировали контент с геолокационными метками и учётом местонахождения человека, чаще обращались к сервиу и его приложениям в течение последующего месяца. Те же, кому показывались твиты без географических меток, реже обращались к Twitter.

«Наша главная цель – получить эти знания и масштабировать их до уровня всего мира. Существует два ключевых компонента, которые следует учитывать. Первый заключается в том, чтобы понять, откуда поступает контент, и где происходит обсуждение темы: в какой-либо стране, городе или же где-то совсем рядом. Второй момент предполагает понимание того, информация о каких географических точках больше всего интересует пользователей. Важно понимать, в какой стране проживает каждый отдельно взятый владелец аккаунта, и информацию о каких географических точках он отслеживает активнее всего. Создание реалтайм-обсуждений событий, происходящих в конкретных географических точках, предоставит нам

неограниченные возможности», – комментирует планы сервиса микроблогов представитель пресс-службы Twitter.

Напомним, что в начале лета этого года представители Foursquare объявили о том, что функционал сервиса полностью пересмотрен. В частности, для пользователей исчезла возможность оставлять чекины – функциональность была перенесена в отдельное приложение Swarm. Запуск обновлённого сервиса откроет перед пользователями все возможности «персонализированного поиска географических объектов и заведений». Именно с этой целью изначально и разрабатывался Foursquare.

В августе 2014 г. геосервис рекомендаций ввел временные подсказки. Функция подходит для освещения особых событий в любимых местах: распродаж, выставок и т. д. Когда пользователь начинает печатать подсказку в Foursquare, в нижнем левом углу появляются часы со словом Forever. Нажимая на часы, можно выбрать период актуальности совета в виде определенной даты или временного отрезка.

Несколько дней назад Foursquare выпустил обновлённое мобильное приложение для iPad. По словам разработчиков, этот выпуск приурочен к праздничному сезону. По их мнению, этот период связан с активными путешествиями и поездками. Новое приложение призвано помочь пользователям планшетов iPad находить интересные места, заведения и достопримечательности в зависимости от своего местоположения.

Однако разработчики сервиса не желают останавливаться только на разработке пользовательских приложений и их монетизации. Геолокационный сервис стремится к тому, чтобы стать крупным поставщиком данных для сторонних клиентов. В частности, для Twitter ***(Twitter расширит геолокационные возможности, благодаря партнёрству с Foursquare // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_rasshirit_geolokatsionnye_vozmozhnosti_blagodarya_partnyorstvu_s_foursquare). – 2014. – 23.12).***

***

22 декабря аналитик инвестиционного банка SunTrust Robinson Humphrey Р. Пек предсказал уход Д. Костоло из Twitter в 2015 г. По словам эксперта, есть «множество интересных кандидатов», способных возглавить социальную сеть.

По словам З. Керравалы, основателя и главного аналитика ZK Research, к Д. Костоло есть много вопросов касательно его способности руководить Twitter. «Если компания не проделает хорошую работу или разочарует ближайшими квартальными результатами, инвесторы будут настаивать на его отставке», – отметил эксперт.

В настоящее время Twitter находится в состоянии замедляющегося роста. Согласно данным финотчета компании, в III квартале ежемесячная активная аудитория интернет-сервиса подскочила на 4,8 % относительно

прошлогодней, составив 284 млн пользователей. Во второй четверти этот показатель динамики роста числа подписчиков измерялся 6,3 %.

Давление на акции Twitter усилилось после того, как фотохостинг Instagram объявил о росте ежемесячной аудитории на 50 %, до 300 млн человек, что превышает размер базы активных пользователей Twitter.

Непростые для Twitter времена привели к уходу нескольких топ-менеджеров в 2014 г. Среди них был глава по разработке продуктов Д. Граф, которого в ноябре понизили в должности, а спустя месяц отправили в отставку.

П. Мурхед, основатель, президент и старший аналитик компании Moor Insights & Strategy, говорит, что по сравнению с Facebook ситуация в Twitter гораздо хуже, и руководство компании уже чувствует серьезное давление со стороны акционеров и своих сотрудников.

З. Керравала считает уход Д. Костоло благоприятным шагом для Twitter. П. Мурхед сомневается, что смена руководства поможет компании.

«Думаю, что Д. Костоло следует поработать год под пристальным наблюдением совета директоров. Компания слишком молода и только недавно стала публичной», – добавил сотрудник Moor Insights & Strategy ***(Глава Twitter в 2015 году может уйти в от ставку // InternetUA (http://internetua.com/glava-Twitter-v-2015-godu-mojet-uiti-v-otstavku). – 2014. – 24.12).***

***

Крупнейшая социальная сеть Facebook запускает собственную версию видеоплейлистов, созданных по типу аналогичного функционала в YouTube. Об этом сообщает searchengines.ru

Журналисты издания заметили новый функционал на странице канала ABC News. В ответ на вопрос о запуске, компания подтвердила изданию, что в настоящее время она тестирует новый дизайн вкладки «Видео» на избранных публичных страницах – телеканала ABC News и издания The New York Times.

По словам представителей Facebook, в ближайшие недели доступ к обновлённому видеоразделу получат все администраторы бизнес-страниц. Новый функционал позволит им выбрать определённый ролик (Featured Video) для его показа на странице в увеличенном формате с лентой комментариев в режиме реального времени.

Ниже выбранного видео будет расположен плейлист, включающий другие ролики, доступные пользователям для онлайн-просмотра. Нововведение сделает раздел «Видео» в Facebook похожим на каналы в YouTube.

Напомним, что ранее в этом месяце Facebook и ABC News запустили новый видеофункционал под названием Facecast – одноминутные новостные ролики, транслирующиеся на странице канала в социальной сети ***(Facebook запускает плейлисты по типу YouTube на публичных страницах // Media***

бізнес (http://www.mediabusiness.com.ua/content/view/41894/118/lang,ru/). – 2014. – 25.12).

***

Социальная сеть «ВКонтакте» поделилась с AIN.UA актуальной статистикой по украинскому сегменту. В своем масштабном исследовании компания подытожила количество и активность десктопных, а также мобильных пользователей, гендерное и возрастное распределение и популярность различных категорий сайта (http://ain.ua/2014/12/26/556768).

За летние месяцы среднесуточное количество пользователей «ВКонтакте» в Украине, по данным Liveinternet, немного упало, однако к октябрю почти сравнялось с предыдущим пиковым периодом, который пришелся на июнь. А 13 ноября соцсеть установила новый рекорд – за сутки на сайт зашло 12,1 млн пользователей из Украины.

Украинская аудитория «ВКонтакте» постепенно подрастает, возрастной сегмент 12–17 лет – самый маленький. На сайте превалируют пользователи постарше. Самые большие возрастные категории: 18–24 г. и 35–44 г.

По охвату аулитории в Украине «ВКонтакте» уступает только Google, постепенно увеличивая разрыв с Mail.ru. В ноябре, по данным ИнАУ, такая тенденция сохраняется – социальная сеть стремительно наращивает охват и среднедневную долю.

Хорошие новости для администраторов сообществ и медиа: самым популярным разделом среди украинских пользователей является именно новостная лента, на которую приходится 47 % всех просмотров страниц. Также популярными остаются фотографии.

В целом, пользователей «ВКонтакте» с платформы Android в несколько раз больше, чем iOS, что немудрено, учитывая распространенность устройств на операционной системе от Google.

За год количество мобильных пользователей заметно возросло. Так, в феврале 2014 г. с Android-устройств на сайт заходило примерно 2,5 млн человек, а в ноябре 2014 г. их количество возросло до 7,26 млн. С iOS-устройств в феврале заходило менее 1 млн пользователей, а теперь их количество возросло почти до 2 млн.

Суточные показатели также растут. Android-пользователи показывают более заметную динамику, в то время как суточная статистика по iOS растет скромнее, а в летние месяцы наблюдался заметный спад активности. Суммарно на сайт, во данным LiveInternet, ежедневно заходит 4,3 млн мобильных пользователей.

Данные по распределению устройств, с которых украинцы заходят на сайт, к сожалению актуальны только по состоянию на август. Тогда все еще превалировали десктопные заходы, однако 30 % пользователей заходят одновременно с двух типов устройств – стационарных и мобильных.

Реклама во «ВКонтакте»

Самой активной аудиторией остается старший возрастной сегмент – 35–44 года, CTR которых достигает 0,042 %. Однако дороже всех рекламодателям обходились пользователи от 18 до 26 лет – средняя стоимость одного перехода (CPC) в ноябре составила более 3,5 грн из-за того, что некоторые рекламодатели завышали ставку. В настоящее время, по данным рекламного отдела «ВКонтакте», CPC составляет 1–2 грн в данном сегменте ***(Яровая М. Украинцы во «ВКонтакте» – масштабное исследование компании // AIN.UA (http://ain.ua/2014/12/26/556768). – 2014. – 26.12).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Народний депутат, радник голови МВС А. Геращенко повідомив, що на заснованому групою волонтерів сайті зібрано понад 7500 профілів у соціальних мережах терористів, сепаратистів і їхніх поплічників.

«Інформація повільно, але напевне акумулювалася на сайті Центру досліджень ознак злочинів проти основ Національної безпеки України, миру, безпеки громадян, заснованого групою волонтерів під керівництвом Георгія Туки. Адреса сайту – http://psb4ukr.org. Сьогодні в базі даних Центру в результаті копіткої праці десятків волонтерів, об'єднаних єдиним поривом любові до України, зібрано більш ніж 7500 профілів терористів, сепаратистів і їхніх поплічників», – написав він на своїй сторінці Facebook.

За його словами, інформацією із сайту центру «Миротворець» уже давно користуються МВС, СБУ, розвідка, прикордонна служба ***(Волонтери зібрали дані про 7500 сепаратистів // LB.ua (http://ukr.lb.ua/news/2014/12/16/289422_volonteri_zibrali_dani_pro_7500.html). – 2014. – 16.12).***

***

У мережі працює сайт Vata.Club, куди анонімно вносяться дані про «ватників». У м. Черкаси сайт видає 439 людей, в основному місцеві сепаратисти «засвітилися» в соцмережах. Розробники сайту обіцяють, що вся цікава інформація буде передаватись у компетентні органи: «Vata.Club – проект створений для збору та фіксації проявів та підтримки сепаратизму та тероризму в мережі з подальшою їх структуризацією. Помітивши в мережі сепаратиста або ватніка, анонімно додайте його в нашу базу, а ми організуємо йому побачення із СБУ» ***(У Черкасах виявили 439 осіб схильних до сепаратизму // Дзвін (http://dzvin.org/u-cherkasah-vyyavyly-439-osib-shylnyh-do-separatyzmu/). – 2014. – 25.12).***

***

У Twitter з’явився користувач, який заздалегідь повідомляє про підготовку поліцейських рейдів у Туреччині проти опонентів влади, зокрема проти опозиційних медійників. Його прогнози підтверджувалися. До цього привертає увагу кореспондент Spiegel online Х. Казім. Витяги з цього мікроблогу, зазначає видання, потрапляють у заголовки турецької преси.

Зазначений анонім приховується під псевдонімом Ф. Авні. Нещодавно він знову поставив у скрутне становище президента Р. Ердогана, спонукаючи його до роз’яснень після повідомлення у Twitter про жорсткі масові акції охоронців порядку стосовно критиків режиму.

У твіттах повідомляється, що Р. Ердоган, міністр внутрішніх справ Е. Ала, міністр юстиції Б. Боздаг і начальник Національного розвідувального управління (МІТ) Х. Фідан вирішили здійснити кампанію проти 400 опонентів уряду. Серед останніх – близько 150 відомих журналістів, а також десятки поліцейських, які давали нелояльні до влади свідчення у зв’язку із звинуваченнями в корупції членів уряду.

Згідно з прогнозом Ф. Авні, поліцейські рейди мали відбутися одночасно в кількох провінціях країни. Арешту підлягали головні редактори газет Zaman, Today’s Zaman, Bugün та Taraf, які критикують уряд. Слідом за ними – бізнесмени-власники друкарень, що видають опозиційні видання, та інші критики влади.

У наступному твітті Ф. Авні написав, що після оприлюднення наміру їх скасували.

Біля будівлі газети Zaman у Стамбулі на знак протесту проти прогнозованих арештів зібралися декілька десятків журналістів.

Ф. Авні вже висував декілька прогнозів, що справдилися, зазначає автор кореспонденції. Наприклад, у серпні він повідомляв, що в Стамбулі та в інших містах буде здійснено операцію проти поліцейських і через їхні «фальшиві звинувачення» під арешт потраплять 32 охоронців порядку. Наступного дня за звинуваченням у шпигунстві звільнили з роботи 33 співробітників правоохоронних органів.

«Хто ж цей таємничий інформатор?» – ставить питання автор публікації зі Стамбула і намагається знайти відповідь: «Старший офіцер поліції, котрий заздалегідь поінформований про майбутні дії влади і стоїть на боці тих, хто може завдати шкоди Ердогану? Чи, може, це група критиків?»

Ф. Авні пише про себе, що він належить до «внутрішнього кола» Р. Ердогана. Президента він ніколи не згадує по імені, а називає тираном.

У коротких реченнях, розміщених у соціальній мережі, він раз-по-раз користується висловом «Я побачив у твоїх очах...». Це має наводити на думку, що йдеться про когось із безпосереднього оточення Р. Ердогана. Дехто підозрює, що за особою Ф. Авні приховуються кілька критиків влади.

Як би там не було, кількість прихильників утаємниченого автора сенсаційних твітів неухильно зростає. Турецька влада заблокувала його акаунт. Однак невдовзі він започаткував новий – unter @fuatavnifuat, який

має вже 596 тис. фолоуерів ***(Анонімний користувач Twitter попередив про операцію Ердогана щодо арешту 150 журналістів // Телекритики (http://www.telekritika.ua/kontekst/2014-12-14/101557). – 2014. – 14.12).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

«ВКонтакте» даст возможность администраторам продвигать страницы и сообщества в ленте новостей. Для этого разработан блок рекомендаций – четыре небольших баннера, содержащие название паблика, аватар и кнопку «Перейти», пишет Marketing Media Review (http://mmr.ua/news/id/vkontakte-pozvolit-reklamirovat-soobschestva-v-novostnoj-lente-42533/).

По словам разработчиков, нововведение удешевит и облегчит привлечение подписчиков в сообщества.

Новый формат будет запущен до конца декабря в десктопной версии сайта. Внедрять его будут в несколько этапов: сначала доступ получат партнеры, а потом все желающие.

Напомним, что реклама в ленте новостей социальной сети появилась в 2013 г. А в октябре 2014 г. появились инструменты для продвижения приложений в мобильных ***(ВКонтакте позволит рекламировать сообщества в новостной ленте // Marketing Media Review (http://mmr.ua/news/id/vkontakte-pozvolit-reklamirovat-soobschestva-v-novostnoj-lente-42533/). – 2014. – 15.12).***

***

Соціальні мережі: як особиста інформація може зашкодити вашій кар'єрі

В эпоху доступного Интернета все больше рекрутеров и руководителей компаний, прежде чем пригласить кандидата на собеседование, просматривают его странички в социальных сетях. И это относится не только к профилям на специализированных порталах по поиску работы (как http://www.trud.ua/kiev.html), где собраны и структурированы вакансии Киева и Украины, но и таким популярным ресурсам как Facebook и «ВКонтакте». Чтобы у работодателя сложилось о вас только хорошее впечатление, предлагаем взять на заметку несколько советов, которые значительно облегчат вам жизнь. Итак, начиная искать работу, проследите, чтобы на страничках ваших профилей не присутствовали:

1. Нецензурная лексика, политические и религиозные записи

Если с бранью и «крепкими» высказываниями все ясно (убрать немедленно и навсегда), то с политическими и религиозными убеждениями будет сложнее. Сейчас, в тяжелое, кризисное время, четкая политическая позиция является плюсом, но ее можно прописать парой-тройкой предложений, не засоряя профиль волнами резких и негативных записей. То же правило относится и к религии: слишком ярых приверженцев того или

иного вероисповедания работодатель не рискнет нанимать на работу, опасаясь, что они будут отвлекать коллег от задач своими замечаниями или теориями. Также не стоит исключать опасность конфликта на религиозной почве.

2. Откровенные фотографии

Начиная искать работу, постарайтесь удалить, или хотя бы скрыть фотографии, позиционирующие вас как легкомысленного человека (фото с распитием алкоголя и курением сигарет, опасными, незаконными поступками и т. д), а также снимки, описывающие вашу личную жизнь чересчур навязчиво (объятья, поцелуи) и, естественно, откровенные фото.

3. Слова-раздражители

Даже если вы пользуетесь только профессиональными социальными сетями, размещая на них свои резюме и контакты, постарайтесь «очистить» информацию от слов, вызывающих тоску у ректутеров, и потенциальных деловых партнеров. Эксперты издания Business Insider считают, что использование слов-раздражителей в заполнении профиля на профессиональных сайтах – неуместно, и даже неуважительно. Речь идет о таких словах как «обширный», «ответственный», «командный игрок». Появились также и новые выражения, которые пришли к нам из английского языка совсем недавно, но уже вызывают негативные эмоции: «динамичный», «интенсивный», «креативный».

Таким образом, проведя нехитрую «ревизию» и убрав двусмысленную информацию, вы сможете не только повысить шансы найти работу мечты, но и положительно зарекомендовать себя в глазах друзей и знакомых ***(Соціальні мережі: як особиста інформація може зашкодити вашій кар'єрі // Телекритика (http://www.telekritika.ua/kontekst/2014-12-17/101652). – 2014. – 17.12).***

***

Платформа управления кампаниями социальных медиа SocialBro выпустила инструмент мониторинга, который использует полный доступ к данным Twitter (Firehose), что позволяет проводить глубокий анализ данных по всей длине и ширине контента Twitter в режиме реального времени.

С этим дополнением SocialBro обеспечивает своим пользователям полный мониторинг исторических данных Twitter в режиме реального времени, позволяет собирать идеи и запускать маркетинговые кампании с использованием существующих инструментов.

Новый функционал мониторинга поддерживает сложные поисковые запросы с комбинациями хэштегов, упоминаний, мест, ключевых слов и настроений. Это позволяет пользователям применять кросс-фильтр и видеть срезы данных по нескольким факторам, а также учитывать демографические данные, такие как пол, местонахождение, языки и даже деятельность конкурентов.

Новые данные могут быть использованы компаниями для повышения социальной вовлеченности, используя целевой контент и кампании для сегментированных аудиторий. Например, после медиа-кампании новые подписчики могут быть вовлечены с помощью купона или бесплатного ознакомительного предложения.

Генеральный директор и соучредитель SocialBro Х. Бурон утверждает: «Маркетинговая платформа SocialBro является единственным решением на рынке, который сочетает полный доступ к данным Twitter с возможностью анализа и действий для экспоненциальных улучшений эффективности кампании».

Однако новый отчет компании Forrester Research «Стратегии социальных отношений, которые работают» показал, что маркетологи напрасно обращаются к лидерам социальных медиа – Facebook и Twitter – в попытке установить прочные связи с потребителями. На самом деле очень мало людей видят сообщения от топовых брендов на Facebook и Twitter, поэтому фокусировка на социальных сетях может быть пустой тратой времени, денег и ресурсов ***(Платформа социального маркетинга SocialBro добавила полный доступ к данным Twitter // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/platforma_sotsialnogo_marketinga_socialbro_dobavila_polnyy_dostup_k_dannym_twitter). – 2014. – 18.12).***

***

В недавно вышедшем отчете Kenshoo говорится, что возврат инвестиций (ROI) у маркетологов розничных сетей в 2014 г. возрос.

Авторы исследования подсчитали ROI по количеству кликов, полученных брендами в социальной сети. Также в отчете указывается на то, что за год рейтинг кликабельности брендов возрос в семь раз, пишет MarketingWeek .

Все более высокий спрос на новостные ленты и мобильную рекламу со стороны маркетологов привел к тому, что конкуренция между рекламодателями в Facebook возросла, что, в свою очередь, спровоцировало и рост расценок на рекламу. Это стало результатом того, что Facebook отказалась от рекламных колонок с правой стороны экрана и стала включать рекламу прямо в новостные ленты пользователей.

Высокий спрос на рекламные площади в новостных лентах А. Янг из We Are Social объясняет тем, что подобное размещение предоставляет рекламодателям больше возможностей для оптимизации и таргетинга.

«Бренды пользуются все более продвинутыми способами работы в Facebook. Это помогает им разрабатывать полностью отслеживаемые кампании, поскольку они пользуются текущими данными по аудитории, что в свою очередь приводит к принятию методики прямого ответа и позволяет наилучшим образом высчитывать ROI», – говорит А. Янг.

Отношения между Facebook и маркетологами не всегда были гладкими. Например, в отчете Forrester за 2013 г. говорится, что компания оказывала не так уж и много поддержки социальным взаимоотношениям между брендами и потребителями.

Опубликованный 9 декабря отчет Seeking Alpha подчеркивает, что если бы Facebook открыла возможность рекламироваться в мобильном поиске, то это помогло бы социальной сети лучше задействовать полученные данные о потребителях. Facebook уже обновила возможности поиска по ключевым словам в постах и фотографиях, но все еще не планирует продавать рекламу в мобильном поиске. Seeking Alpha заявляет, что поиск по ключевым словам мог бы помочь в выявлении того, что именно хочет купить пользователь в каждый конкретный момент времени.

Пока не ясно, приведет ли объявленное Facebook в прошлом месяце сокращение органической рекламы и рост платной к увеличению расценок. «Похоже, что в 2015 г. цены продолжат расти, хотя и не так резко, как это было совсем недавно», – отмечает А. Янг ***(Маркетологи розничных сетей отмечают удвоение ROI в Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/marketologi_roznichnyh_setey_otmechayut_udvoenie_roi_v_facebook). – 2014. – 16.12).***

***

Крупнейшая в мире социальная сеть Facebook внедрила новую опцию – возможность добавлять призывающие к действию кнопки в верхней части страницы. Кнопки Book Now (забронировать), Contact Us (связаться с нами), Use App (использовать приложение), Play Game (играть), Shop Now (магазин), Sign Up (зарегистрироваться) и Watch Video (смотреть видео) могут направить в любое место как в социальной сети, так и вне ее.

Dollar Shave Club протестировал кнопку Sign Up и был доволен результатами, – утверждает директор компании по приобретениям Б. Ким.

В течение трехнедельного теста кнопка Sign Up, призывающая к действию, показала в 2,5 раза более высокий уровень конверсии по сравнению с другими сопоставимыми социальными размещениями, направленными на привлечение нового пользователя.

В США функция будет реализована в ближайшие несколько недель, глобальный релиз запланирован на начало 2015 г.

Неделей ранее Facebook представил первые результаты использования мобильной кнопки Like в приложениях. Согласно данным компании, использование мобильной кнопки помогает значительно повысить вовлечённость пользователей приложений ***(Facebook внедряет призывающие к действиям кнопки для бизнес-страниц // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_vnedryaet_prizyvayuschie_k_deystviyam_knopki_dlya_biznes_stranits). – 2014. – 18.12).***

***

Социальная сеть Facebook любит экспериментировать в разных видах деятельности. Однако стремление стать полноценным игроком на рынке электронной коммерции выражено особо ярко. Как сообщает engadget.com, социальная сеть планирует запустить продажи разных групп товаров на своем сайте.

Концепция, которая может сделать Facebook конкурентом торговых площадок eBay и Craigslist, позволит пользователям продавать товары на сайте соцсети с помощью простой кнопки, размещенной рядом с опцией «опубликовать». Согласно статье, разработчик из Новой Зеландии Indy Griffiths разместил в Twitter-ленте сообщение о том, что он получил возможность реализовать продажу своих товаров на сайте Facebook в тестовой группе.

В посте было указано, что как только товар загружается на сайт, торговцу предоставляется возможность заполнить форму, указать цену, описание, добавить картинку и опции доставки. Затем объявление попадает в ленту и доступно всем пользователям к просмотру, им можно также поделиться или совершить покупку непосредственно на Facebook ***(Станет ли Facebook следующим eBay? // InternetUA (http://internetua.com/stanet-li-Facebook-sleduuasxim-eBay). – 2014. – 19.12).***

***

Twitter анонсировал новые таргетинговые опции для мобильной рекламы – оператор мобильной связи и новые устройства.

Опция позволяет таргетировать рекламу на пользователей, в зависимости от оператора мобильной связи, привязанного к их профилю, либо исключать таких пользователей из ЦА.

Используя данную настройку, рекламодатели могут таргетировать рекламные объявления (либо исключить из ЦА) на пользователей, которые недавно начали пользоваться Twitter на новом устройстве или с использованием нового мобильного оператора. Эта настройка идеальна для владельцев мобильных приложений, которые хотят охватить новую аудиторию.

При выборе ЦА можно учитывать оператора мобильной связи пользователя и новые устройства ***(Twitter представил новый таргетинг для мобильной рекламы // ProstoWeb (ttp://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_predstavil_novyy_targeting_dlya_mobilnoy_reklamy). – 2014. – 22.12).***

***

Чего ожидать от социальной сети «ВКонтакте» в 2015 году?

2014 г. стал для «ВКонтакте» годом перемен внутренних и, по большей части, управленческих. 2015 г. обещает стать годом перемен пользовательских. Особенно этого ждут рекламодатели, мечтающие о

новостной ленте с авторскими материалами, понятной и прозрачной статистике и честности в процессе купли-продажи сообществ «ВКонтакте», пишет Marketing Media Review (http://mmr.ua/news/id/chego-ozhidat-ot-socialnoj-seti-vkontakte-v-2015-godu-42677/).

Введение суточных лимитов на постинг в сообществах даст кратковременный эффект

Пятьдесят постов в сутки вместо 200 – это, безусловно, шаг навстречу качеству со стороны администрации. Уверен, что такое нововведение болезненно ударит по накрутчикам всех рангов. Но изменит ли оно рынок рекламы в сообществах? Вряд ли. Серьезные изменения пришли бы с цифрой 25, но снижение лимита в четыре раза однозначно покажет положительную динамику развития. Внимание пользователей на рекламные посты в ленте новостей возрастет, у рекламодателей появится больше мотивации заказывать рекламу, а у администраторов – тщательно готовить контент.

Официальные рекламные публикации в ленте новостей

На увеличении рекламных охватов хотят заработать не только администраторы-любители, но и администрация социальной сети. Возможно, такой шаг будет «первой ласточкой» в цепочке действий, цель которых – увеличение доли официальной рекламы в сети. Все-таки биржа постов «ВКонтакте» не обрела той народной популярности, которую ей пророчил сам П. Дуров.

Улучшение статистики биржи постов «ВКонтакте»

Администрация обязательно возьмется за улучшение статистики своего главного рекламного проекта 2014 г. Показатель охвата записи в сообществе вводит в заблуждение рекламодателей вместо того, чтобы помогать им определить перспективу будущего рекламного размещения. Во-первых, рекламу не репостят, поэтому сравнивать охват контентной записи с охватом рекламной достаточно нерепрезентативно. Особенно учитывая, что чрезмерным количеством постов в сообществе можно «накрутить» показатель охвата, но значительно ухудшить реальную эффективность рекламы.

Глобальным решением был бы инструмент, измеряющий не сам факт попадания поста в рабочую область монитора сообщества, а среднее число времени, которое потратил среднестатистический пользователь на ознакомление с рекламной публикацией в ленте. Таким образом можно было бы вывести понятие «доля внимания пользователя на пост» из условного в реальное.

Открытие и бурный стартовый рост раздела «видеоканалы»

Разговоры о том, что «ВКонтакте» вот-вот запустит новый раздел, ведутся с 2013 г., но в 2015 перспектива открытия направления реальнее, чем когда-либо: видео как формат контента становится популярнее текстов и, естественно, информативнее графического контента, да и «Одноклассники» свои видеоканалы уже запустили. Скорее всего, на первых порах возможность создать видеоканал получат немногие желающие

(видеоблогеры, производители авторского контента и центральные телеканалы страны), но ближе к лету раздел наберет огромную популярность. Этому поспособствуют и владельцы сообществ, сконцентрировавшие у себя большие потоки донорского трафика, и сама администрация социальной сети, заинтересованная в скорейшем росте своего нишевого «детища».

Легальная передача сообществ между пользователями

Сообщество «ВКонтакте» с получением администратором возможности зарабатывать превращается в бизнес-инструмент, из которого можно извлекать прибыль. Необходимость разрешить пользователям легально передавать друг другу право управлением сообществом на каких-либо взаимовыгодных условиях назрела давно. Поскольку существуют администраторы, умеющие извлекать прибыль, и те, кто хотел бы продать свое право администрирования или сдать его в аренду официально. Например, Buzzcraft уже инвестировало в сообщества «ВКонтакте» суммарно более 20 млн р. И мы готовы инвестировать дальше, но хотелось бы, чтобы были озвучены единые правила купли-продажи сообществ, которые бы позволили проводить сделки в атмосфере спокойствия и стабильности ***(Чего ожидать от социальной сети ВКонтакте в 2015 году? // Marketing Media Review (http://mmr.ua/news/id/chego-ozhidat-ot-socialnoj-seti-vkontakte-v-2015-godu-42677/). – 2014. – 24.12).***

***

Если вы хотите подняться на уровень выше и увеличить доходы компании за счет SMM, обратитесь к опыту тех брендов, которые съели на этом собаку. Отличный кейс – компания KLM («Королевская авиационная компания», Нидерланды), которая делает 25 млн евро в год благодаря успешной стратегии продвижения в социальных сетях, пишет Marketing Media Review (http://mmr.ua/news/id/gramotnaja-strategija-prodvizhenija-v-socialnyh-setjah-prinosit-milliony-kejs-klm-42693/).

В основу этой статьи положены некоторые пункты этой стратегии со слов ее основного изобретателя и вдохновителя К. Фогель-Майер. Отработав многие годы в компании KLM, К. Фогель-Майер в настоящее время занимает должность менеджера отдела соц. медиа. В ее обязанности входит разработка и внедрение новых программ продвижения бренда в социальных сетях для привлечения внимания целевой аудитории, повышения продаж и уровня лояльности клиентов.

По словам К. Фогель-Майера, социальные маркетологи всего лишь гости на чужой вечеринке. Главным звеном в онлайн-ритейле всегда был и остается клиент. Опыт клиента – вот что важно для KLM при разработке стратегии SMM.

Итак, давайте посмотрим, что является приоритетным для успешного продвижения бренда в сети:

Выжить в новой маркетинговой реальности

Облетая 67 стран по всему миру, KLM вынуждена приспосабливаться к огромному рынку за пределами Нидерландов. Известный бренд с 95-летней историей и длинным списком владельцев, наследующих компанию, что влечет за собой множество процедур, затрудняющих развитие соц. стратегий, все же смог быстро адаптироваться к новой маркетинговой реальности.

А эта новая реальность означает – теперь потребители оценивают не то что ты говоришь, а только то что ты делаешь. Если люди, а это ваши потенциальные покупатели, лайкнули или подписались на вашу страничку в соц. сети, вы должны это уважать, иначе они также легко могут и отписаться. Если вы постите сообщение, которое не понравится людям или будет неправдой, то поднимется просто цунами негативных отзывов, вам это надо?

KLM уяснили это после чемпионата мира по футболу (World Cup 2014), когда они твитнули «Прощайте друзья» (Adios Amigos) после победы Голландии над Мексикой. В ответ на твит последовало 90 тыс. записей, 70 % из которых были негативными.

Возросли из пепла

Обширная социальная деятельность KLM в сети берет свое начало в 2010 г., когда полеты над Европой были запрещены из-за исландского облака пепла, тогда компании впервые пришлось задействовать соц. сети для ответа своим клиентам.

Если ранее соц. медиа использовались лишь для стандартных маркетинговых сообщений, то в тот момент нужно было реагировать быстро, так как тысячи вопросов стали стекаться на Facebook и Twitter, поскольку все другие каналы обслуживания были заняты.

Столкнувшись с дилеммой ответить на запросы или проигнорировать их, KLM выбрали первое. И без раздумываний над стратегией они стали отвечать своим клиентам по ходу того, как разворачивалась ситуация.

Это послужило началом социальной стратегии KLM, которая до сих пор остается основой их успеха.

Используя модель последнего клика (мы говорим о переходе, который привел к целевому действию, т. е. покупке), KLM ежегодно может поднять 25 млн евро через продажи в соц. медиа. И это довольно-таки весомая часть прибыли, и все благодаря фокусу на опыте клиента, который лежит в основе всего, что делает KLM.

Вот три основных направления в соц. стратегии авиалинии:

1. Услуги
2. Бренд и репутация
3. Коммерция

Чтобы оказывать качественные услуги, в том числе в сети, компания должна охотно отвечать на все вопросы клиентов, даже если они имеют негативную коннотацию.

Это непростая задача, учитывая, что KLM получает 45 000 отзывов в неделю, из которых около 5000 реальные запросы, требующие проработки.

Тем не менее KLM в среднем укладывается в 23 минуты, чтобы откликнуться на запрос, и общается на 11 различных языках (скоро увеличит охват до 14).

Это хорошо, но нет предела совершенству, и это может оказаться недостаточным для некоторых клиентов, особенно для тех, кто спешит на свой пересадочный рейс. Поэтому, чтобы клиенты не нервничали в ожидании ответа, каждые пять минут в верхней части изображения заголовка в Twitter KLM публикует время, необходимое для ответа на запросы.

Оплата прямо в социальных сетях

Мониторя и анализируя фидбэк клиентов, команда KLM по соц. вопросам имеет реальное представление о том, чего ожидают пассажиры от их компании.

Многие клиенты спрашивали об оплате напрямую через соц. сети, поэтому, обсудив с отделом информационных технологий и отделом расчетов возможность реализации этой задумки, KLM внедрили новый инструмент оплаты в соц сетях.

Этот инструмент работает через Facebook и Twitter. Для оплаты пассажир получает ссылку в личном сообщении, а затем самостоятельно выбирает предпочитаемый способ оплаты и завершает сделку. Соц. агент KLM получает сообщение, что платеж получен, а пассажир – подтверждение об оплате. Реализация проекта обошлась компании в 3500 евро, а теперь приносит 80 тыс. евро с продаж еженедельно.

Как сказала К. Фогель-Майер о продвижении в социальных сетях, «это как рваться вперед и наломать дров. Но лучше попробовать, или вы никогда не узнаете, работает ли это. Может быть, вы потерпите неудачу, тогда вы поймете, что это неправильно; но нужно немедленно идти дальше и пробовать снова» ***(Грамотная стратегия продвижения в социальных сетях приносит миллионы: кейс KLM // Marketing Media Review (http://mmr.ua/news/id/gramotnaja-strategija-prodvizhenija-v-socialnyh-setjah-prinosit-milliony-kejs-klm-42693/). – 2014. – 25.12).***

***

Facebook тестирует новую функцию Sell Something (продать что-то) в приложении Groups. Кнопка находится рядом с Write Post (написать сообщение) и Ask a question (Задать вопрос).

Если пользователь выберет опцию, ему будет предложено рассказать, что он продает. Это позволит ввести цену и выбрать, будет ли эта цена договорной. Затем следует описать предмет. Продавцы также имеют возможность предлагать доставку и оплату.

Пока неясно, сколько пользователей имеют доступ к функции. Facebook не объявлял о ней официально, и не каждый пользователь может увидеть ее.

Это новейшая попытка Facebook создания большего количества финансовых операций в пределах своей сети. Сеть также тестирует кнопку buy и планирует добавить платежи в Messenger ***(В приложении Facebook***

Groups теперь можно «что-то продать» // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_prilozhenii_facebook_groups_teper_mozhno_chto_to_prodat). – 2014. – 24.12).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Ученые из Университета Олбани провели исследование, которое показало, что зависимость от Facebook похожа на алкоголизм и наркоманию. Об этом сообщает MedDaily.

Отмечается, что в эксперименте приняли участие 292 студента в возрасте от 18 лет и старше. Добровольцы оценивали свое отношение к социальным сетям, отвечая на вопросы, подобные тем, которые обычно используются для диагностики зависимого поведения.

Почти 90 % оказались активными пользователями Facebook. Они уделяли социальной сети примерно треть времени, проводимого ими в Интернете. 67 % получали уведомления из Facebook на свой смартфон.

10 % пользователей Facebook не могли контролировать посещение социальной сети. Участники испытывали сильное желание зайти на сайт, чувствовали раздражение, если не могли этого сделать, и проводили в Facebook все больше и больше времени.

Исследователи обнаружили, что люди, которые не моли жить без социальных сетей, часто имели проблемы с алкоголем. Кроме того, многие респонденты, зависимые от Facebook, не могли контролировать свои эмоции, что в предыдущих исследованиях было связано с наркоманией.

Исследователи полагают, что у Facebook есть несколько характеристик, которые могут способствовать развитию зависимости, похожей на наркотическую. Уведомления или новый контент в новостной ленте пользователей выступает в качестве награды. Невозможно предсказать, когда появится новый контент, потому люди вновь и вновь заходят на свою страницу. Это способствует формированию зависимости. Ученые считают: зависимость от Facebook следует официально признать одной из поведенческих зависимостей ***(Facebook обозвали зависимостью // Вечерние Вести (http://gazetavv.com/news/ukraine/1418801161-facebook-obozvali-zavisimostyu.html). – 2014. – 17.12).***

***

Социальные сети: польза и вред для психики

Социальные сети обозначили тенденции развития Интернета в сторону интеграции, объединения возможностей в рамках единых, многопользовательских веб-платформ. Эти платформы предоставили возможность пользователю общаться с друзьями, читать новости, смотреть фильмы, слушать музыку, делиться этим с другими участниками, принимать участие в обсуждениях, объединяться по интересам, создавать сообщества и все эти возможности сосредоточены на одном сайте!

Бесспорно, социальные сети – большое технологическое достижение, которое сулит много возможностей. Но вместе с этими возможностями приходят и беды… Нельзя сказать, что социальные сети это один сплошной вред, так же как нельзя сказать то же самое, например, про компьютер игры. При правильном, дисциплинированном подходе к интернет-технологиям можно получить какую-то пользу и облегчить себе жизнь. Но всегда существует риск того, что работа с социальными сетями отразится вредными последствиями на нашей психике.

Какие это могут быть последствия? В чем заключается опасность социальных сетей? Об этом пойдет речь ниже.

Зависимость от социальных сетей

Социальные сети обладают большим аддиктивным потенциалом, то есть, значительным риском возникновения зависимости. Для этого существует несколько причин. Первая причина заключается в том, что работа в социальных сетях раздражает центры удовольствия в нашем мозгу. Мы испытываем приятные эмоции, каждый раз, когда читаем доброжелательный комментарий под своей фотографией, получаем «лайк», когда кто-то оставляет положительный отзыв и т. д.

Желание повторного получения этих эмоций несет нас вновь на просторы соцсетей, заставляя там проводить все больше и больше времени.

Вторая причина кроется в особенностях усвоения информации при работе в многопользовательских веб-платформах. Человек, который сидит, например, во «ВКонтакте», получает много разнородной информации мелкими порциями за маленький промежуток времени: прочитал коротенький комментарий, ответил, тут же открыл новости, там уткнулся взглядом в интересный пост в сообществе про науку, стал читать, параллельно включив аудиозапись, недочитал, так как внимание отвлекло сообщение от друга, ответил и зашел на страничку этого друга посмотреть что там новенького.

К такому режиму работы мозг привыкает очень быстро. Дело даже не только в самом удовольствии и особенностях усвоения информации, а в удобстве, быстроте и доступности соцсетей!

Чтобы получить удовольствие от мнения другого человека о твоей фотографии, не надо много мучиться: залогинился (хоть с телефона) и одним кликом просмотрел сколько человек «лайкнуло» твое фото на пляже! Чтобы

занять свое внимание чем-то не напрягающим и увлекающим, не нужно искать интересную статью в поиске: открыл контакт и начал читать новости и смотреть обновления друзей. Все быстро и удобно.

Быстрота и доступность – важные предпосылки формирования любой зависимости. Человек инстинктивно ищет самые легкие пути для достижения удовольствия, пусть эти пути неэффективны и приводят к вредным последствиям. Взять хотя бы привычку курить. Быстро и доступно.

Зависимость от времяпрепровождения в социальных сетях ведет к следующим проблемам.

Снижение продолжительности концентрации внимания

Мозг привыкает к работе с информацией из социальлных сетей и постепенно теряет способность длительное время удерживать внимание на чем-то. Развивается синдром дефицита внимания и гиперактивности. Это побочный эффект, порожденный философией интеграции информации: когда работа с единственным веб-интерфейсом начинает объединять в себе множество функций, таких как общение, прослушивание музыки, обсуждение встреч и т. д., у пользователя появляется соблазн преступить к всему сразу и совершать параллельно несколько процессов.

Это плохо сказывается на способностях нашего мышления. Становится трудно удерживать внимание долго, например, на чтении книги. Наш ум, следуя приобретенной привычке, начинает перескакивать с одного предмета на другой. Поэтому возникают сложности с тем, чтобы последовательно размышлять, обдумывать одну проблему: внимание постоянно «уплывает».

Особенно эта проблема остро стоит в контексте подрастающего поколения. Детское мышление намного более «пластично», чем взрослое и поэтому легче может перенять вредные стандарты мышления, которые формируют, в том числе, соцсети.

Информационная зависимость

Социальные сети могут превратиться в, своего рода, жвачку для мозга. Мы привыкаем постоянно получать какую-то информацию и если этого не происходит, начинаем испытывать информационную ломку. Она выражается в том, что нам становится трудно расслабиться в тех ситуациях, когда в мозг поступает мало данных, например, когда едем в метро или находимся на даче. Ведь наш мозг вечно обеспокоен тем, чтобы не переставать жевать эту жвачку и требует новых порций информации, так как привык каждый день получать ее из социальных сетей.

Утомление, стресс

Работая в режиме непрекращающегося потока информации и сменяющих друг-друга эмоциональных впечатлений, мозг сильно утомляется, организм испытывает стресс. К тому же, во время работы в соцплатформах вы смотрите в монитор, а переизбыток такой деятельности сам по себе ведет к утомлению, что бы вы при этом ни читали.

Отчуждение, снижение интеллекта

Когда вы много времени сидите в соцсетях, ваш мозг занят бессмысленной и бесцельной активностью, которую нельзя назвать полноценной интеллектуальной работой. Вы просто занимаете его чем-то, чтобы он все время был занят, не думая о качестве поступающей информации. Вместо этого вы могли бы о чем-нибудь подумать, прийти к решению жизненных проблем, построить планы на будущее, придумать какую-нибудь полезную идею, прочитать хорошую книгу и т. д. Но это все невозможно пока ваш ум озадачен пережевыванием интернет-жвачки, превращая вас в бездумного и отчужденного зомби.

Из-за того, что информация поступает быстро и непрерывно, вы и ее не успеваете переварить, обдумать. Эмоции не получают развития в ответ на поступающие впечатления, так как для этого требуется время и покой, которых нет в условиях судорожного усвоения информации.

Вы даже не можете сказать, что вам больше всего понравилось, так как вы спешили проглотить все как можно быстрее и не было времени, чтобы сформировалась оценка, некий эмоциональный отклик.

Сострадание, эмпатия, заинтересованность и увлеченность исчезают, не успевая толком оформиться в вашей психике, так как одна информация резко сменяет другую.

Должен отметить, что вышеназванные последствия вреда могут появиться не только из-за зависимости от социальных сетей. Эти симптомы могут стать как результатами чрезмерного увлечения компьютерными играми и Интернетом вообще, так и следствием многих проявлений современной жизни: интенсивной работы, стремительного темпа жизни, беспорядочного потребления информации, скуки…

Можно ли пользоваться социальными сетями без вреда?

Несмотря на страшные вещи, которые описаны выше, соцсети это не абсолютное зло, просто нужно пользоваться ими с умом и во всем знать меру, как и во многих других вещах. Социальные сети имеют ряд полезных функций, которые очень облегчают жизнь и работу в Интернете.

Социальные сети могут принести много пользы: помочь вам найти старого друга, узнать о новой книге или музыкальном альбоме, организовать встречу и мероприятие. Но злоупотребление общественными сетями (Интернетом, работой, компьютерными играми) может привести к зависимости, потери внимания, трате времени, отчуждению и отупению. Социальные сети это не великое зло, как многие считают. Это и хорошо и плохо. В ваших силах брать от них только хорошее и отсеивать плохое ***(Давтян В. Социальные сети: польза и вред для психики // UAINFO (http://uainfo.org/blognews/466541-socialnye-seti-polza-i-vred-dlya-psihiki.html). – 2014. – 25.12).***

Маніпулятивні технології

Россия атакует кременчугские социальные сети. Как сообщает администратор группы «Я люблю Кременчуг» А. Попенко, за последние сутки в группу неожиданно добавилась более 2000 человек и по статистике все эти люди жители России.

Мы попросили прокомментировать сложившуюся ситуацию эксперта, лидера общественного движения «Ай лав Кременчуг» А. Редькина. По его словам, он тоже заметил повышенную активность россиян в социальных сетях «Одноклассники» и «ВКонтакте».

«Причем в социальной сети «Одноклассники» – это превратилось в настоящую эпидемию спама», – сообщает А. Редькин.

Подписчики группы «Ай лав Кременчуг» регулярно жалуются на оскорбления со стороны фейковых и реальных страниц, которые зарегистрированы на территории Российской Федерации.

Почему так происходит и что может объяснить масштабный спам кременчугских социальных сетей?

Возможно, это связано с тем, что в социальных сетях началось распространение патриотического проекта кременчугского шоумена и радиоведущего С. Разумовского «#ТП або Так Повелося», который критикует политику России ***(Российские боты атакуют кременчугские группы и паблики в соцсетях // Кременчуг Today (http://kremenchugtoday.com.ua/news.php?id=38693). – 2014. – 16.12).***

***

Соціальні мережі представляють переселенця з Донбасу переважно як «утриманця» та «сепаратиста», пише «Корреспондент.net» (http://ua.korrespondent.net/ukraine/3457537-separatysty-utrymantsi-pereselentsi-z-donbasu-zaznauit-uperedzhen).

У соціальних мережах, у яких спілкується найбільш активна частина населення, поширюють негативні стереотипи про вимушених переселенців з Донбасу. Найбільш поширеними є ярлики та штампи: «Усі донецькі – сепаратисти», «Люди, які не хочуть працювати», «Вони вважають, що їм всі винні», або зневажливе прізвисько – «вата».

«Об'єктом мого дослідження були соціальні мережі, в яких спілкуються люди з різними політичними симпатіями», – каже в спілкуванні з DW блогер та журналіст із Донецька Н. Казьоннова. «Насправді наш регіон таврують усі: і блогери – так само вихідці з Донецької та Луганської областей, і громадські діячі, і самі мешканці. Це порочне коло, яке важко розірвати», – зазначає Н. Казьоннова. Її дослідження відбулося в рамках проекту «Навчання з прав людини для журналістів зі Східної України» за фінансової підтримки Генерального консульства Німеччини в Донецьку та методичної підтримки Інституту масової інформації. Головний аспект цього проекту – ситуація з правами змушених переселенців з Донбасу.

«Переселенців з Донецька просимо не турбувати»

Одна з ключових проблем переселенців, пов'язаних з упередженнями проти них – труднощі з орендою житла. Один з міфів, який також тиражується, полягає у тому, що у разі невиплати орендної плати, переселенців з Донбасу буцімто не можна виселити за законом. «Я сама зіткнулася з такою проблемою, коли, шукаючи квартиру, натрапляла в Інтернеті на оголошення – "переселенців з Донбасу просимо не турбувати"», – розповідає Н. Казьоннова.

В інформаційному просторі також склалося дуже чітке розділення. Ті, хто виїхав із Криму – це патріоти України, а з Донбасу – це сепаратисти, які тільки і вимагають житло та гроші, зауважує Н. Казьоннова. І ніхто, за її словами, не бере до уваги, що з Криму, за офіційною статистикою, виїхало всього 20 тис. людей, а з Донбасу – майже 600 тис. Тому і співвідношення проблем зовсім різне, зазначає Н. Казьоннова. Щоправда, чим далі на Захід України, тим менше й негативу. У цього явища теж є пояснення – більшість переселенців наразі мешкають саме в східних областях України, зазначає дослідниця.

Жертви російської пропаганди?

В Україні існують регіони з різними ментальностями. Але наразі ці відмінності використані для розпалювання протистояння, каже DW доктор психологічних наук П. Горностай. «Це яскравий приклад впливу стереотипів, але він на руку тим, хто воює проти нас – я маю на увазі кремлівський режим. Саме йому вигідно, щоб протистояння ще більше посилювалося. І ті, хто начебто вважають себе патріотами України, так само заковтують гачок пропаганди і стають її жертвами», – зауважує експерт. Тобто ті, хто кричить «кляті сепаратисти» і «вата» – вони як раз і працюють проти єдності народу, зазначає експерт.

З цією думкою погоджується і керівник дослідницького проекту «Навчання з прав людини для журналістів зі Східної України», голова громадської організації «Альянс» С. Закревська. Але, на її переконання, це не єдина причина стигматизації донеччан.

Влада знайшла крайнього?

Можливо, навіть більш вагому роль відіграє невміння чи небажання влади організувати роботу з переселенцями, вважає С. Закревська. «Наш моніторинг показав: Київ віддає якісь розпорядження, а на місцях роблять вигляд, що їх зміст не зрозуміли». Як наслідок – штучно створені шалені черги з переселенців у всі можливі інстанції за якимись то довідками, і паралельно – зростання неприязні з боку місцевих жителів до тих, хто, «понаїхав». «У мене склалося враження, що влада знайшла для себе такого внутрішнього ворога у вигляді переселенців, на якого можна перекласти вину за всі економічні негаразди», – вважає С. Закревська. На критику у Міністерстві соціальної політики лише руками розводять. «Адже хто знав, що в Україні буде війна, внутрішні переселенці, біженці. Сьогодні ми спостерігаємо ще і шалений ріст безробіття», – зауважує заступник

директора Департаменту ринку праці та зайнятості Міністерства соціальної політики О. Мовчан. За її словами, кількість претендентів на одну вакансію за рік зросла вдвічі з п'яти до 10 людей. Через це – і зростання соціального напруження. Це загальна проблема, вона не стосується виключно біженців», – виправдовується чиновниця міністерства.

Схід і Захід разом?

Якщо переселенці не будуть реагувати на ситуацію, то вона буде тільки загострюватися, обростати кількістю нісенітниць та чуток. Це призведе тільки до поширення негативних настроїв проти донеччан, зазначає блогер Н. Казьоннова. «Нам буде все складніше доводити, що ми такі ж самі, як і мешканці інших регіонів, незалежно від того, якою мовою ми розмовляємо чи яке закінчення в нашому прізвищі». Натомість вона вважає, що розраховувати в цьому плані на державу було б наївно – держава наразі зайнята іншими питаннями. На її погляд, потрібна ініціатива від народу. «Я наведу маленький приклад, але він дуже показовий. Я беру участь у такому русі – у Львові наші переселенці створили ініціативну групу, яку назвали "Схід та Захід разом". Ми не хочемо бути чужими у Львові, ми хочемо дружби та розуміння, що ми всі – українці», – каже Н. Казьоннова. З нею погоджується і психолог П. Горностай. «Самі переселенці мають бути відкритими, йти на контакт, активно шукати роботу. Тоді їх поведінка в першу чергу і буде ламати стереотипи щодо них», – зазначив експерт ***(«Сепаратисти!», «Утриманці!»: Переселенці з Донбасу зазнають упереджень // Корреспондент.net (http://ua.korrespondent.net/ukraine/3457537-separatysty-utrymantsi-pereselentsi-z-donbasu-zaznauit-uperedzhen). – 2014. – 18.12).***

***

По оперативным данным группы «Информационное Сопротивление», структуры информационно-психологических операций (ИПсО) ГРУ ГШ ВС РФ и ФСБ РФ получили задачу на проведение широкомасштабной информационной операции по срыву или существенному воспрепятствованию готовящемуся в Украине четвертому этапу мобилизации.

Об этом сообщает на своей странице в Facebook народный депутат и координатор группы «ИС» Д. Тымчук.

По его словам, операцию россияне планируют проводить во взаимодействии со структурами «информационной войны» российско-террористических войск, созданными в оккупированных районах Донбасса специалистами ГРУ ГШ ВС РФ.

Главная цель операции – путем проведения широкомасштабной дезинформационной кампании сорвать, либо же максимально затруднить проведение мобилизации. Тем самым не позволив командованию Вооруженных сил Украины и других вооруженных формирований нарастить

количество оперативных резервов, либо же существенно замедлить и усложнить этот процесс.

«Целевыми группами и объектами воздействия обозначены военнообязанные граждане Украины, а также члены их семей. Задача – создать негативный фон вокруг проводимой т. н. антитеррористической операции (невыносимые бытовые условия, в которых находятся украинские военнослужащие в зоне АТО; представление сил АТО как “пушечного мяса”; представление терроризма на Донбассе как “народно-освободительного движения” и т. д.). В ходе операции планируется широко использовать формирование “должного структурированного общественного мнения в социальных сетях” при помощи видео- и аудиоматериалов, разнообразных “свидетельств очевидцев”. Кроме того, структурам ИПсО в РФ и на Донбассе поставлена задача организовать “непосредственное или косвенное воздействие” на аудиторию через некоторые украинские СМИ для создания так называемой “вторичной правдоподобности”, прежде всего путем публикации “достоверных материалов журналистских расследований”», – отмечает Д. Тымчук.

«По вопросам координации действий в рамках данной операции собственно российских структур ИПсО и созданных на оккупированной территории Донбасса соответствующих структур уже состоялось как минимум 2 организационно-административных совещания», – добавляет Д. Тымчук ***(Дезинформаторы от ГРУ и ФСБ попытаются сорвать мобилизацию в Украине // Вечерние Вести (http://gazetavv.com/news/policy/1418980526-dezinformatory-ot-gru-i-fsb-popytayutsya-sorvat-mobilizatsiyu.html). – 2014. – 19.12).***

***

Бывший глава BBC П. Хоррокс призвал министров Великобритании пересмотреть траты телеканала за рубежом из-за агрессивной политики российских и китайских каналов, пишет Marketing Media Review (http://mmr.ua/news/id/telekanal-bbc-prosit-pravitelstvo-uvelichit-finansirovanie-chtoby-protivostojat-rossijskoj-propagande-42646/).

По словам П. Хоррокса, корпорация направила в Министерство иностранных дел Великобритании запрос, «хотят ли в министерстве что-нибудь сделать с финансированием, чтобы увеличить освещение событий в Украине», однако ответа не получили.

Его поддерживает в этом вопросе глава комитета британской Общины лордов по культуре, СМИ и спорту Д. Уиттингдэйл. «Нас очень сильно превосходят россияне, эту тему я уже поднимал с BBC. Масштаб того, как мы проигрываем информационную войну, поражает», – заявил Д. Уиттинглдэйл.

МИД Великобритании спонсировал World Service BBC до апреля 2014 г. Теперь же бюджет службы новостей складывается из обязательных взносов за телевидение с домашних хозяйств.

Аудитория всей телерадиокомпании BBC составляет 265 млн человек в неделю, 191 млн из них – пользователи всемирной службы WS. Аудитория российской службы новостей RT составляет не менее 700 млн человек.

В конце ноября немецкий Russia Today утверждал, что Украиной руководят «фашисты», а США и Польша готовят ядерный удар по России ***(Телеканал BBC просит правительство увеличить финансирование, чтобы противостоять российской пропаганде // Marketing Media Review (http://mmr.ua/news/id/telekanal-bbc-prosit-pravitelstvo-uvelichit-finansirovanie-chtoby-protivostojat-rossijskoj-propagande-42646/). – 2014. – 22.12).***

***

У Facebook було створено фейкову сторінку голови Національного банку

Повідомлення Національного банку України

«Звертаємо вашу увагу на те, що сьогодні вночі в соціальній мережі Facebook було створено фейкову сторінку Голови Національного банку України Валерії Гонтаревої.

Зміст матеріалів на цій сторінці є недостовірним і не відповідає дійсності. У зв'язку з цим просимо утриматися від поширення та посилання на матеріали зазначеної вище сторінки, які є провокацією.

Водночас нагадуємо, що єдиним офіційним аккаунтом центрального банку у Facebook є ця офіційна сторінка Національного банку України: https://www.facebook.com/NationalBankOfUkraine.

Наголошуємо, що Голова Національного банку України не зареєстрована в жодній із соціальних мереж» ***(У Facebook було створено фейкову сторінку Голови Національного банку // Новини Полтавщини (http://np.pl.ua/2014/12/u-facebook-bulo-stvoreno-fejkovu-storinku-holovy-natsionalnoho-banku/). – 2014. – 26.12).***

***

Instagram начал кампанию по удалению поддельных аккаунтов, ботов и пользователей, которые рассылают спам, пишет Business Insider.

Ранее руководство Instagram заявило, что в декабре этого года займётся решением проблемы «неактивных или поддельных аккаунтов». Специалисты оценили масштаб работы в 10 млн аккаунтов, которые потенциально могут удалить. То же предупреждение было разослано пользователям приложения.

Некоторые участники Instagram выразили недовольство после того, как заметили резкое сокращение числа своих подписчиков. Они заявили о потере от 50 до 500 подписчиков. В знак протеста они отписались от официального аккаунта соцсети в Instagram. Таким образом, за последние сутки он потерял более 30 % подписчиков.

Считается, что в первую очередь сокращение количества фолловеров затронет аккаунты знаменитостей, а также тех, кто пишет к каждому посту

по 15–20 хэштегов (это привлекает спамботов, за счёт которых увеличивается количество поклонников страницы). После этого предположения, программист З. Аллиа создал инфографику, показывающую, сколько подписчиков могут потерять самые популярные пользователи социальной сети. На первом месте в ней находится аккаунт Instagram ***(Instagram начал массовую чистку среди фейковых аккаунтов // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_nachal_massovuyu_chistku_sredi_feykovyh_akkauntov). – 2014. – 26.12).***

Зарубіжні спецслужби і технології «соціального контролю»

Китай открыто оспаривает видение свободного и открытого Интернета. Руководствуясь соображениями поддержания хрупкого баланса между контролем информации, социальной и политической стабильности, с одной стороны, и продолжением модернизации и экономического роста для интернет-аудитории свыше 600 млн человек – с другой, китайское правительство пытается изменить то, как страны понимают свою роль в управлении Интернетом через концепцию под названием «Интернет-суверенитет».

Интернет-суверенитет относится к тому, что страна имеет право контролировать деятельность в Интернете в рамках своих границ. Это то, что Китай называет естественным продолжением власти государства справляться со своими внутренними и внешними делами. Для Соединенных Штатов и других западных стран, однако, управление Интернетом делегировано и распространяется на круг заинтересованных сторон, включая правительства, гражданское общество, частный сектор, научные, а также национальные и международные организации.

Л. Вэй, глава китайского Государственного Интернет и Информационного бюро и директор мощной стратегической группы по кибербезопасности, состоящей из высших руководителей Китая, является административным руководителем китайского Интернета. С большим опытом работы в китайском пропагандистском аппарате, Л. Вэй продвигает свою концепцию интернет-суверенитета за рубежом, в том числе в поездках в Силиконовую долину.

В своем выступлении на американо-китайском форуме интернет-индустрии, он попытался размыть грань между американской и китайской моделями управления Интернетом. Он приравнял американский подход с участием многих заинтересованных сторон к китайской «многосторонней» (ориентированной государством) поддержке управления Интернетом.

Влияние Л. Вэй опирается на годы активного китайского продвижения интернет-суверенитета во внутрикитайских пропагандистских усилиях, правительственных официальных документах, интернет-конференциях, двусторонних и многосторонних встречах, и встречах Организации Объединенных Наций.

Административный контроль Интернета вписывается в китайскую стратегию кибербезопасности: для поддержания правления коммунистической партии над Китаем. Обеспечение интернет-активности позволило бы Китаю установить контроль над распространением информации, контролировать «опасные» веб-сайты и социальные медиа, и устранить потенциальные источники беспорядков.

Список запрещенного в Китае контента в Интернете включает в себя любую информацию, которая: ставит под угрозу государственную безопасность, вредит государственным чести и интересам, распространяет слухи и разрушает социальный порядок и стабильность. Эти серьезные правила подкрепляются китайской литературой по стратегии кибербезопасности. Китайские киберученые, например, отмечают случаи, когда утрата контроля над Интернетом свергла режимы в Тунисе и Египте. Ничто не пугает правящую компартию Китая больше, чем перспектива неконтролируемого Интернета, приводящего к тому же результату в Китае.

Китай работает с международным сообществом на этом фронте, желая сигнализировать другим странам, что является ответственным и готовым к сотрудничеству партнером по вопросам технологий. Понимая, что нормами международного права до сих пор не установлены порядки управления Интернетом и киберактивностью, Китай вкладывает значительные усилия, чтобы установить курс на международное регулирование в области управления Интернетом.

Риторика интернет-суверенитета набрала обороты после того, как Э. Сноуден обнародовал информацию о программах наблюдения Агентства национальной безопасности США. Рост антиамериканских настроений дает Китаю возможность предложить развивающимся странам рассмотреть преимущества контроля над Интернетом.

Тем не менее, Интернет-суверенитет – лишь один из аспектов стратегии кибербезопасности Китая, и его реализация может затруднять или противоречить другим приоритетам – таким, как экономический рост или расширение доступа в Интернет для граждан. В свете этих конкурирующих целей, Китаю будет трудно поддерживать модель «Интернета с китайской спецификой».

Расширение доступа в Интернет увеличить количество граждан, чья интернет-активность в Китае будет контролироваться, требуя все большие ресурсы центрального правительства. Ограничение доступа к информации может негативно сказаться на стремлении китайских компаний выходить на международные рынки, замедляя экономический рост. Жесткое регулирование вынуждает некоторые компании – такие как Google, который покинул Китай в 2010 г., отказаться от ведения бизнеса в Китае ***(Как «Интернет с китайской спецификой» уничтожает Сеть // InternetUA (http://internetua.com/kak--internet-s-kitaiskoi-specifikoi--unicstojaet-set). – 2014. – 18.12).***

***

Немецкие исследователи обнаружили серьёзные уязвимости в семействе протоколов ОКС-7 (Общий канал сигнализации № 7 или SS7) – наборе сигнальных телефонных протоколов, используемых для настройки большинства телефонных станций (PSTN и PLMN) по всему миру.

Найденные баги позволяют стороннему наблюдателю очень легко перехватывать телефонные переговоры и трафик SMS, даже если в сотовых сетях используются самые современные стандарты шифрования.

Проблема в устаревшей инфраструктуре ОКС-7, а именно – в некоторых предусмотренных протоколом служебных функциях, таких как поддержка связи при быстром перемещении пользователя, переключении с одной соты на другую. Из-за отсутствия должных мер безопасности злоумышленник может подключиться к сети и получить трафик в незашифрованном виде.

Операторы сотовой связи используют современные станции связи 3G и 4G, но при этом они по-прежнему пользуются устаревшей инфраструктурой ОКС-7 для обмена трафиком между сетями.

При достаточной квалификации, если разобраться в функциях ОКС-7, то хакеры могут «определить местоположение абонента в любой точке мира, прослушивать разговоры в реальном времени или записывать зашифрованные звонки и текстовые сообщения для дальнейшей расшифровки», пишет газета The Washington Post.

О слабой защищённости ОКС-7 давно известно в сообществе ИБ, но новое исследование демонстрирует простые практические методы взлома системы, поэтому оно должно привлечь внимание к проблеме. Опять же, открытым остаётся вопрос о том, кому было известно об уязвимостях до настоящего времени и воспользовался ли он этими знаниями ***(Уязвимость в протоколах ОКС-7: прослушка телефонов по всему миру // InternetUA (http://internetua.com/uyazvimost-v-protokolah-oks-7--proslushka-telefonov-po-vsemu-miru). – 2014. – 22.12).***

***

Facebook и Twitter решили отказаться от блокировок страниц сторонников А. Навального. Обе социальные сети готовы к полной блокировке на территории России.

Об этом сообщает телеканал «Дождь» со ссылкой сразу на несколько источников.

После слушания в Замоскворецком суде Москвы, где государственное обвинение потребовало по делу «Ив Роше» для О. Навального восемь лет тюрьмы, а для А. Навального по совокупности 10 лет, сторонники политика создали страницу в Facebook для планирования уличных акций в его поддержку.

20 декабря она была заблокирована. Как пояснил «Дождю» пресс-секретарь Роскомнадзора В. Ампелонский, социальная сеть это сделала по

требованию Генеральной прокуратуры на основании федерального закона от 2013 г. о досудебной блокировке сайтов.

После того как об этом стало известно, Facebook осудил бывший посол США в России М. Макфол, а также редакции некоторых влиятельных американских изданий – в частности Washington Post.

Источники, знакомые с ситуацией, рассказали «Дождю», что обсуждение сложившейся ситуации происходило в штаб-квартире корпорации в Калифорнии, после чего было принято решение не блокировать все последующие страницы сторонников А. Навального. Об этом «Дождю» сообщил также один из создателей этой страницы Л. Волков.

Facebook осознает при этом, что подобные действия могут привести к полной блокировке соцсети в России и принимает эти риски.

При этом другой источник сообщил, что 22 декабря компания Twitter также приняла решение не блокировать аккаунты, публикующие информацию об акции сторонников А. Навального.

Пользователям будут пересылаться письма с требованием Роскомнадзора удалить эту информацию, однако к тем, кто откажется сделать это, никакие санкции применяться не будут, рассказал источник. В компании также готовы к полной блокировке на территории России ***(Из-за Навального в России могут отключить Facebook и Twitter // Українська правда (http://www.pravda.com.ua/rus/news/2014/12/22/7052853/). – 2014. – 22.12).***

***

Интернет стирает грань между частной и публичной информацией, демонстрирует исследование аналитической компании Pew Research Center. По мнению опрошенных экспертов, к 2025 г. граница между этими сферами может полностью исчезнуть.

Приватность всегда была гибким концептом, однако благодаря Интернету грань между частным и публичным становится все тоньше. На это придется отреагировать как политикам, так и технологическим компаниям. Для того чтобы выяснить, насколько успешной будет эта реакция, международная аналитическая компания Pew Research Center провела исследование, посвященное будущему приватности.

Pew опросили более 2,5 тыс. экспертов – IT-специалистов, социологов, интернет-пионеров, поинтересовавшись у них, удастся ли политикам и разработчикам создать «безопасную, массово признанную и вызывающую доверие инфраструктуру обеспечения права на неприкосновенность частной жизни к 2025 году» и предложить людям доступные возможности защищать собственную личную информацию.

Примерно 55 % из опрошенных Pew экспертов заявили, что не верят, что в ближайшие 10 лет такая инфраструктура будет создана, однако 45 % отметили, что это возможно. Но, вне зависимости от ответа, большинство

экспертов оказались солидарны в том, что онлайн-жизнь публична по своей природе.

«Почти все согласны, что среда меняется, – говорит соавтор исследования Л. Рэйни. – Примерно половина заявила, что мы приспособимся к этому, а другая половина – что это неумолимо поглотит человеческие жизни… и оставит людей в положении, где у них будет мало контроля за собственной приватностью».

Проблема приватности уже сегодня находится в центре глобальных дискуссий. ООН работает над резолюцией Генеральной Ассамблеи, в которой призовет государства уважать и защищать право людей на частную жизнь.

Исследование – попытка взглянуть на приватность в свете технологических перемен, стремительно растущей монетизации цифрового общения и изменяющихся отношений граждан и правительства, которые будут продолжаться в ближайшее десятилетие. «Мы находимся на перекрестке», – отмечает главный советник министерства национальной безопасности США В. Бутримас.

«Джордж Оруэлл, возможно, был оптимистом», – отметил один из коллег В. Бутримаса.

Многие эксперты согласились, что безопасность и защита личной информации – «фундаментальные проблемы цифрового мира». Один из вопросов, активно поднимаемых опрошенными специалистами: сможет ли обычный человек решить, хочет ли он, чтобы за ним следили?

«В будущем люди разделятся на тех, для кого важнее приватность, и тех, для кого важнее удобство», – считает профессор Н. Финнманн, глава датской исследовательской организации DigHumLab.

«Причина того, что люди недостаточно заботятся о защите частной информации, в том, что опыт большинства людей учит их, что предоставление своих данных позволяет коммерческим (и государственным) организациям сделать их жизнь легче, отвечая на их потребности. В то же время негативные результаты обычно очень серьезны, но сравнительно редки», – рассуждает старший исследователь компании British Telecom Б. Бриско.

Уже сегодня мы живем в эпоху беспрецедентного наблюдения, говорит главный сотрудник компании Sage Bionetworks Д. Уилбэнкс. «Я не думаю, что 10 лет – это достаточно для политиков, чтобы догнать технологический прогресс. У нас никогда не было повсеместного наблюдения – и тем более повсеместного наблюдения, которое выбирают добровольно».

Широко распространенное использование таргетированной рекламы – один из главных соучастников «убийства» приватности, считают эксперты.

«Люди больше не пугаются, когда видят рекламу, относящуюся к вещам, которые они искали. Это уже решенная проблема», – считает Л. Рэйни.

Социальные и культурные нормы постоянно меняются, говорит директор программы по исследованию цифровых медиа Техасского университета в Остине О. Зунига. Это касается и восприятия приватности, отмечает он. «К 2025 г. много проблем, моделей поведения и информации, которые мы считаем частными сегодня, таковыми не будут, – рассказал он Pew. – Информация будет еще более распространенной, еще более гибкой, еще более портативной. Цифровая частная сфера и цифровая публичная сфера будут, очень вероятно, полностью пересекаться».

«Мы увидели, что публичность становится модальностью по умолчанию, заменяя приватность, – отмечает главный исследователь GigaOm Research. – Для того чтобы существовать онлайн, необходимо публиковать вещи, которыми будут делиться другие люди, и делать это в публичных, открытых местах. Если нет – у людей будет меньше шансов завести новых друзей, найти или расширить круг общения, узнать новое и участвовать в онлайн-экономике» ***(К 2025 году цифровая приватность может исчезнуть // InternetUA (http://internetua.com/k-2025-godu-cifrovaya-privatnost-mojet-iscseznut). – 2014. – 22.12).***

***

Проблема в Skype позволяет легко организовать прослушку и наблюдение за собеседником незаметно для него. Об этом сообщил пользователь с ником Ponkers на социальном сайте Reddit. Он назвал это «кошмарным сном» людей, уделяющих повышенное внимание охране своей личной жизни.

Для того чтобы воспользоваться этой возможностью, необходимо наличие двух устройств с приложением Skype. На обоих устройствах абонент А должен войти в одну и ту же учетную запись Skype. Оба устройства должны быть подключены к сети. Затем абонент А осуществляет вызов абонента Б, у которого устройство на Android. Во время дозвона (когда идут гудки) абонент А отключает от сети устройство, с которого осуществлялся вызов. После этого Android-устройство абонента Б автоматически перезвонит на второе устройство абонента А, на котором он также вошел в свою учетную запись. Когда абонент А снимет трубку, между устройствами будут установлены голосовая и видеосвязь, и он сможет слышать и видеть все, что происходит на другом конце линии. Второй собеседник об этом может не знать.

Ponkers сказал, что обнаружил проблему при использовании целевого устройства на Android. Он не знает, можно ли использовать этот метод с аппаратами на других платформах. Он также сообщил, что контакт ему удавалось установить не всегда, а только примерно в одном случае из трех.

Абонент Б в данной ситуации сможет узнать, что за ним наблюдают, если увидит экран смартфона – на нем будет видно приложение Skype. Он также сможет узнать, что его смартфон перезванивал собеседнику.

Запись на сайте Reddit собрала множество комментариев. Многие подтвердили информацию, попытавшись воспроизвести проблему на различных устройствах, включая Nexus 5, Samsung Galaxy S4 и персональный компьютер. Некоторые заявили, что теперь вынуждены удалить Skype.

Пользователь Ponkers, сообщивший о проблеме, сказал, что с ним немедленно связалась корпорация Microsoft, с целью сотрудничества. Он предполагает, что проблема будет устранена в самое ближайшее время ***(Skype позволяет тайно наблюдать за собеседником // InternetUA (http://internetua.com/Skype-pozvolyaet-taino-nabluadat-za-sobesednikom). – 2014. – 25.12).***

***

Американский окружной судья США У. Мартини постановил, что правоохранительные органы имеют право создавать поддельные учётные записи в социальных сетях и использовать их в ходе расследования. Это решение было озвучено в ответ на запрос Д. Гатсона, обвиняемого в краже драгоценностей. Обвиняемый пытался заставить суд не обращать внимание на доказательства, добытые якобы незаконным путём.

Социальные сети стали очень популярным инструментом правоохранительных органов за последние годы. Преступники, зная об этом, стали действовать более скрытно, но при этом они нередко делают некоторые компрометирующие материалы доступными для пользователей, находящихся в списке контактов. Полицейские в свою очередь создают профили в социальных сетях, зарегистрированные на ложных людей, и пытаются добавить подозреваемых в список друзей.

Открытым остаётся вопрос о том, насколько законными являются подобные действия. Например, по правилам использования службы Facebook, нельзя регистрировать учётную запись на несуществующего человека. В Twitter аккаунт может вовсе не представлять человека или организацию, учётные записи в этой соцсети принадлежат абстрактным понятиям, или неодушевлённым предметам, например, космическому телу.

В случае с Instagram правила также не являются строгими, и судье не составило труда оправдать действия полицейских. «Для обмена данного типа информации по согласию не требуется выдача ордера», – говорится в его заявлении. Полицейские просто предложили подозреваемому через «аккаунт под прикрытием» добавить их в друзья, не нарушая его прав на приватность.

В ходе слушаний всплыл также ещё один прецедент, важный в контексте работы полиции в соцсетях. В 2012 г. другой окружной судья США постановил, что если пользователь из списка друзей подозреваемого сотрудничает с правоохранительными органами, он имеет право предоставлять им доступ к публикациям, которые видит сам.

В России Фемида также активно использует социальные сети для поимки преступников, но законодательные нормы здесь пока ещё далеки от

того, чтобы чётко урегулировать права и обязанности сторон ***(Полиция США законно заводит ложные аккаунты для слежки в соцсетях // InternetUA (http://internetua.com/policiya-ssha-zakonno-zavodit-lojnie-akkaunti-dlya-slejki-v-socsetyah). – 2014. – 28.12).***

Проблема захисту даних. DDOS та вірусні атаки

Аналитики шведской компании Detectify обратили внимание на весьма распространённую, но часто недооцениваемую угрозу кибербезопасности – забытые поддомены, пишет Блог Imena.UA (http://www.imena.ua/blog/hijacking-of-abandoned-subdomains/).

Многие крупные компании открывают на основном домене десятки поддоменов, связывая DNS-записи с посторонними доменами для служебных целей, а потом забывают о них.

Когда срок регистрации сторонних доменов истекает, их может подобрать любой посторонний. Таким образом, потенциальный злоумышленник получает сразу несколько векторов атаки.

К примеру, на зарегистрированном домене можно создать вредоносный сайт, привлекая пользователей вызывающим доверие адресом. Кроме того, забытый поддомен всегда можно использовать для рассылки почты с визуально авторитетного ящика.

В ходе сканирования сети аналитики выявили более 200 крупных организаций, подверженных этой уязвимости. Среди них довольно известные корпорации и сайты, входящие в топ-100 самых посещаемых ресурсов.

Исследователи показали действие описанной тактики на реальном примере. Они обнаружили, что компания Microsoft много лет назад запустила поддомен racing.msn.com и связала его DNS-запись с доменом msnbrickyardsweeps.com. Срок регистрации указанного домена истёк, так что шведы зарегистрировали адрес msnbrickyardsweeps.com и перенаправили его на поиск Bing. В настоящее время эксперты Detectify запустили онлайн-сканер для проверки домена на подобную уязвимость.

Напомним, гражданам Украины стали доступны 62 новых домена newTLD, и со временем этот список будет пополняться. На сегодняшний день украинцы могут регистрировать свои сайты в зонах .marketing, .academy, .technology, .company и многих прочих ***(Забытые поддомены представляют серьёзную угрозу безопасности в сети // Блог Imena.UA (http://www.imena.ua/blog/hijacking-of-abandoned-subdomains/). – 2014. – 15.12).***

***

Новая бесклиентская система позволяет злоумышленнику извлекать корпоративные данные через монитор. Использование этого метода не

оставляет следов компрометации сервера приложений или QR-кодов, пишет Блог Imena.UA (http://www.imena.ua/blog/your-data-stolen-through-pixels/).

Для совершения атаки хакеру необходимо получить физический доступ к целевой машине и установить устройство записи с поддержкой HDMI и клавиатуру Arduino.

На сегодняшний день предотвратить такую атаку невозможно. Технологию уже окрестили главной угрозой для существующих практик по предотвращению утечки данных.

Способ позволяет извлекать данные через монитор. Метод работает на предположении, что у взломщика есть доступ к ПК, но не к самим данным. При этом система вообще не оставляет никаких индикаторов компрометации сервера приложений.

В настоящее время разработкой методов противодействия новой технике взлома занимается Компьютерная группа реагирования на чрезвычайные обстоятельства Австралии.

Ранее аналитики установили, что хакеры часто используют черновики писем почтовых сервисов Gmail и Yahoo! чтобы контролировать пользовательские устройства.

Используя почту, хакеры применяют черновики электронных писем для запуска командных и управляющих запросов на заражённых системах. Подобный метод слежки весьма сложно определить ***(Новая хакерская техника взлома даёт доступ к любым данням // Блог Imena.UA (http://www.imena.ua/blog/your-data-stolen-through-pixels/). – 2014. – 15.12).***

***

16 грудня соцмережа Facebook піддалася атаці нового вірусу, який почав активно поширюватися в останні кілька годин.

Користувачі отримують від своїх друзів посилання у повідомленнях зі своєю аватаркою і написом «OMG». Юзери, які клікнули на посилання, починають «відзначати» ще 20 своїх френдів у «приватному відео». Кожен, хто натисне на лінк або спробує відтворити неіснуюче відео, піддається зараженню.

Фахівці радять у жодному випадку не відкривати ці повідомлення від друзів, а якщо все ж відкрили – негайно змінити пароль та перевірити ваш пристрій на віруси ***(У Facebook блискавично поширюється вірус під назвою "OMG" // Телеканал новин «24» (http://24tv.ua/home/showSingleNews.do?u_facebook_bliskavichno_poshiryuyetsya_virus_pid_nazvoyu_omg&objectId=521562). – 2014. – 16.12).***

***

Компанія Facebook зуміла видалити вірус, який поширився в соціальній мережі.

Джерелом інтернет-вірусу, з яким зіткнулися користувачі Facebook, було розширення YouTurn для браузера Chrome. Зараз шкідливі посилання і джерела поширення видалено, ідеться в повідомленні.

Видалити вірус користувачі можуть самостійно: для цього необхідно змінити пароль до свого акаунту, а потім видалити всі опубліковані вірусом матеріали на своїй сторінці ***(Facebook зумів видалити новий вірус // LB.ua (http://ukr.lb.ua/news/2014/12/16/289530_facebook_zumiv_vidaliti_noviy_virus.html). – 2014. – 16.12).***

***

Исследователи обнаружили уязвимость переполнения буфера в Honeywell OPOS Suite – комплексе ПО, который предоставляет стандартный интерфейс программирования для объединения PoS-терминалов в единую систему под управлением ОС Windows. Honeywell OPOS Suite используется в различных торговых сетях и прочих компаниях, где для оплаты покупок применяются PoS-системы.

Как сообщается в бюллетене, уязвимости подвержены все версии Honeywell OPOS до 1.13.4.15. Производитель уже выпустил исправление, устраняющее данную брешь.

Уязвимость существует в файлах HWOPOSScale.ocx и HWOPOSSCANNER.ocx. Поскольку в обоих случаях затрагивается один и тот же компонент, бреши присвоили лишь единичный идентификатор (CVE-2014-8269).

Уязвимость существует из-за того, что управляющие элементы не проверяют длины принимаемой строки перед тем, как скопировать ее в буфер. Удаленный пользователь может выполнить произвольный код. Для успешной эксплуатации бреши требуется, чтобы жертва перешла на вредоносную страницу в браузере или открыла вредоносный сайт ***(В Honeywell OPOS Suite обнаружена серьезная уязвимость // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/12/16/Honeywell-OPOS-Suite-flaw.html). – 2014. – 16.12).***

***

14 декабря Google внесла в «черный список» более 11 тыс. доменов, затронутых вредоносной кампаний SoakSoak. Все инфицированные интернет-ресурсы работали под управлением CMS WordPress, следует из блога компании Sucuri.

У ИБ-экспертов пока нет достаточного количества данных для того, чтобы указать на конкретный вектор осуществления атак. Тем не менее, предварительный анализ показывает, что в рамках вредоносной кампании злоумышленники могли эксплуатировать уязвимость плагина Revslider.

В компании говорят, что поисковик заблокировал сайты в связи с появлением на них вредоносного JavaScript-кода. Последний инфицирует

клиентские браузеры посетителей. В то время как Google внес в список блокировки только 11 тыс. ресурсов, дополнительное сканирование, проведенное специалистами Sucuri, показало, что число затронутых сайтов превышает сто тысяч.

Как следует из блога компании, об инфицировании сайта свидетельствует наличие файла wp-includes/js/swobject.js. Кроме того, в загрузчике шаблонов wp-includes/template-loader.php появляется новая функция FuncQueueObject. Специалисты подчеркивают, что наличие этих «нововведений» позволяет осуществление следующего: при посещении инфицированной интернет-страницы JavaScript-код загружает, декодирует и запускает вредоносное ПО с сайта SoakSoack.ru ***(Google заблокировал более 11 тысяч сайтов на WordPress // InternetUA (http://internetua.com/Google-zablokiroval-bolee-11-tisyacs-saitov-na-WordPress). – 2014. – 16.12).***

***

Исследователи безопасности обнаружили компьютерный червь, эксплуатирующий опасную брешь.

IT-эксперты из SANS Institute обнаружили червя, предназначенного для создания бэкдоров в системах хранения данных (NAS) QNAP, путем эксплуатации уязвимости ShellShock. Разработчики тайваньской компании, производящей атакуемые устройства, предоставили исправления безопасности еще в октябре этого года, однако из-за того, что процесс их установки вызывает у многих пользователей различные сложности, большинство систем QNAP остаются незащищенными.

По данным исследователей, в настоящее время червь распространяется исключительно среди устройств, работающих на базе операционной системы Linux.

«Атакующие используют QNAP CGI сценарий /cgi-bin/authLogin.cgi, один из наиболее популярных векторов эксплуатации Shellshock-уязвимости. Данный сценарий вызывается при входе в систему без необходимости предварительного прохождения аутентификации», – следует из сообщения экспертов.

Интересно также, что один из компонентов вредоноса предназначен для «хищения кликов» и ориентирован на сети сервиса онлайн-рекламы JuiceADV ***(ShellShock-уязвимость используется для инфицирования систем хранения данных QNAP // InternetUA (http://internetua.com/ShellShock-uyazvimost-ispolzuetsya-dlya-inficirovaniya-sistem-hraneniya-dannih-QNAP). – 2014. – 16.12).***

***

Компания F-Secure разместила в своем блоге сообщение о новой программе-вымогателе OphionLocker, которая распространяется посредством вредоносных рекламных кампаний, использует набор эксплоитов Rig и

осуществляет шифрование файлов по правилам эллиптической криптографии.

Проникнув в систему, вредонос шифрует определенные типы файлов, а затем вымогает 1 биткоин (352 дол. по нынешнему курсу) за ключи для расшифровки. Инструкции касательно платежа и получения ключей предлагаются по по URL-адресу на узле Tor2web.

Как сообщают эксперты из F-Secure, в случае инфицирования в виртуальной среде требование заплатить за ключи не поступает, а сами ключи не работают. Возможно, это связано с тем, что виртуальную среду используют антивирусные продукты. Смена тактики, очевидно, призвана затруднить анализ вредоносного ПО и тем самым увеличить продолжительность его жизни.

Ophion Locker был обнаружен автором блога Trojan7Malware. Впервые новая криптографическая схема и скрытый в сети Tor C&C-сервер были использованы в ходе вредоносной кампании, связанной с CTB-Locker ***(F-Secure предупреждает о появлении новой программы-вымогателя // InternetUA (http://internetua.com/F-Secure-preduprejdaet-o-poyavlenii-novoi-programmi-vimogatelya). – 2014. – 17.12).***

***

Во всех текущих версиях ядра Linux обнаружена уязвимость (CVE-2014-9322), позволяющая киберпреступнику повысить привилегии в системе. Проблема проявляется только в расширении x86_64. Брешь была выявлена в результате исследования ранее обнаруженной уязвимости CVE-2014-9090, позволяющей вызвать отказ в обслуживании. Обновление для этой проблемы применимо и к CVE-2014-9322.

Следовательно, вышедшие ранее обновления пакетов с ядром для Ubuntu и Fedora исправляют и данную уязвимость. Следует заметить, что патч от 9 декабря для RHEL/CentOS не содержит исправления проблемы.

В том случае, если уязвимость CVE-2014-9090 не устранена, возникает новый вектор атаки, который может привести не только к краху ядра, но и позволить выполнение кода с повышением привилегий. Уязвимость можно легко эксплуатировать в системах, в которых не активированы функции защиты SMAP (Supervisor Mode Access Prevention) и UDEREF.

Проверить свои системы на наличие уязвимости можно при помощи тестового эксплоита (sigreturn). Помимо CVE-2014-9322, в ядре Linux обнаружены еще две менее опасные бреши – CVE-2014-8133 и CVE-2014-8134, которые могут стать причиной утечки 2–4 байт из стека ядра ***(Во всех текущих версиях ядра Linux обнаружена уязвимость // InternetUA (http://internetua.com/vo-vseh-tekusxih-versiyah-yadra-Linux-obnarujena-uyazvimost). – 2014. – 17.12).***

***

Один из пользователей по имени Н. Малкольм в процессе поиска технической информации в Google нашёл множество фрагментов кода социальной сети Facebook, который, якобы, должен содержаться в секрете (http://www.imena.ua/blog/a-look-inside-facebooks-source-code/).

В обнаруженном случайно фрагменте оказался вывод командной строки с псевдонимами разработчиков Facebook, названиями служебных серверов и структурой директорий, на которых хранятся рабочие библиотеки.

После дальнейшего исследования Н. Малкольм нашёл ещё больше закрытых данных Facebook, включая служебные логии, показывающие, какие программы разработчики используют для юнит-тестов, и какие у них системы контроля версий.

Наконец, Н. Малкольм отыскал пароль, предположительно принадлежащий самому М. Цукербергу. Все найденные фрагменты кода можно скачать по ссылке. Пароль к архиву – sintheticlabs.com

Специалисты считают, что такая крупная утечка фрагментов исходного кода несёт огромный риск для безопасности Facebook, поскольку в этом коде могут быть ошибки, которые захотят использовать мошенники ***(В Интернете обнаружен исходный код Facebook // Блог Imena.UA (http://www.imena.ua/blog/a-look-inside-facebooks-source-code/). – 2014. – 18.12).***

***

Исследователи Proofpoint обнаружили первую широкомасштабную хакерскую атаку, в которой использовались телевизоры и по меньшей мере один холодильник. Это первый ботнет из домашней бытовой техники и из сферы «Интернета вещей».

В своем пресс-релизе Proofpoint отметили, что взлом, о котором идет речь, осуществлен между между 23 декабря 2013 г. и 6 января 2014 г. Устройства из ботнета трижды в день отправляли письма пакетами в 750 тыс. за раз со 100 тыс. устройств предприятиям и частным лицам по всему миру. Три четверти писем отправлялось с обычных компьютеров, и где-то четверть – с домашних устройств, таких как мультимедийные центры, роутеры, телевизоры. Как минимум один холодильник был частью этой сети.

И самое главное – оказалось, что не нужно быть слишком умным, чтобы взломать домашние гаджеты вроде телевизора или холодильника. Многие просто не сменили дефолтный пароль ***(Хакеры впервые атаковали бизнес через холодильник // InternetUA (http://internetua.com/hakeri-vpervie-atakovali-biznes-cserez-holodilnik). – 2014. – 21.12).***

***

Последние исследования сетевой безопасности выявили серьёзную уязвимость более чем в 12 млн бытовых и офисных маршрутизаторах по всему миру. Эта уязвимость позволяет любому достаточно

квалифицированному хакеру отслеживать пользовательский трафик или даже полностью перехватывать контроль над устройством. Слабое место кроется в модуле под названием RomPager, разработанном компанией AllegroSoft и присутствующим во многих бытовых моделях сетевых устройств – маршрутизаторах, точках доступа и других. В самом программном обеспечении нет ничего плохого, это важный компонент, обеспечивающий устройство веб-интерфейсом. По сути, RomPager является всего лишь компактным веб-сервером, который не занимает много места в прошивке устройства, имеющей обычно серьёзные ограничения по объёму.

Но версии RomPager до 4.34, как оказалось, содержат серьёзную недоработку, которая позволяет атакующему использовать специальным образом сформированный cookie-файл, который вызовет ошибку в памяти устройства и позволит перехватить права администратора. В числе прочего, взломанное устройство позволяет хакеру отслеживать в обычном текстовом виде весь пользовательский трафик, что уже означает полную потерю приватности. Возможны и другие вредоносные действия, к примеру, изменение настроек DNS или удалённое управление веб-камерами и прочими устройствами, подключенными к сети. Можно себе представить, что может натворить злоумышленник, получивший полный доступ к системам «умного дома». Нашедшие уязвимость исследователи нарекли её Misfortune Cookie (Несчастливое Печенье). Она получила официальный идентификатор CVE-2014-9222.

Точно определить, какие устройства подвержены этой атаке, довольно сложно, поскольку они редко выдают информацию о версиях всего используемого в прошивке программного обеспечения, а кроме того, ряд производителей мог вручную закрыть уязвимость без обновления версии RomPager. Но уже предварительное сканирование выявило, как минимум, 12 млн уникальных устройств, несущих в себе эту уязвимость. В этот список вошло около 200 моделей различных производителей, включая LinkSys, D-Link, Edimax, Huawei, TP-Link, ZTE и Zyxel. Исследователи из компании Check Point пока не обнаружили свидетельств, что данная уязвимость активно используется злоумышленниками, но не исключено, что именно она является причиной двух массивных серий взломов в 2014 г., когда пострадали сотни тысячи маршрутизаторов и их владельцев. В первом случае речь шла примерно о тысяче маршрутизаторов LinkSys, а во втором взломано было более 300 тыс. различных устройств разных производителей.

Сама проблема Misfortune Cookie была выявлена ещё в 2002 г., соответствующая «заплатка» была выпущена тремя годами спустя, но, как видно, разработчики и производители соответствующего оборудования либо не обратили на это внимания, либо не придали проблеме должного значения – в противном случае, первое же сканирование не показало бы 12 млн потенциально уязвимых устройств. Гарантированный метод убедиться в том, что вы не подвержены атаке по этому направлению – выяснить, какая версия RomPager работает на вашем устройстве. Если она имеет номер 4.34 или

выше, то всё в порядке. Кроме того, следует проверить, не закрыл ли эту уязвимость сам производитель устройства без обновления версии интегрированного веб-сервера. Дополнительную информацию можно найти в опубликованной Check Point документации (на английском языке). И как обычно, мы рекомендуем не пренебрегать обычными мерами сетевой безопасности ***(Серьёзная уязвимость найдена в 12 миллионах маршрутизаторов // InternetUA (http://internetua.com/ser-znaya-uyazvimost-naidena-v-12-millionah-marshrutizatorov). – 2014. – 20.12).***

***

Специально для злоумышленников, которые для проведения своих атак нуждаются в ботнетах, однако, не хотят создавать их самостоятельно, теперь появилась Vawtrak – сравнительно большая сеть инфицированных систем. При этом ботнет может быть разбит на более мелкие, поддерживающие множество различных веб-инъекций.

Как следует из отчета SophosLabs, Vawtrak представляет собой «реализацию сервиса, работающего по схеме Crimeware-as-a-Service (CaaS), где часть сети может быть арендована, к примеру, для повышения эффективности финансовых атак».

Кроме того, Vawtrak (известный также, как NeverQuest и Snifula) может быть установлен на мобильные устройства, использован в целях блокировки антивирусного ПО и в случае необходимости адаптирован к специфическим условиям.

По мнению экспертов Sophos, Vawtrak является одной из наиболее серьезных угроз среди всех активных ботсетей. При этом большая его часть используется для проведения атак на банки Германии и Японии ***(В сети зафиксирована волна заказных атак // InternetUA (http://internetua.com/v-seti-zafiksirovana-volna-zakaznih-atak). – 2014. – 21.12).***

***

Вредонос Dubbed Spark похищает данные из платежных терминалов станций техобслуживания автомобилей.

Исследователь безопасности Э. Меррит из компании Trustwave сообщает о вредоносном ПО Dubbed Spark, разновидности вредоноса Alina. Dubbed Spark отличается от основной версии прежде всего тем, что создан на языке программирования AutoIt.

Обычно скомпилированные сценарии весьма примитивны. Но в данном случае мы наблюдаем достаточно изощренную технику эксплуатации. Из-за простоты использования AutoIT злоумышленники могут без труда изменить сигнатуры вредоносного файла и обойти обнаружение антивирусным ПО.

Согласно анализу, проведенному сотрудниками Trustwave, сценарий на AutoIt содержит функции для выделения пространства в памяти и использования его для размещения бинарного кода. Затем сценарий вносит изменения в таблицу адресов импорта и выполняет вредоносный код.

Вредоносный бинарник встраивается в переменную размером 4000 байт, а функции сценария обеспечивают его загрузку и выполнение. Сценарий преобразуется в исполняемый файл Windows при помощи утилиты Aut2Exe. Исполняемый файл, в свою очередь, создает новый бинарник с вредоносным кодом.

Пресс-секретарь Trustwave Э. Росс сообщает о том, что вредонос был обнаружен в ходе изучения множественных инцидентов безопасности, имевших место в платежных системах станций автосервиса. По данным компании, вредоносом инфицированы множественные PoS-терминалы на территории США.

Вредоносное ПО Alina было обнаружено в конце 2012 г. Trustwave ассоциирует Spark с Alina по ряду причин. Прежде всего, вирус Alina ведет реестр процессов, которые не предназначены для карточных данных. Вредонос Spark ведет аналогичный реестр с добавлением некоторых приложений. Вредоносное ПО и его основная версия обладают одинаковым алгоритмом поиска платежных данных, а для маскировки перехвата карточных данных используют схожие схемы шифрования. Как и все другие версии Alina, Spark добавляет себя в ключ реестра HKCU\Software\Microsoft\Windows\CurrentVersion\Run\hkcmd, что обеспечивает запуск после перезагрузки системы, сообщают эксперты.

Кроме того, вредоносное ПО Spark имеет общие сходства с вредоносом JackPOS, которое заключается в использовании сценария AutoIt в качестве загрузчика ***(Эксперты обнаружили новую разновидность вредоносного ПО Alina // InternetUA (http://internetua.com/eksperti-obnarujili-novuua-raznovidnost-vredonosnogo-po-Alina). – 2014. – 22.12).***

***

Специалисты «Лаборатории Касперского» обнаружили новую модификацию вредоноса ZeuS. Банковский троян под названием Chthonic инфицирует компьютеры жертв под управлением Windows, позволяя злоумышленникам удаленно получить доступ к целевой системе и осуществить мошеннические транзакции.

Вредонос нацелен на множество систем интернет-банкинга: более чем 150 различных банков и 20 платежных систем, расположенных в 15 странах мира. В основном, его потенциальными мишенями являются банки Великобритании, Испании, США, России, Японии и Италии.

Заражение трояном происходит двумя способами: путем рассылки писем с эксплоитами и загрузки вредоносного ПО с помощью бота Andromeda.

В случае, когда рассылались электронные письма с эксплоитами, кибермошенники прикрепляли к сообщению специальный RTF документ, нацеленный на эксплуатирование уязвимости, позволяющей удаленное выполнение кода в Microsoft Word. Для того чтобы не вызывать подозрений, файлу было присвоено расширение .DOC.

Главным оружием новой модификации являются веб-инъекции – возможность вставить в код загружаемой в браузере страницы свой код и картинки. Это позволяло преступникам получить не только логин и пароль жертвы, но также ее номер телефона, одноразовые пароли и PIN-коды.

По словам специалиста «Лаборатории Касперского» Ю. Наместникова, новый вредонос представляет собой следующий этап эволюции ZeuS. Он использует шифрование ZeuS, виртуальную машину подобную ZeusVM и KINS, а также загрузчик Andromeda ***(Специалисты обнаружили новую модификацию трояна ZeuS // InternetUA (http://internetua.com/specialisti-obnarujili-novuua-modifikaciua-troyana-ZeuS). – 2014. – 21.12).***

***

В семействе троянов Boleto обнаружен новый вредонос, меняющий способ атаки в зависимости от того, какой браузер использует жертва. Об этом сообщает компания RSA в своем отчете.

Троян Onyx представляет собой усовершенствованную версию вредоноса Eupuds, которая отличается лишь способом инфицирования жертв. В то время как Eupuds вставляет вредоносный код в память браузера во время его выполнения, Onyx использует более гибкий способ атаки. Если жертва использует для платежа в банке Boleto брузер Chrome или Firefox, вредонос встраивает себя в программу под видом расширения и выполняет вредоносный JavaScript-код. При использовании Internet Explorer атака выполняется с помощью интерфейса COM внутри браузера.

В отличие от Eupuds, Onyx не изменяет банковский код Boleto. Он повреждает штрих-код, прилагаемый к платежному документу, загружая собственную версию изображения с вредоносного сервера или генерируя случайные черно-белые полосы ***(Семейство троянов Boleto пополнилось новым вирусом // InternetUA (http://internetua.com/semeistvo-troyanov-Boleto-popolnilos-novim-virusom). – 2014. – 22.12).***

***

Компания Cisco сообщила, что два ее программных продукта Cisco ASA (Adaptive Security Appliance) и модуль Cisco Application Control Engine (ACESM) уязвимы к новому виду атаки по TLS с эксплуатацией бреши POODLE.

Уязвимость возникла в результате некорректной реализации паддинга блочного шифра в протоколе TLSv1 при использовании режима сцепления блоков шифротекста (Cipher Block Chaining). Эксплуатация бреши позволяет неавторизованному киберпреступнику расшифровать содержимое защищенного канала коммуникации и получить доступ к важным данным.

По словам разработчика, в серии Cisco ACE 4700 данная проблема не обнаружена, но компания предупреждает, что некоторые сканеры могут идентифицировать эти программные продукты как уязвимые. Cisco

планирует выпустить обновления, исправляющие брешь, но когда это произойдет пока не уточняется.

О том, что POODLE можно эксплуатировать для атак по TLS стало известно в октябре этого года, вскоре после того как уязвимость была обнаружена. Как пояснил специалист Google А. Лэнгли, паддинг в TLS представляет собой модифицированную версию паддинга в SSL 3.0 ***(Два программных продукта Cisco уязвимы к атаке по TLS // InternetUA (http://internetua.com/dva-programmnih-produkta-Cisco-uyazvimi-k-atake-po-TLS). – 2014. – 19.12).***

***

Українські Кібер Війська заблокували сайти терористів ntribunal.su і ungu.org. Про це на своїй сторінці у Facebook повідомляє відомий український хакер Є. Докукін.

«Операція “Відплата” триває. Також блокуються й інші сайти», – написав він ***(Українські хакери заблокували два сайти терористів // InternetUA (http://internetua.com/ukra-nsk--hakeri-zablokuvali-dva-saiti-terorist-v). – 2014. – 23.12).***

***

Традиционно в канун рождественских и новогодних праздников растет не только объем покупок, в том числе и онлайн, но и уровень мошенничества. Результаты исследования, проведенного «Лабораторией Касперского» совместно с компанией B2B International, показали, что более половины пользователей, потерявших деньги в результате мошенничества во время онлайн-транзакций, не смогли вернуть похищенное в полном объеме.

Несмотря на то что многие финансовые организации декларируют готовность возмещать денежные средства, потерянные в результате киберпреступления, лишь 29 % респондентов сообщили, что смогли полностью возместить свои потери. 13 % также смогли добиться частичной компенсации, а 58 % вообще не смогли вернуть свои деньги. При этом такие финансовые потери могут быть весьма ощутимы – 16 % респондентов сообщили о суммах свыше 500$.

Ситуация осложняется тем, что не все пользователи в полной мере осознают опасность кибермошенничества – 17 % опрошенных уверены, что онлайновые преступления, связанные с кражей денег, происходят редко и их не коснутся. 52 % уверены, что вообще не могут стать целью кибератаки. Однако статистика показывает, что в течение 12 месяцев порядка 46 % пользователей хоть раз столкнулись с финансовыми киберугрозами.

«Даже если вы уверены, что в случае онлайн-мошенничества финансовая компания или онлайн-магазин вернут вам потерянные средства, все равно нужно быть начеку. В случае, если украденное будет возмещено полностью, что, согласно статистике, случается чуть более чем в четверти случаев, возместить потерянные время и нервы будет невозможно. Поэтому

так важно уделять особое внимание защите конфиденциальной информации, к которой относятся и ваши финансовые данные», – говорит Е. Харченко, руководитель отдела управления продуктами для домашних пользователей «Лаборатории Касперского» ***(Половина онлайн-покупателей не могут вернуть деньги в результате кибермошенничества // InternetUA (http://internetua.com/polovina-onlain-pokupatelei-ne-mogut-vernut-dengi-v-rezultate-kibermoshennicsestva). – 2014. – 23.12).***

***

Команда экстренного реагирования на киберугрозы промышленных систем управления (ICS-CERT) предупредила об обнаруженных исследователями Google критических уязвимостях в реализации протокола NTP, которые позволяют получить доступ к серверам с правами суперпользователя. Уязвимыми являются версии протокола 4.2.8 и ниже.

В уведомлении ICS-CERT сообщается, что эксплуатируя эти уязвимости, атакующий может выполнить произвольный код с привилегиями процесса ntpd. Примечательно, что осуществить подобную атаку может хакер даже с весьма средними навыками, а эксплоиты являются легкодоступными.

Две «серьезные» и четыре «менее серьезные» бреши, обнаруженные экспертами Google Н. Мехта и С. Роттгером, были исправлены 18 декабря текущего года. Бреши возникают в том числе из-за слабого ключа по умолчанию и слабых генерируемых случайных чисел. Три уязвимости могут вызвать переполнение буфера.

Перед развертыванием патча ICS-CERT рекомендует администраторам протестировать его, а также создать резервные копии настроек промышленных систем контроля. Кроме того, целесообразно свести к минимуму их взаимодействие с Сетью, в том числе поместить удаленные устройства и сети систем управления (где это возможно) за межсетевые экраны и в изолированных зонах ***(Обнаружены серьезные уязвимости в реализации протокола NTP // InternetUA (http://internetua.com/obnarujeni-sereznie-uyazvimosti-v-realizacii-protokola-NTP). – 2014. – 22.12).***

***

Хакеры готовят атаку на анонимную сеть Tor. Об этом сообщил глава проекта Р. Дингледин.

Сообщается, что атака нацелена на серверы директорий Tor, которые являются точками подключения к сети и отвечают за маршрутизацию трафика, позволяя пользователям оставаться анонимными. В результате этой атаки сеть может оказаться неработоспособной, но анонимность пользователей системы будет сохранена. По словам Р. Дингледина, хакерская атака ожидается в ближайшие несколько дней.

Tor – это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Сегодня ее используют миллионы пользователей, включая спецслужбы. Tor позволяет

получить доступ к заблокированным ресурсам, однако также эту сеть часто используют для распространения противоправной информации и контента ***(Хакеры готовят атаку на Tor // InternetUA (http://internetua.com/hakeri-gotovyat-ataku-na-Tor). – 2014. – 22.12).***

***

Facebook рассылает пользователям сообщения о новом вирусе, обнаруженном на просторах сети. Вредоносная программа занимается «заражением» программного обеспечения мобильных устройств, имитируя YouTube.

Алгоритм работы очень простой и основан на доверчивости пользователей. Якобы от лица друзей приходит сообщение со ссылкой. Выглядит все правдоподобно: имеется даже фотография френда на автарке, а иногда сообщение действительно приходит от знакомого – если он уже «заражен». Перейдя по ссылке, пользователь оказывается на сайте, очень похожем на популярный видеохостинг Yotube. Предлагается просмотреть видео, зачастую – порнографического характера. Но, чтобы запустить его, необходимо скачать бесплатное расширение для браузера.

После установки «расширение» не только заражает мобильное устройство, но и начинает рассылать вредоносное сообщение всем друзьям пользователя. «Мы уже неоднократно предупреждали: Facebook не несет ответственности за сторонние сайты, даже если они выглядят надежными. Не устанавливайте ничего на устройства, не скачивайте незнакомые программы, не вводите персональные данные, номера телефонов ни в какие формы, отличные от тех, что предлагает сеть. Мы ищем источник вируса, но хвастаться пока что нечем. Будьте осторожными. Если приходят подозрительные сообщения, обращайтесь в службы Facebook. И меняйте пароль, возможно, он уже у злоумышленников» ***(В Facebook появился новый вирус // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_facebook_poyavilsya_novyy_virus). – 2014. – 23.12).***

***

Исследователь безопасности Ф. Алонсо обнаружил две XSS уязвимости в открытой Flash-библиотеке FlexPaper, которая используется на портале WikiLeaks для просмотра PDF-файлов. Как отмечается на форуме ресурса, компоненты Flash могут быть использованы злоумышленниками для деанонимизации пользователей Tor, а также для размещения ссылок на внешний контент с целью дискредитации WikiLeaks.

«Учитывая тот факт, что большинство браузеров используют плагины для чтения файлов PDF, мы настоятельно рекомендуем WikiLeaks напрямую давать ссылки на файлы и не использовать стороннее программное обеспечение, которое может поставить под угрозу безопасность пользователей», – подчеркнул один из участников форума.

Портал WikiLeaks использует открытую Flash-библиотеку FlexPaper для отображения PDF-файлов. Однако из-за различных программных ошибок FlexPaper уязвима к XSS-атакам и подмене содержания (Content Spoofing). Разработчики ПО осведомлены о проблеме и уже выпустили обновление с исправлением уязвимости ***(В используемой WikiLeaks открытой Flash-библиотеке обнаружены XSS уязвимости // InternetUA (http://internetua.com/v-ispolzuemoi-WikiLeaks-otkritoi-Flash-biblioteke-obnarujeni-XSS-uyazvimosti). – 2014. – 24.12).***

***

Є. Докукін та його команда проводять операцію, мета якої: захопити Wi-Fi точки доступу в Криму і Росії. Хакер попереджує, що у разі, якщо ви бачите назву Glory to Ukraine! або «Вітання» Путіну, слід знати, що ця мережа під контролем українців, повідомляє «Преса України».

Наразі під контролем українських експертів перебувають мережеві пристрої в Криму і Росії. Вони мають змогу вмикати та вимикати Wi-Fi, змінювати пароль або взагалі його відмінити.

Нагадуємо, що відомий український хакер Є. Докукін відтепер споглядає не лише окуповані території. Дедалі частіше йому вдається подивитись на різні місця РФ. На цей раз хакер зазирнув до «відділу ФСБ» у Москві ***(Кібервійськові здійснюють захоплення ворожих Wi-Fi точок доступу в Криму і Росії // StykNews.info (http://styknews.info/novyny/polityka/2014/12/25/kiberviiskovi-zdiisniuiut-zakhoplennia-vorozhykh-wi-fi-tochok-dostupu-v-k). – 2014. – 25.12).***

***

Исследователи Trend Micro опубликовали в блоге компании детали атаки на крупную корейскую электростанцию, подвергшуюся кибератаке с использованием вируса, удаляющего MBR – данные для загрузки операционной системы, располагающиеся в первых секторах жесткого диска. По их данным, вредоносное ПО инфицировало целевые системы путем эксплуатации уязвимости в приложении Hangul Word Processor, которое повсеместно используется в Южной Корее. Помимо этого, злоумышленники прибегли к методам социального инжиниринга.

Специалисты идентифицировали используемый киберпреступниками вредонос как TROJ_WHAIM.A – обыкновенный вирус, удаляющий MBR. Помимо своей основной задачи, он также перезаписывает некоторые файлы на целевой системе. Вредонос устанавливается в виде службы, благодаря чему может работать даже после перезагрузки ОС. Более того, он использует имена файлов и папок, а также описания легитимных системных файлов, благодаря чему его становится сложнее обнаружить.

Исследователи отметили, что уже наблюдали подобное поведение вирусов в прошлом. К примеру, в марте 2013 г. неизвестные злоумышленники атаковали сайты нескольких правительственных

организаций Южной Кореи, используя аналогичное вредоносное ПО. Более того, в недавней атаке на Sony применялась точно такая же атака.

Во всех трех атаках вредонос перезаписывал MBR, заполняя его определенными строками. В атаке, о которой сообщает Trend Micro, использовалась строка «Who Am I?», в то время как при нападении на Sony хакеры заполнили MBR строкой «0xAAAAAAAA».

Trend Micro не считает, что все три нападения совершила одна и та же киберпреступная группировка. Атаки были хорошо задокументированы и, скорее всего, при совершении последующих нападений хакеры попросту использовали наработки своих коллег ***(Корейская электростанция подверглась кибератаке с применением вируса, удаляющего MBR // InternetUA (http://internetua.com/koreiskaya-elektrostanciya-podverglas-kiberatake-s-primeneniem-virusa--udalyauasxego-MBR). – 2014. – 26.12).***

***

Социальные сети являются одним из наиболее эффективных инструментов для продвижения товаров и услуг благодаря возможности размещать контекстную рекламу. При этом попытки сделать рекламу более эффективной приводят к нарушению прав пользователей – соцсети не только анализируют публикации, которые интересуют клиентов, но и сканируют их личные сообщения. Об этом пишет 3dnews.ru

Американский окружной судья на этой неделе постановил, что Facebook должна ответить на групповой иск с обвинением в нарушении конфиденциальности пользователей. Социальная сеть не имеет права просматривать личную переписку человека, и более эффективная реклама, или даже улучшение сервиса не оправдывают её.

Юристы Facebook попытались изменить решение судьи, сославшись на Закон «О приватности электронных коммуникаций» от 1986 г. В этом документе говорится о допустимом перехвате данных поставщиками услуг связи, который возникает в ходе рабочего процесса.

В ответ судья заявил, что руководство Facebook не объяснило, как именно содержимое сообщений оказывается раскрытым для сотрудников компании в ходе «рабочего процесса».

Идея подачи коллективного иска возникла ещё в 2013 г., когда житель США М. Кэмпбелл пожаловался на то, что Facebook использует его личные сообщения для составления скрытого профиля, повышающего эффективность рекламы. Проведённое впоследствии расследование показало, что Facebook прекратила сканировать сообщения пользователей в октябре 2012 г. При этом компания продолжает «анализировать» сообщения для защиты пользователей от вирусов и спама.

Если в ближайшее время ничего не изменится, через несколько месяцев компании М. Цукерберга придётся отвечать не перед одним пользователем, а перед всеми клиентами, зарегистрированными до октября 2012 г. включительно ***(Facebook оштрафуют за эффективную контекстную***

рекламу // Media бізнес (http://www.mediabusiness.com.ua/content/view/41899/118/lang,ru/). – 2014. – 26.12).

***

Троян требует выкуп в 1500 долларов

Как указано в отчете антивирусной компании ESET, усилиями которой была раскрыта кибератака, вредоносная программа специализируется на шифровании документов, изображений и некоторых других файлов на компьютере пользователя. Для восстановления доступа к данным жертве предлагается заплатить выкуп в размере 1180 евро или 1500 дол. Оплата производится в виртуальной криптовалюте Bitcoin, причем в новой версии трояна для каждой жертвы заводится отдельный электронный кошелек.

По оценкам аналитиков ESET, в ходе вредоносной кампании было заражено около 40 тыс. компьютеров в разных странах мира и зашифровано свыше 280 млн документов. В декабре скорость распространения TorrentLocker достигала 700 ПК в сутки. При этом 1,45 % жертв (около 600 пользователей) полностью или частично оплатили выкуп, пополнив бюджет злоумышленников на 300–600 тыс. дол.

Операторы TorrentLocker распространяют троян в фишинговых письмах с исполняемым файлом, замаскированным под документ Microsoft Office, в приложении. В другом сценарии фишинговые сообщения содержат вредоносный документ MS Office с макросом на языке Visual Basic. При открытии документа макрос осуществляет загрузку вредоносной программы с удаленного сервера. После запуска исполняемого файла TorrentLocker выполняет поиск и шифрование документов, соответствующих шаблону – более 230 различных типов файлов.

«Мы считаем, что за вредоносной кампанией по распространению TorrentLocker стоит та же группа лиц, которая ранее использовала для подобных целей сложное банковское ПО Hesperbot, – комментирует М. Левейе, вирусный аналитик ESET. – Авторы программы изменили некоторые внутренние алгоритмы, которые использовались в предыдущих версиях. Эти меры затрудняют анализ вредоносного ПО и расшифровку файлов пользователей» ***(Троян требует выкуп в 1500 долларов // InternetUA (http://internetua.com/troyan-trebuet-vikup-v-1500-dollarov). – 2014. – 25.12).***

***

Специалисты ИБ-компании Sucuri обнаружили новую вредоносную кампанию, озаглавленную WPcache-Blogger, которая компрометирует тысячи WordPress-сайтов посредством эксплуатации уязвимости в плагине Revslider.

В отличие от кампании SoakSoak, WPcache-Blogger использует три различных вредоносных фрейма (malframe), которые создают одну вредоносную кампанию:

1. Wpcache-blogger – в этой кампании в качестве главного распространителя вредоносного ПО и C&C-сервера используется домен wpcache-blogger.com. В результате атаки было инфицировано 12 418 веб-сайтов из «черного списка» Google.

2. ads.akeemdom.com – по мнению специалистов Sucuri, эта вредоносная кампания осуществляется авторами SoakSoak, но в гораздо меньшем масштабе. Пока в ходе атаки было заражено 6086 заблокированных Google веб-сайтов.

3. 122.155.168.0 – кампания началась вскоре после SoakSoak и продолжается почти неделю. Атака затронула 9731 домен.

За короткое время вредоносная кампания WPcache-Blogger инфицировала 28 235 ресурсов, которые попали в «черный список» Google. По данным экспертов Sucuri, в ходе атак было скомпрометировано более 50 тыс. WordPress-сайтов. Следует отметить, что не все из них заблокированы ***(Вредоносная кампания WPcache-Blogger компрометирует тысячи WordPress-сайтов // InternetUA (http://internetua.com/vredonosnaya-kampaniya-WPcache-Blogger-komprometiruet-tisyacsi-WordPress-saitov). – 2014. – 27.12).***

***

Как отмечают специалисты ИБ-компании «Лаборатория Касперского», новогодние и рождественские праздники являются самым благоприятным периодом для злоумышленников, которые пользуются предпраздничным ажиотажем в своих целях. Именно в это время возрастает количество успешных фишинговых атак.

В так называемую Черную пятницу (начало распродаж), которая в этом году пришлась на 28 ноября, эксперты зафиксировали значительный рост фишинговых атак на популярные платежные системы и крупные торговые интернет-площадки, предлагающие скидки на товары. Количество попыток пользователей зайти на фишинговые веб-сайты, имитирующие эти ресурсы, вдвое и более раз превысило обычные показатели.

Эксперты заблокировали немалое количество фишинговых рассылок электронной почты, приуроченных к Черной пятнице. В этих сообщениях получателю предлагалось совершить выгодные приобретения или подтвердить свою ученую запись на том или ином платежном сервисе.

Для того чтобы не стать жертвами мошенников при использовании услуг интернет-магазинов, специалисты рекомендуют создать специальную карту для online-покупок с небольшим количеством средств на ней, не переходить по сомнительным ссылкам в сообщениях электронной почты и в соцсетях, не переходить по ссылкам, присланным от имени банковских организаций и платежных систем.

Также не стоит пользоваться услугами online-банкинга и совершать online-покупки в публичных местах, поскольку на таких компьютерах может быть установлено шпионское ПО, кейлоггеры или перехватчики интернет-

трафика. Обязательно нужно проверять, используется ли при передаче конфиденциальных данных шифрованное соединение. Если соединение защищенное, адрес веб-сайта должен начинаться с https, а в адресной строке или в строке состояния браузера должна присутствовать иконка замочка ***(В преддверии Нового года возрастает количество фишинговых атак // InternetUA (http://internetua.com/v-preddverii-novogo-goda-vozrastaet-kolicsestvo-fishingovih-atak). – 2014. – 27.12).***

***

Чем страшны вирусы для Facebook?

Некоторое время назад на странице Facebook с хэштегом #ZemanRuskaDevka некий явный представитель «русского мира» поместил грозное сообщение «Ни в коем случае не заходите на эту страницу, вы можете заразиться вирусом». На фоне недавней пандемии вируса OMG, который поразил многих пользователей русскоязычного сегмента Facebook, такие предупреждения смотрятся довольно угрожающе. Но есть ли основания ему верить? И вообще, чего стоит, а чего не стоит бояться при использовании Facebook?

Прежде всего, необходимо акцентировать, что Facebook на сегодняшний день не позволяет в любом виде вставлять HTML-теги, PHP-код или Java-скрипты. Таким образом, не существует штатной возможности встроить вредоносный код в пост на стене. Тем не менее, злоумышленник может опубликовать ссылку на вредоносный сайт и разослать ее по своим «друзьям». Однако пользователь пострадает, только если перейдёт по ней, – отмечает О. Сыч, технический директор антивирусного проекта Zillya!.

Именно по такому шаблону развивалась недавняя эпидемия вируса OMG. Алгоритм атаки был следующий: пользователь получал от своего друга уведомление, что его отметили на фотографии. При открытии уведомления он видел список участников, отмеченных на фото и ссылку, куда надо перейти, чтобы просмотреть изображение. Пока что уловка злоумышленников никакой угрозы не представляет, но подвох следует далее.

Если пользователь бездумно щёлкал по ссылке, то попадал на внешний сайт, где ему предлагали загрузить плеер для проигрывания видео. На самом деле вместо загрузки плеера устанавливалось вредоносное расширение для браузера. Далее на стене пользователя в Facebook автоматически появлялось сообщение, что он поделился ссылкой, и размещалось адресное обращение (через @имя) ко всем друзьям из его списка. Если друзей очень много, то публиковалось несколько сообщений, по 10 друзей в каждом.

Жертвы подобного вредоносного расширения рискуют лишиться своих учётных записей, поэтому эксперты советуют, в первую очередь, сменить пароль входа в Facebook. О том, как это сделать безопасно и надежно, можно прочитать в оригинале статьи. Далее необходимо проверить компьютер на наличие зловредного кода. Специалисты также рекомендуют отключить в настройках приватности аккаунта функцию, которая позволяет упоминать

пользователей в записях. Кроме того, надо удалить все подозрительные плагин-модули в веб-браузере. Например, в Chrome это можно сделать через меню «Настройки > Расширения». К счастью, разработчики Facebook среагировали на эпидемию довольно быстро: примерно на следующий день после первых заражений они принудительно удалили все вредоносные ссылки во всех аккаунтах.

Тем не менее, стоит отметить, что нынешний вирус – это, выражаясь языком интернет-слэнга, баян. Ещё в августе 2011 г. появился вирус, который точно так же распространялся путём публикации постов от имени пострадавшего, каждый из которых содержал ссылку на сайт-вирусоноситель и отмечались его друзья (в одном посте упоминается 10 человек). Что интересно, годом раньше аналогичный вирус был обнаружен в сети «ВКонтакте».

Кроме того, в марте 2013 г. появился аналогичный троян, который также был опасен исключительно ссылкой на вредоносный сайт.

Собственно, давно известно, что самое слабое звено в защите – сам пользователь. Ведь о том, что нельзя бездумно щёлкать на подозрительные ссылки, говорилось уже много раз. Но кто, получив от якобы близкого друга сообщение «Посмотри, какие классные фотки!» удержится от соблазна? И никто не думает, что лучше на минуту отложить просмотр и проверить, а кто же на самом деле прислал сообщение. Вот и смотрят потом «классные фотки» все друзья жертвы.

Всегда необходимо помнить, что учётную запись любого вашего друга могут взломать. Поэтому надо взять за правило никогда не кликать на ссылки, которые ведут на странный и неизвестный домен. Всегда лучше переспросить, что вам прислали и действительно ли это прислал ваш друг. А если сомнения останутся и после полученных ответов, то лучше позвонить и уточнить. Потому что некоторые вирусы способны даже отвечать в чате.

Итак, если некто пишет, что нельзя посещать какую-либо страницу Facebook из-за угрозы вируса, то можно особо не обращать на такие предупреждения внимания. Потому что, опасны только ссылки, ведущие на внешние веб-ресурсы. А если их не нажимать, то страница социальной сети угрозы не представляет.

Основную угрозу в Facebook представляют ссылки на внешние сайты

Вместе с тем Facebook – это живой, постоянно изменяющийся проект, в котором добавляются новые механизмы, возможность трансляции рекламы, различные API и т. п. Именно в таких новшествах и состоит главная угроза, – акцентирует О. Сыч. Стоит разработчикам пропустить какую-то возможность инкапсуляции кода в контент ресурса, как злоумышленники воспользуются ею.

В своё время были прецеденты, когда злоумышленники забрасывали вредоносный контент в рекламную сеть, информация из которой транслировалась на сайтах, входящих в данную сеть, и в результате появлялся риск заразиться на совершенно «белых» и нормальных сайтах.

В целом, можно предположить только два варианта кибератаки на пользователей через Facebook:

1. Кто-то найдёт уязвимость в этой соцсети.

2. Facebook позволит крутить в своей сети посторонний контент (скорее всего рекламный), и вот тогда надо особое внимание уделить качеству фильтрования этого контента.

Тем не менее, периодически возникающие вирусные эпидемии заставили разработчиков социальной сети принять более крутые меры. Facebook совместно с разработчиком Eset намерены создать бесплатный антивирус для ликвидации вредоносных программ, распространяемых через социальную сеть. Основная цель состоит в том, чтобы предложить пользователям технологию, которая улучшит защиту их устройств. Предполагается, что онлайн-сканнер вирусов значительно уменьшит количество вредоносных ссылок.

В случае обнаружения зловредного кода Facebook будет присылать пользователям уведомление со ссылкой на скачивание антивируса. После установки программа проведёт сканирование компьютера, однако процесс и результаты проверки будут отображаться только в Facebook ***(Чем страшны вирусы для Facebook? // InternetUA (http://internetua.com/cem-strashni-virusi-dlya-Facebook). – 2014. – 27.12).***

***

Кражи конфиденциальной информации из организаций в 2014 г. участились, сообщается в исследовании, проведенном компанией Zecurion.

Интернет стал самым распространенным каналом утечек данных (26,7 %), отмечают аналитики. При этом число утечек через электронную почту и флешки стабильно сокращается – по итогам 2014 г. оно составило 7,8 и 6,1 % соответственно.

Хакеры чаще всего получали доступ к конфиденциальным данным розничных сетей (17,8 %), госорганизаций (16,8 %) и медучреждений (16,5 %).

Суммарный ущерб от утечек информации в 2014 г. составил 17,782 млрд дол., в 2013 г. эта сумма была существенно больше: 25,11 млрд дол. Средний ущерб от каждой утечки составил 25,51 млн дол. ***(Кражи конфиденциальных данных из организаций участились в 2014 году // InternetUA (http://internetua.com/kraji-konfidencialnih-dannih-iz-organizacii-ucsastilis-v-2014-godu). – 2014. – 28.12).***