СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(13–26.01)

2014 № 2

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(13–26.01)
№ 2

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Facebook меняет алгоритм работы новостной ленты – теперь она будет формироваться не из обновлений статусов ваших друзей, а из контента онлайн-СМИ, отобранного самим Facebook. 13 января социальная сеть сделала еще один шаг на пути к превращению в «персонализированную газету для всех и каждого» (цитата основателя М. Цукерберга) – купила стартап Branch, сеть обмена и обсуждения сетевых информационных материалов. Об этом сообщает «ЛигаБизнесИнформ».

О намерении сделать из Facebook полноценный новостной ресурс М. Цукерберг впервые заявил в начале 2013 г. В августе новостная лента начала перемещать наверх старые, но популярные посты. «Мы хотим, чтобы лента показывала посты не в том порядке, в каком они были опубликованы, а в том порядке, в каком их хотят читать», – заявляли в Facebook.

Это изменение привело к тому, что ранее популярные статьи многих международных изданий, опубликованные порой несколько лет назад, начали появляться в лентах пользователей и набирать новые лайки, количество которых доходило порой до полумиллиона. В октябре сеть отчиталась о том, что именно благодаря ей реферальный интернет-трафик (переходы по ссылкам, размещенным на сторонних ресурсах) журнала TIME, к примеру, за год возрос более чем на 200 %.

Однако 2 декабря Facebook объявила о новом пересмотре принципов работы алгоритма новостной ленты. Вверх по ленте начали перемещаться посты, получившие новые комментарии или лайки.

И если раньше после очередных изменений все СМИ рапортовали о приросте показателей, то результатом новых изменений стало укрупнение ведущих англоязычных интернет-СМИ за счет небольших локальных изданий. По данным компании Ignite Social Media, общее количество пользователей, видящих тот или иной пост, сократилось на 44 %. Некоторые компании потеряли до 75 % подписчиков.

В то же время отдельные интернет-медиа, у которых и без того были миллионы подписчиков, зафиксировали значительный скачок показателей. К примеру, сайт Upworthy через три дня после введения Facebook нового алгоритма отчитался о рекордных показателях по аудитории. Месячная аудитория сайта превысила 87 млн человек. Еще в октябре их было 47 млн.

Причина такой поляризации – в предвзятости Facebook. Как сообщил Л. Бекстром, отвечающий в компании за развитие новостной ленты, в интервью AllThingsD, отдельные издания получили в Facebook статус качественных, и их посты демонстрируются в ленте в первую очередь. Другие же были оценены как поставщики низкопробного контента.

То есть получить от Facebook максимальный трафик смогут теперь лишь крупные медиапроекты, публикующие уникальные или обладающие высоким вирусным потенциалом материалы. Нишевые медиа и бренды, до сих пор

собиравшие небольшую аудиторию, доносить до нее свои посты больше не смогут. Чтобы попасть в новостные ленты пользователей, им придется платить Facebook за рекламу.

Для украинских онлайн-СМИ эти изменения не критичны, уверен гендиректор United Online Ventures (bigmir.net, i.ua, korrespondent.net, forbes.ua и др.) Д. Лисицкий. «Украинский сегмент Facebook невелик, и трафика генерирует немного. К примеру, охват наших сайтов больше, чем весь охват соцсети в Украине», – говорит он.

Изменения будут полезны как для пользователей Facebook, так и для СМИ – ведь они заставят издания генерировать более качественный контент, уверен Д. Лисицкий. «В то же время посты, пытающиеся нагнать трафик в мертвые группы, теперь не увидит вообще никто – и это хорошо», – отмечает он. По его мнению, соцсеть способна решать за пользователя, что он будет читать. «Facebook основывается на статистике поведения пользователя. Это достаточно объективные данные», – отмечает он.

Однако социальные сети привлекают пользователей, прежде всего, возможностью самостоятельно выбирать, чей контент они хотят видеть, а также демонстрировать свой собственный контент. И если Facebook превратится в агрегатор новостей онлайн-СМИ, то вполне может потерять часть своей аудитории ***(Как Facebook будет сам выбирать, что читать пользователям // Новости Донбасса (http://novosti.dn.ua/details/216264/). – 2014. – 14.01).***

***

«Яндекс» заключил договор с Facebook, согласно которому получил полный доступ к публичным данным соцсети. Теперь записи из Facebook можно найти в поиске по блогам, позже они появятся и в основном поиске «Яндекса» – на yandex.ua, передает proIT.

Сервис получает открытые данные пользователей Facebook из стран СНГ и Турции. В настоящее время в поиске по блогам доступны записи жителей Украины, России, Беларуси и других стран СНГ. Свежие посты попадают на blogs.yandex.ua почти сразу после публикации.

Например, пользователи могут посмотреть, что говорят в Facebook о новых сериях про Шерлока Холмса. Чуть позже будут доступны не только посты, но и комментарии к ним.

Как уточняют в компании, в поиск не попадут профили и записи, закрытые для широкой публики.

«Данные Facebook будут использоваться также для улучшения ответов поиска – например, по запросам о недавних событиях. Там, где это уместно, “Яндекс” будет добавлять в результаты поиска свежие статьи или видеоролики, вызвавшие интерес в Facebook. Кроме того, популярность материалов в этой соцсети будет учитываться при ранжировании», – поясняют в компании ***(«Яндекс» получил доступ к открытым данным украинцев в Facebook // КОММЕНТАРИИ (http://comments.ua/ht/446434-yandeks-poluchil-dostup-***

otkritim-dannim.html). – 2014. – 14.01).

***

Пользователи видеохостинга YouTube вновь смогут управлять опубликованными под видео комментариями с помощью специального раздела YouTube Inbox. Сообщение об этом 13 января появилось в официальном блоге принадлежащего Google видеохостинга.

«Многие из вас писали, что активно пользовались этим разделом. Судя по всему, его удаление было ошибкой», – говорится в опубликованном представителями сервиса посте. Постепенно раздел управления комментариями будет возвращен во все аккаунты на YouTube.

Раздел YouTube Inbox позволяет пользователям отслеживать опубликованные ими комментарии, отвечать на чужие сообщения под видео, а также блокировать, удалять и помечать как спам нежелательные посты. Ранее, в ходе обновления видеохостингом системы комментирования, этот раздел был удален. На смену ему пришла единая система комментариев, привязанная к соцсети Google+. Посты пользователей Google+ стали отображаться под видео выше остальных. Кроме того, приоритет получили комментарии, оставленные друзьями и знакомыми опубликовавшего ролик человека (раньше комментарии сортировались под видео по времени своего размещения).

Видеохостинг YouTube был запущен в 2005 г. Спустя год сервис был куплен компанией Google. В 2013 г. ежемесячная аудитория сайта достигла 1 млрд человек. Каждый месяц пользователи YouTube просматривают в общей сложности более 6 млрд часов видеозаписей. Каждую минуту на сервис загружается около 100 часов новых видеоматериалов ***(YouTube вернул раздел управления комментариями // Лента.Ру (Россия) (http://lenta.ru/news/2014/01/14/bummer/). – 2014. – 14.01).***

***

Сервис микроблогов Twitter поменял внешний вид веб-интерфейса, сделав его более похожим на дизайн приложений для мобильных операционных систем iOS и Android, сообщает IT Expert со ссылкой на «РИА Новости».

Как следует из сообщения официального аккаунта Twitter, самым заметным изменением стало перемещение блока с информацией о профиле пользователя в левую колонку, правая колонка теперь полностью занята лентой сообщений. Под профилем также появилось поле для быстрого набора сообщения, которое теперь можно отправить прямо с главной страницы аккаунта.

При нажатии на кнопку «новый твит» и использовании горячих клавиш появляется традиционное всплывающее окно. Также было незначительно изменено цветовое решение сайта – все основные цвета остались прежними, с

черного на белый изменился цвет панели навигации, а цифры в профиле стали голубыми.

Twitter уже некоторое время использует подобный дизайн веб-интерфейса, представив его тестовой группе пользователей несколько недель назад, сообщает интернет-издание TechCrunch. В ближайшее время в сервисе микроблогов также могут появиться новые функции – возможность редактирования сообщений и привязка твитов к карте.

Активная аудитория Twitter превышает 232 млн пользователей в месяц, а ежедневная – 100 млн пользователей. При этом около 76 % аудитории сервиса пользуется им со смартфонов или планшетов. Каждый день на сервисе размещается свыше 500 млн сообщений-твитов ***(Twitter изменил дизайн веб-интерфейса // IT Expert (http://itexpert.in.ua/rubrikator/item/33250-twitter-izmenil-dizajn-veb-interfejsa.html). – 2014. – 14.01).***

***

Социальная сеть Facebook запустит свое новостное приложение для мобильных устройств. Проект под названием Paper (букв. «Газета») может появиться уже до конца января, сообщает Recode со ссылкой на анонимные источники.

Приложение будет сделано по схожей схеме с приложением Flipboard, созданным для чтения новостей из разных источников. Paper будет собирать популярные и важные новости как из СМИ, так и из статусов пользователей Facebook. Paper будет либо мобильным приложением, либо самостоятельным от Facebook сайтом, приспособленным под чтение на мобильных устройствах.

В последние месяцы Facebook активно шла по пути превращения в «персонализированную газету для всех и каждого» ***(Facebook запустит новостное приложение // Лента.Ру (http://lenta.ru/news/2014/01/15/faceboard/). – 2014. – 15.01).***

***

В социальной сети Facebook появился информационный блок со ссылками на самые обсуждаемые пользователями темы. Об этом представители компании 16 января сообщили в официальном блоге соцсети.

Блок под названием Trending отображается в правой верхней части новостной ленты и состоит из трех тем. Судя по опубликованному Facebook скриншоту, каждая тема сопровождается заголовком и кратким описанием того, почему эта дискуссия попала в тренды соцсети. Кликнув по заголовку, пользователь может попасть на страницу с постами других людей, посвященными выбранной теме.

Список трендов персонализирован – наполнение блока зависит не только от текущих новостных поводов, но и от интересов и предпочтений конкретного человека. Пока, как сообщается, раздел трендов доступен пользователям

браузерной версии социальной сети в США, Канаде, Великобритании, Австралии и Индии. В мобильных версиях Facebook блок может отображаться в тестовом режиме.

Запуск Trending стал еще одним шагом социальной сети на пути к превращению в «персонализированную газету». Блок с трендами появился на сайте через несколько дней после сообщения о переходе на работу в Facebook команды разработчиков приложения Branch. С помощью Branch интернет-пользователи могут создавать так называемые «ветки обсуждения», объединенные общей новостной темой или материалом. Создатели приложения занялись в Facebook разработкой продукта под названием Facebook Conversations, призванного упростить обсуждение в соцсети новостей ***(В новостной ленте Facebook появился блок трендов // Лента.Ру (Россия) (http://lenta.ru/news/2014/01/17/trendybook/). – 2014. – 17.01).***

***

Интернет-пользователи, особо увлеченные социальными сетями, выбрали из всего вороха сайтов для общения три самых необычных, пишет «Обозреватель» со ссылкой на econet.ru (http://tech.obozrevatel.com/testdrive/56013-tri-samyie-neobyichnyie-sotsseti-v-internete.htm).

Для тех, кто устал смотреть на котиков, добро пожаловать в сети, посвященные зомби и вампирам LostZombies.com. Обсуждения фильмов, придумывание возможных сценариев, фото и видео ходящих мертвецов, форумы и блоги. Участники форума обещают выпустить фильм на основе собственного сюжета.

Примета новой эпохи: хотите, чтобы сон сбылся, расскажите о нем в REMcloud.com – Twitter для сновидений, где каждый может запостить свой сон в общую ленту. Главное – вспомнить сон утром и успеть его записать. Не запоминаете сны? Тогда делитесь с миром мечтами на www.matchadream.com.

Если есть темные силы, то где-то собираются и светлые. К таким местам, можно причислить пользователей соцсети добрых дел lineforheaven.com. Если вы хотите сделать доброе дело, но не можете придумать, куда приложить силы, здесь вы найдете целый список с заданиями для «исправления кармы». За выполненные задания вам начисляют баллы – своеобразный пропуск в рай ***(Три самые необычные соцсети в Интернете // Обозреватель (http://tech.obozrevatel.com/testdrive/56013-tri-samyie-neobyichnyie-sotsseti-v-internete.htm). – 2014. – 15.01).***

***

В соцсети «ВКонтакте» появились лицензионные фильмы с рекламой, пишет «Обозреватель» (http://tech.obozrevatel.com/news/53098-v-vkontakte-poyavilis-litsenzionnyie-filmyi.htm).

Как пояснил Digit.ru пресс-секретарь «ВКонтакте» Г. Лобушкин, защита от копирования для размещенных видео обеспечивается соцсетью с помощью специальных программных решений.

Просмотр фильмов бесплатный, так как правообладатели получают прибыль от показа рекламы.

Одним из первых правообладателей, разместивших свои фильмы в соцсети, стала компания Star Media, сообщество которой в настоящее время насчитывает немногим более 3 тыс. участников.

Компания выложила фильмы «Последняя роль Риты», сериал «Ящик Пандоры» и др.

Как показало тестирование, рекламу, которая транслируется в начале фильмов, есть возможность «пропустить» через 3 с, кликнув на соответствующую ссылку ***(В «ВКонтакте» появились лицензионные фильмы // Обозреватель (http://tech.obozrevatel.com/news/53098-v-vkontakte-poyavilis-litsenzionnyie-filmyi.htm). – 2014. – 17.01).***

***

Количество американских пользователей Facebook в возрасте от 13 до 17 лет сократилось за последние три года на 25,3 %. К такому выводу пришла исследовательская компания iStrategyLabs, собравшая свои данные с помощью платформы для рекламодателей Facebook Social Advertising.

В январе 2011 г. более 13,1 млн американских подростков было зарегистрировано в соцсети. К январю 2014 г. эта цифра снизилась до 9,8 млн. Падение было зафиксировано и в возрастной группе от 18 до 24 лет. Количество пользователей этого возраста сократилось на 7,5 % – с 45,4 млн до 42 млн человек. Число школьников и студентов упало примерно на 60 %, в то время как число выпускников колледжей и университетов возросло на 64 %.

Наибольший рост – в 80 % – показала возрастная группа старше 55 лет. Если три года назад в Facebook было зарегистрировано всего 15,5 млн американцев этого возраста, то сегодня уже 28 млн. Рост в группе от 25 до 34 лет составил 32,6 % – до 44 млн человек. Рост в группе от 35 до 54 лет составил 41,4 % – до 56 млн.

О падении интереса подростков к Facebook писал и сайт TechCrunch. По данным издания, в рейтинге самых популярных приложений в американском AppStore Facebook стоит на 14 месте, тогда как фотосервис SnapChat – на шестом, а Instagram – на 11-м. SnapChat и Instagram, отмечает TechCrunch, активно пользуются именно подростки ***(Количество подростков в Facebook сократилось на четверть // InternetUA (http://internetua.com/kolicsestvo-podrostkov-v-Facebook-sokratilos-na-csetvert). – 2014. – 16.01).***

***

Facebook и Twitter теряют пользователей. Эра соцсетей заканчивается,

Интернет ожидают новые революции.

Два самых знаковых сервиса эпохи расцвета социальных сетей – Facebook и Twitter – переживают не лучшие времена. Общие цифры потерь в пользовательских базах неизвестны. Но независимые аналитические агентства дают пессимистические оценки по отдельным странам. Так, в конце апреля 2013 г. эксперты компании Socialbakers заявили: только за полгода соцсеть Facebook потеряла около 9 млн активных пользователей в США и 2 млн в Великобритании.

Популярным становится «виртуальный суицид». Социологи из Венского университета опросили тех, кто недавно удалил свои аккаунты в Facebook. Чаще всего причинами такого решения называли страх перед интернет-зависимостью и тревогу за личные данные. Facebook и прежде упрекали в чрезмерной запутанности интерфейса и проблемах с приватностью данных пользователей. Но в 2013 г. проблема приобрела больший размах. Руководство Facebook меняло настройки приватности, что ещё больше обострило ситуацию. Попытки проталкивать рекламу в ленты новостей пользователей также добавили негатива. Согласно результатам исследования, опубликованного авторитетным изданием Business Insider, большинство пользователей крупнейшей соцсети (около 80 %) вообще никогда не кликают на рекламные объявления.

«Это ставит под вопрос эффективность всей бизнес-модели Facebook», – считает Б. Визер, медиа-аналитик американской компании Pivotal Research Group.

Не лучше идут дела и у Twitter. Этот сервис долго был антиподом Facebook, предлагая более простой интерфейс, идеально подходящий для мобильных устройств. Twitter облюбовали политики и знаменитости. Однако и здесь успех оказался невечным.

В 2013 г. Twitter покинули десятки звёзд, включая А. Болдуина, Д. Лав Хьюитт, М. Сайрус, Д. Майера, М. Фокс. Большинство из них указывали в качестве причины негатив со стороны многомиллионной армии фолловеров, невозможность эффективно управлять коммуникациями с аудиторией.

Instagram, Reddit, Path и Pinterest – образцы тех сервисов, которые теперь нравятся людям, утверждает американский копирайтер и топ-менеджер рекламного агентства Vayner Media Л. Кингма. Главное их отличие – они построены вокруг ценности публикуемой информации, а не вокруг личности пользователя, который её публикует. «Будущее Интернета за сервисами, в которых содержание постов будет важнее личностей», – убеждён Л. Кингма. Facebook, Twitter и так и не набравшая большой популярности сеть Google+ в основном построены на личностном факторе.

Пока сложно сказать, что придёт на смену соцсетям в нынешнем виде, говорят эксперты. Не исключено, что успеха сможет добиться сервис, ориентированный на мобильные устройства нового поколения с дополненной реальностью, включая носимые гаджеты вроде Google Glass ***(Как закончится***

эра соцсетей // InternetUA (http://internetua.com/kak-zakoncsitsya-era-socsetei). – 2014. – 17.01).

***

Один из создателей социальной сети «ВКонтакте» П. Дуров объявил о новом рекорде, который поставило его детище. Соответствующее сообщение размещено на его странице.

«“ВКонтакте” взял новую высоту – 60 млн человек за сутки», – отметил гендиректор социальной сети ***(Посещаемость «ВКонтакте» превысила 60 миллионов в сутки // SiteUA (http://it.siteua.org/ИТ-Новости/526647/Посещаемость__ВКонтакте__превысила_60_миллионов_в_сутки). – 2014. – 21.01).***

***

Сервис для публикации фотографий и коротких видеороликов Instagram лидирует по темпам прироста аудитории среди мировых соцсетей – за второе полугодие 2013 г. количество его активных пользователей возросло на 23 %, свидетельствуют данные аналитиков из GlobalWebIndex.

В число лидеров по темпам прироста активной аудитории также входят блогхостинг Reddit (+13 %), соцсеть LinkedIn и китайский сервис Tencent Weibo (оба +9 %). Аутсайдерами этого списка оказались соцсеть Facebook и видеохостинг YouTube, потерявшие по 3 % аудитории, российские сайты «ВКонтакте» (–3 %) и «Одноклассники» (–4 %), а также сервис MySpace (–12 %).

В то же время Facebook остается лидером по проникновению на мировом онлайн-рынке – аккаунты в соцсети имеют более 80 % интернет-пользователей в возрасте от 16 до 54 лет. К показателю проникновения в 60 % приближаются YouTube и Google+, вслед за ними по числу аккаунтов идут Twitter, LinkedIn, Instagram и Pinterest. Отметим, что выводы GlobalWebIndex основаны на ответах 170 тыс. пользователей из 32 стран мира, в число которых не входил Китай.

Более 66 % пользователей заходят в соцсети с мобильных телефонов – ПК и планшеты для аналогичной цели используют по 64 % респондентов. Однако, исходя из данных GlobalWebIndex, при использовании мессенджеров и Twitter пользователи отдают предпочтение планшетам (44 %).

Популярность социальных ресурсов разнится по регионам. Так, в Северной Америке сравнительно высока активность пользователей в Facebook, на YouTube, в Instagram и Pinterest. Жители Азиатско-Тихоокеанского региона активно проявляют себя в Twitter, Google+ и LinkedIn, похожая тенденция наблюдается также на Ближнем Востоке и в Африке – примечательно, что этот регион уступает лишь США по активности в Facebook, а в Google+ и LinkedIn опережают остальных.

В Китае самым популярным сайтом остается Sina Weibo с проникновением в 80 %. Латинская Америка отличилась активностью на YouTube, в Instagram, Tumblr и Orkut, тогда как жители Европы уступили почти по всем показателям в десятке крупнейших соцсетей мира ***(Instagram лидирует среди соцсетей по темпам прироста аудитории // Marketing Media Review (http://mmr.ua/news/id/instagram-lidiruet-sredi-socsetej-po-tempam-prirosta-auditorii-37997/). – 2014. – 21.01).***

***

Социальная сеть Facebook является фаворитом среди подростков, а слухи о ее «смерти» сильно преувеличены, передает The Daily Mail со ссылкой на результаты нового исследования.

По словам основателя и руководителя исследовательской фирмы GlobalWebIndex Т. Смита, существует мало доказательств того, что спад популярности Facebook среди подростков, отмеченный University College London, отражает широкую тенденцию. Результаты нового масштабного исследования показывают, что социальная сеть Facebook остается самой популярной среди молодежи.

Согласно результатам опроса 170 тыс. пользователей в 32 странах мира, Facebook по-прежнему используют 48,5 % молодых людей в возрасте от 16 до 19 лет.

На втором по популярности месте находится видеохостинг YouTube, который регулярно используют 29 % подростков. Третью строчку занимает социальная сеть Twitter, которую ежемесячно используют 26 % подростков по всему миру ***(Новое исследование: слухи о «смерти» Facebook среди подростков преувеличены // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/novoe_issledovanie_sluhi_o_smerti_facebook_sredi_podrostkov_preuvelicheny). – 2014. – 23.01).***

***

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

Згідно з останніми даними, істотно зросла щоденна аудиторія Twitter – 4 %, що становить близько 500 тис. Місячна аудиторія Twitter (частка людей, які хоча б один раз на місяць заходили в Twitter) теж зросла й становить 21 % – це 2,5 млн.

Варто зауважити, що багато твітерян користуються Twitter виключно через мобільний додаток цього сервісу, і вони не включені в дослідження ***(Щодня близько 500 тис. українців заходять у Twitter // Watcher (http://watcher.com.ua/2014/01/24/schodnya-blyzko-500-tys-ukrayintsiv-zahodyat-u-tviter/). – 2014. – 24.01).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Министерство здравоохранения Украины открывает свои официальные страницы в социальных сетях Facebook, «ВКонтакте» и YouTube.

Посетить страницу МОЗ Украины в социальной сети Facebook можно по адресу: https://www.facebook.com/moz.ukr, «ВКонтакте» – https://vk.com/moz_ukr, YouTube – https://www.youtube.com/user/mozukr.

Минздрав Украины приглашает к общению на своих страницах представителей медицинской отрасли и неравнодушных к вопросам, связанным со здоровьем, сообщили «Индустриалке» в пресс-службе МОЗ Украины ***(Министерство здравоохранения Украины открывает свои официальные страницы в социальных сетях Facebook, «ВКонтакте» и YouTube // Индустриалка (http://iz.com.ua/zaporoje/30316-zaporozhcy-mogut-obschatsya-s-medikami-cherez-socseti.html). – 2014. – 14.01).***

***

В Facebook активисты создали сообщество «Аэромайдан» – вступить в него приглашают всех, кто путешествует на самолетах, работает в аэропортах или же имеет свой личный авиатранспорт. Двери сообщества открыты и для владельцев радиоуправляемых самолетиков. Анонсировано создание группы, участники которой будут активистами Аэромайдана с дистанционно-управляемыми самолетами и вертолетами. Сообщество уже нравится 71 пользователю соцсети.

Если инициатива будет продолжена, то в скором времени украинцев может ожидать целая волна разнообразнейших «майданов» – к примеру, железнодорожный майдан, на Крещение – гидромайдан, и может быть, даже межгалактический космомайдан! Ближе к весне и лету – могут быть объявлены мотомайдан и веломайдан ***(В соцсетях создан «Аэромайдан», на очереди – гидромайдан, космомайдан, веломайдан // IT Expert (http://itexpert.in.ua/rubrikator/item/33262-v-sotssetyakh-sozdan-aeromajdan-na-ocheredi--gidromajdan-kosmomajdan-velomajdan.html). – 2014. – 15.01).***

***

Начал работу официальный канал Донецкого городского совета на сервисе, предоставляющем услуги видеохостинга YouTube. Теперь узнавать о жизни родного города каждый его житель может не только прочитав новости на официальном сайте донецкого городского головы и городского совета, но еще и посмотрев видео к ним. Об этом сообщает пресс-служба Донецкого городского совета ***(У Донецкого горсовета появился канал на YouTube // Новости Донбасса (http://novosti.dn.ua/details/216438/). – 2014. – 17.01).***

***

Реакция соцсетей, которые просто «взорвались» от принятых 16 января парламентом документов, учитывая засилье в них пользователей, которые не очень симпатизируют властям, была достаточно предсказуемой, сообщает корреспондент IT Expert.

Отдельные комментаторы отмечают, что большинство из принятых 16 января документов были внесены в тот же день, и 95 % из тех, кто проголосовал «за», просто физически не знали, за что они голосуют, и «купились» на слова спикера В. Рыбака, что все согласовано с позицией Президента. Кроме того, в отдельных постах оспаривается легитимность самого факта голосования, мол не было в зале 235 депутатов (количество проголосовавших «за») и просят журналистов предоставить видеозапись с «картинкой» зала. «Как оказалось, с “регионалов” собирали подписи только за регистрацию, то есть протоколы голосования не велись», – пишет на своей странице в Facebook политолог А. Палий.

Пользователь В. Гладчук добавляет: «Закон об уголовной ответственности за клевету был принят Верховной Радой без соблюдения процедуры, публичного обсуждения, без электронной фиксации и фактического подсчета голосов».

Заведующий отделом Национального института стратегических исследований Д. Дубов указывает на то, что «мы, среди прочего (если все будет подписано), получим законодательно закрепленное определение “критический объект национальной информационной инфраструктуры”».

В отдельных постах проскакивает мысль о том, что законы являются приведением законодательства к общепринятой практике. «А симки по паспорту, наверное, только у нас и остались. В общем, стран, где контракт не нужен, меньше, чем там, где он нужен обязательно. То же и с доступом к Интернету», – пишет пользователь А. Худотеплый.

По поводу обязательной регистрации интернет-СМИ ориентированный на ТС журналист и политолог К. Долгов написал: «Надо будет – зарегистрируемся. Будут прессовать – нарвутся на “ответку”».

В еще одной части пользователей «теплится надежда», что еще не все потеряно. «Понаписывать законов можно каких угодно. Но воплотить их в жизнь – значительно сложнее. Так что не все так безнадежно», – считает председатель Независимого медиа-профсоюза Украины Ю. Луканов.

Напомним, что за принятие проекта закона № 3879 (зарегистрирован в Верховной Раде депутатом-«регионалом» В. Колесниченко) проголосовало 235 из 226 необходимых для принятия решения депутатов.

Были внесены следующие изменения:

– покупка SIM-карт с паспортом;

– введены штрафы за работу информагентств без регистрации;

– разрешено НКРСИ блокировать доступ к сайтам без решения суда;

– введена уголовная ответственность за клевету и экстремистскую

деятельность и т. д. ***(Решения Рады «взорвали» соцсети // IT Expert (http://itexpert.in.ua/rubrikator/item/33318-resheniya-rady-vzorvali-sotsseti.html). – 2014. – 17.01).***

***

Телекомпания NBC заключила партнерское соглашение с Facebook для освещения Олимпиады в Сочи. Об этом сообщает The Huffington Post.

Компания будет продвигать свой контент через специальную страницу NBC Olympics. 16 января NBC представила там видеосюжет о дружбе между американским конькобежцем Д. Сельски, перенесшим серьезную травму, и поддержавшим его рэпером Маклемором.

Кроме того, телекомпания проведет на своей странице пресс-конференцию с фигуристкой С. Хьюз, которая будет в прямом эфире отвечать на вопросы читателей во время соревнований по фигурному катанию. На NBC Olympics также будут публиковаться опросы, фотогалереи, интересные факты и другие материалы про Олимпиаду.

NBC также планирует продвигать свои материалы в принадлежащем Facebook фотосервисе Instagram. Проект рассчитан на привлечение дополнительных зрителей. Похожим образом NBC уже опробовал этот формат во время Олимпиады в Лондоне в 2012 г.

Олимпиада в Сочи стартует 7 февраля и продлится до 23 февраля. NBC является официальным транслятором игр в Америке. Телекомпания уже пригласила для комментирования игр в эфире российского ведущего В. Познера ***(NBC привлечет олимпийских зрителей через Facebook // Лента.Ру (http://lenta.ru/news/2014/01/17/nbcbook/). – 2014. – 17.01).***

***

Исполняющий председателя Киевской городской государственной администрации А. Голубченко завел официальную страницу в социальной сети Facebook, пишет «Обозреватель» (http://kiyany.obozrevatel.com/politics/19873-i-o--predsedatelya-kgga-zavel-ofitsialnuyu-stranitsu-v-facebook.htm).

«Я присоединился к вам на Facebook, чтобы общаться с вами непосредственно напрямую, чтобы лично отвечать на вопросы киевлян – и делать это как можно оперативнее», – сообщил чиновник.

Он считает, что общение в социальной сети поможет ему еще лучше понимать проблемы и запросы города. По его мнению, это поможет более качественно и эффективно решать проблемы киевлян.

Напомним, 14 декабря Указом Президента Украины председатель КГГА А. Попов был отстранен от исполнения обязанностей ***(И. о. председателя КГГА завел официальную страницу в Facebook // Обозреватель (http://kiyany.obozrevatel.com/politics/19873-i-o--predsedatelya-kgga-zavel-ofitsialnuyu-stranitsu-v-facebook.htm). – 2014. – 22.01).***

***

Название ул. Грушевского, где с 19 января продолжается ожесточенное противостояние между правоохранителями и протестующими, вошло в десятку самых популярных трендов украинского Twitter.

Среди лидеров также «#смотреть», «#Евромайдан», «Киева», «Ukraine» и «Кличко», передает «ВВС Украина».

Кроме того, как сообщил сайт «Trendinalia Украина», словосочетание «На Грушевского» вошло в 20-ку самых популярных трендов за минувшие сутки ***(Тренд «Грушевского» – среди лидеров украинского Twitter // КОММЕНТАРИИ (http://comments.ua/politics/447905-trend-grushevskogo--sredi-liderov.html). – 2014. – 22.01).***

***

У соціальних мережах з'явився термін «євровійна».

Якщо в перші дні протистояння на Грушевського фотоматеріали про нього можна було знайти за хештегом #грушевського, то нині з'явилося посилання #євровійна.

Світлини користувачів Instagram стали більш агресивними, страшними, жорстокими ***(У соціальних мережах з'явився термін Євровійна // Espreso.tv (http://espreso.tv/new/2014/01/22/u_socialnykh_merezhakh_zyavyvsya_termin_yevroviyna). – 2014. – 22.01).***

***

Диоцез Церкви Англии в Бате и Уэллсе выпустил правила поведения в социальных сетях для духовенства. Правила были опубликованы на сайте диоцеза.

В тексте говорится, что диоцез приветствует использование социальных сетей как «важного миссионерского инструмента», однако призывает священников и светский штат относиться к общению в социальных сетях так же, как к выступлению на любой другой публичной площадке. «Ваши действия должны соотноситься с вашей работой и христианскими ценностями; вы берете на себя ответственность за все, что вы делаете, говорите или пишете», – сообщается в документе.

Диоцез опубликовал девять правил поведения в соцсетях, которые в британской прессе окрестили «девятью заповедями». Первое правило призывает священников не спешить публиковать комментарии в соцсетях, а задуматься сперва, хотят ли они, чтобы этот пост прочитали их мать или Бог, а также хотят ли они видеть его опубликованным в СМИ. Кроме того, священники должны помнить, что все комментарии в соцсетях хотя и легко устаревают, никуда не исчезают, а также напоминают, что, говоря о церковных вопросах, они высказывают личное мнение.

Диоцез также призывает священников не писать в соцсетях анонимно, не

забывать о границе между частной и публичной жизнью, соблюдать профессиональную дистанцию (переписываться с группами людей, а не лично с пользователями) и нормы законов. Пасторов также просят не распространять в соцсетях информацию, предназначенную только для служителей церкви, и не делиться слишком активно личной информацией.

Правила поведения в социальных сетях ранее озвучивали представители и других церквей. К примеру, в США католическая церковь в 2010 г. опубликовала подробную инструкцию для клира и любых организаций, связанных с церковью. Патриарх Кирилл не раз призывал священников активнее пользоваться Интернетом и соцсетями, чтобы распространять там православное учение. «Не присутствовать там – значит расписаться в собственной беспомощности и нерадении о спасении собратьев», – заявил он на Архиерейском соборе в феврале 2013 г. Патриарх также велел разработать концепцию присутствия РПЦ в социальных сетях ***(Англиканская церковь опубликовала правила поведения в соцсетях // InternetUA (http://internetua.com/anglikanskaya-cerkov-opublikovala-pravila-povedeniya-v-socsetyah). – 2014. – 23.01).***

***

Президент Венесуэлы Н. Мадуро утвердил новую структуру правительства, в состав которого вошли 29 министров и 111 заместителей министров. Среди них есть заявленный ранее пост заместителя министра по обеспечению высшего народного счастья и новый пост – замминистра по делам социальных сетей.

Как отмечает издание Gaceta Oficial, целью создания новых должностей является достижение наивысшей политической эффективности и «революционного качества построения социализма» в стране.

По данным СМИ, в настоящее время в Венесуэле с населением 29 млн человек работает 2,7 млн чиновников. Их число увеличилось в два раза с момента прихода к власти экс-президента У. Чавеса в 1999 г. ***(В правительстве Венесуэлы появился пост заместителя министра, отвечающего за социальные сети // Росбалт (http://www.rosbalt.ru/main/2014/01/23/1224389.html). – 2014. – 23.01).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Популярный сервис коротких текстовых сообщений может стать новой торговой интернет-площадкой. Как сообщает осведомленный источник, в планах Twitter открыть на ресурсе сервис, с помощью которого пользователи смогут покупать товары прямо на сайте. Об этом сообщает «ЛигаБизнесИнформ».

Twitter намерен заключить соглашение с оператором по приему платежей Stripe. Масштабы и детали будущего проекта пока не ясны.

Напомним, В 2013 г. украинские онлайн-покупатели стали значительно активнее покупать через Интернет все категории товаров (по сравнению с 2012 г. показатели возросли на 6–18 п. п.). Чаще всего через Интернет покупают бытовую и компьютерную технику и электронику (в 2013 г. 73 % онлайн-покупателей сказали, что покупали эту категорию товаров за последние 12 месяцев против 64 % в 2012 г.), свидетельствуют данные исследования GfK Ukraine.

Больше украинских интернет-пользователей стали делать покупки в иностранных интернет-магазинах: в 2012 г. таких было 18 %, в 2013 г. – уже 26 %. В основном они покупали там бытовую/компьютерную технику и электронику, одежду, обувь, аксессуары и подарки. Основные причины покупок за рубежом не изменились: привлекательная цена, качественный и эксклюзивный товар, широкий ассортимент ***(Twitter может стать торговой площадкой – СМИ // Новости Донбасса (http://novosti.dn.ua/details/216599/). – 2014. – 21.01).***

***

Бренды стараются не пропускать крупные события планетарного масштаба и так или иначе играют на трендах, чтобы продвигать свои продукты и услуги. Во время грядущих игр в Сочи внимание маркетологов будет приковано не только к Twitter и Facebook, но еще и к «ВКонтакте».

Недавно сервис по продаже данных из соцсетей Gnip добавил поддержку «ВКонтакте», чтобы позволить брендам лучше ориентироваться в том, что пользователи этой соцсети говорят в преддверии Олимпиады.

Конечно, поначалу количество данных из «ВКонтакте» будет тяжело сравнить с объемами, которые компания выкачивает из Twitter (он является основным источником для Gnip), однако эта информация позволит брендам, которые следят за настроениями пользователей, вроде Coca-Cola или Nike, получить более точную картину.

«“ВКонтакте” был на наших радарах довольно давно, и наши клиенты так же давно интересуются этой соцсетью. А уж в преддверии Олимпиады заинтересованность просто зашкаливает», – сказал CEO Gnip К. Муди. «Они хотят получить способ понимать и измерять результаты того, что они делают».

Среди рекламодателей, которые могут быть особенно заинтересованы в том, что россияне говорят об их маркетинговых усилиях во «ВКонтакте», премиальные бренды и производители электроники.

В новом дата-фиде из «ВКонтакте» может быть заинтересована и компания социальной аналитик Networked Insights.

Я думаю, социальность локальна, и в этом плане людей все больше интересует то, что происходит поблизости», – говорит CTO Networked Insights Б. Берк. Среди клиентов фирмы, которые являются спонсорами Олимпиады,

такие компании, как GE, Samsung, P&G.

Однако на пути использования данных из «ВКонтакте» могут возникать определенные проблемы, считает К. Муди. Помимо языковых различий, существует и разница в том, как люди используют различные социальные сервисы. «Некоторые говорят, что “ВКонтакте” – это русский Facebook, но реальность такова, что между этими платформами есть отличия, так что люди ведут себя в каждой из них по-разному, – сказал он. – Лайк в одной платформе не равнозначен лайку в другой».

В то время, как господин Б. Берк считает, что данные из «ВКонтакте» помогут находить специфичные для России мемы и будут особенно важны для брендов в плане мониторинга вопросов прав человека, которые сопровождают сочинские Игры. Как известно, в России действует закон о запрете пропаганды гомосексуализма среди несовершеннолетних, который вызвал большой резонанс на Западе.

«Поскольку игры проходят в России, то к этому вопросу приковано особое внимание, – говорит Б. Берк. – Бренды очень сильно озабочены тем, как вопросы прав сексменьшиств и прав человека повлияют на Игры и все, что с этим связано» ***(В преддверии Олимпиады в Сочи иностранные бренды осваивают «ВКонтакте» // Marketing Media Review (http://mmr.ua/news/id/v-preddverii-olimpiady-v-sochi-inostrannye-brendy-osvaivajut-vkontakte-37989/). – 2014. – 21.01).***

***

Администрация социальной сети «Одноклассники» предложила владельцам некоторых сообществ ввести для своих подписчиков специальные подарки. Особенностью нового предложения соцсети является то, что владельцы крупных групп сами смогут создать для своей аудитории подарки в отличие от одинаковых виртуальных «подарков для всех».

Таким образом, администраторы групп смогут «заточить» их под свою целевую аудиторию. Планируется, что стоить такой подарок будет 20 р. Часть прибыли социальная сеть перечислит владельцам групп. Впрочем, пока не ясно, какой именно долей администрация сети готова будет поделиться ***(«Одноклассники» дадут заработать владельцам групп // IT Expert (http://itexpert.in.ua/rubrikator/item/33423-odnoklassniki-dadut-zarabotat-vladeltsam-grupp.html). – 2014. – 24.01).***

***

Социальная сеть Facebook объявила, что снова начинает пробные размещения рекламы в мобильных приложениях сторонних разработчиков. Сообщение об этом опубликовано на странице Facebook for Business, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-sobstvennuju-mobilnuju-reklamnuju-set-38020/).

«Чтобы улучшить релевантность рекламы, которую видят люди, обеспечить еще больший охват для рекламодателей Facebook и помочь разработчикам эффективнее монетизировать приложения, мы запускаем небольшое тестирование размещения рекламы Facebook в мобильных приложениях», – отмечается в сообщении.

В социальной сети напомнили, что уже проводили пробные размещения рекламы в 2013 г. Этот тест отличается тем, что Facebook будет работать напрямую с рекламодателями и разработчиками, а не с внешними рекламными платформами. Количество партнеров в тестовом проекте будет ограниченно, сообщили в Facebook.

Facebook уже развивает сервис Ad Exchange, который позволяет рекламодателям использовать данные пользователей для показа рекламы на страницах социальной сети. Решение провести уже третьи с 2012 г. пробные размещения рекламы может свидетельствовать о том, что Facebook обдумывает создание обширной рекламной сети, как это уже делает Twitter, пишет американский Forbes. Осенью 2013 г. сервис микроблогов Twitter приобрел разработчика сервиса MoPub, который помогает рекламодателям таргетировать интернет-пользователей для эффективного доступа к целевой аудитории своих продуктов. После поглощения MoPub продолжит продавать рекламу на огромном количестве сайтов, а не будет ограничиваться Twitter ***(Facebook тестирует собственную мобильную рекламную сеть // Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-sobstvennuju-mobilnuju-reklamnuju-set-38020/). – 2014. – 23.01).***

***

Основатель и генеральный директор социальной сети «ВКонтакте» П. Дуров подтвердил продажу принадлежавших ему акций социальной сети главе «Мегафона» И. Таврину. Сообщение об этом появилось на личной странице П. Дурова во «ВКонтакте».

«Это изменение едва ли отразится на управлении “ВКонтакте” – совет директоров прислушивается к моему мнению не из-за наличия или отсутствия у меня доли, а потому, что я создал эту сеть и понимаю ее глубинные механизмы», – сообщает П. Дуров.

П. Дуров добавил, что последние несколько лет он активно избавлялся от всей собственности. «До достижения идеала мне оставалось избавиться от 12-процентной доли “ВКонтакте”», – написал основатель сети. «Я рад, что достиг своей цели, продав свою долю “ВКонтакте” моему другу И. Таврину» ***(Павел Дуров подтвердил продажу акций «ВКонтакте» // InternetUA (http://internetua.com/pavel-durov-podtverdil-prodaju-akcii--vkontakte). – 2014. – 24.01).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Facebook стає все більше й більше схожим на погані стосунки, від яких треба позбуватися, і якнайшвидше. У пості С. Возз обґрунтована необхідність відмови від Facebook.

1) Ви трохи повернете собі приватне життя.

Налаштування приватності в Facebook зроблені так, що жодна людина не може до кінця зрозуміти, як гарантувати собі шарінг без помилок. Іноді в паблік потрапляє те, що не призначається всім, а іноді крос-постинг може бути тільки для друзів або тільки для вас, хоча ви розраховуєте на широке охоплення. Ще в Facebook про Вас все можуть дізнатись. Раніше, за замовчуванням, ваше ім'я можна було приховати з пошуку, але тепер цю можливість відключили. Як би ви не налаштували свою приватність, ваше ім'я все одно всім буде видно.

Ваша особиста інформація також використовується Facebook для отримання прибутку. Він збирає дані про те, що ви публікуєте, ваші анкетні дані, і ділиться ними з покупцями реклами. А ще він скаже їм, як довго ваш курсор пурхав над їхньою рекламою і в якому місці ви зараз перебуваєте.

Рішення: Видаліть ваш акаунт на Facebook і ви отримаєте більше контролю над тим, що потрапляє в мережу від вашого імені.

2) Покращиться ваше відчуття життя.

Нам здається, що постійний зв'язок зі знайомими, друзями і членами сім'ї має збагатити наше життя... Але дослідження це спростовують. Дослідники з Університету штату Мічиган з'ясували, що чим більше людина проводить часу в мережі Facebook, тим глибше стає її депресія.

Інше дослідження Університету штату Юта доводить, що користувачі Facebook стають дуже незадоволеними своїм власним життям. Цитата: «Ті, хто користувався Facebook довше, погоджувалися, що інші люди набагато щасливіші. Вони стверджували, що життя несправедливе».

Рішення: Припиніть заходити в Facebook і вам не доведеться постійно порівнювати своє життя з життями інших людей.

3) Ви станете більш продуктивним.

Спочатку Facebook стане для вас відмінним інструментом для збереження зв'язку з близькими друзями та членами сім'ї. Потім, із зростанням кількості «друзів», він стане причиною постійного роздратування. Дослідники з Норвегії виділяють кілька рівнів залежності від Facebook.

Згідно зі звітом Social Media дослідницької компанії Nielsen, середньостатистичний американець проводить 6,5 год. на місяць в соціальних мережах, а Facebook домінує в цьому кошику споживання. Блогер M. Fitzpatrick

припускає, що просиджування в Facebook співробітниками на роботі коштує американським компаніям 28 млрд дол. у втратах щорічно.

Рішення: Не заходьте у Facebook, і у вас з'явиться багато вільного часу.

4) Ви не будете заважати своїй кар'єрі.

Занадто просто публікувати в Facebook різні тексти, посилання, картинки та відео. Занадто просто. Вам стало сумно? Публікуйте це в Facebook! І ваші друзі вас підтримають. Проблеми починаються тоді, коли ваші скарги побачить майбутній або поточний роботодавець. Учителька з Джорджії втратила своє робоче місце, коли батько одного з учнів побачив її фото з відпустки в Європі, де вона тримала в руках пінту пива та келих вина. Офіціантка з Північної Кароліни була звільнена після того, як обговорювала поведінку клієнта в Facebook.

Facebook може нашкодити і майбутній роботі. Уже більше половини рекрутерів переглядають профілі в соціальних мережах здобувачів вакансій.

Рішення: Тримайтеся від Facebook подалі і ваша кар'єра піде вгору ***(Психологічна залежність: чому потрібно покинути Facebook? // iМолодь (http://imolod.com.ua/node/4545). – 2014. – 15.01).***

***

Склонность к чрезмерно активному обмену информацией – это болезнь, считают ученые.

Авторы нового исследования, проведенного в Принстоне, воспользовались приемами эпидемиологического моделирования, чтобы обосновать неизбежное угасание популярности этой социальной сети, пишет The Guardian (перевод – Inosmi.ru).

У древних греков была афинская чума, в тюдоровской Англии – потливая горячка, и на протяжении всей истории человечества людей регулярно посещала черная смерть. Сегодня же мы переживаем упадок того, что некоторые эксперты в области медицины назвали социальной болезнью, которой за последнее десятилетие удалось поразить огромное число людей по всей планете.

Согласно результатам нового исследования, которое было проведено в Принстонском университете и авторы которого уподобили Facebook инфекционному заболеванию, эта социальная сеть потеряет около 80 % своих пользователей уже к 2017 г. По оценкам ученых, скоро единственными признаками жизни в Facebook станут авторы рекламы зубных паст, удивляющиеся, почему их никто не лайкает, и Н. Клегг.

Многие ученые скептически отзываются о возможности применить модели динамики болезней по отношению к социальным сетям. Ученые Принстона выстраивают свои аргументы на эпидемиологических моделях, акронимах и огромном множестве формул, где I из уравнений 1b и 1c умножаются на R/N, чтобы получить уравнения 3b и 3c. Честно говоря, это трудно понять. Тем не менее, кажется, что сравнение Facebook с

инфекционным заболеванием вовсе не является натяжкой, и это лишний раз подтверждается высоконаучным медицинским справочным описанием, приведенным ниже.

Лихорадка Facebook

Этиология. Главной причиной развития этого заболевания становятся рекомендации полного энтузиазма приятеля, который уже успел им заразиться. Первопричиной распространения вируса стали заразные особи Harvardus aluminus, паразитов, впервые появившихся в штате Массачусетс, однако в настоящее время его носителями являются миллионы людей. Наиболее целесообразный план действий в этих условиях подразумевает, что вы должны подозревать потенциальных носителей этого вируса во всех окружающих вас людях – даже в своей собственной матери.

Настораживающие признаки. Первым признаком инфицирования становится регистрация в Facebook. Ладно, думаете вы, я с радостью предоставлю свои личные данные владельцам качественно сделанного сайта, потому что это даст мне возможность беспрепятственно обмениваться информацией со своими друзьями. Это вполне разумное желание, которое может не привести ни к каким осложнениям. Однако у большинства пользователей со временем начинают возникать довольно серьезные проблемы.

Основные симптомы. Склонность к чрезмерно активному обмену информацией; неспособность поверить в серьезность своих отношений, если они официально не подтверждены статусом в Facebook; частые пробуждения среди ночи, целью которых является проверка количества лайков, набранных вашим новым статусом, и жгучая ненависть по отношению к самому себе, которую вы испытываете, обнаружив, что единственный лайк вам поставила ваша надоедливая подруга Эмма; прекращение отношений в случае, если вы обнаруживаете, что бывшие вашего друга до сих пор отмечают его на своих фотографиях; непреодолимое желание следить за своим бывшим, отправляющее вас прочесать всевозможные поисковики, откуда вы возвращаетесь ошарашенной, смущенной и несколько пристыженной.

Варианты симптомов. Люди, страдающие тяжелой формой лихорадки Facebook, попадают в довольно немногочисленную, но, тем не менее, статистически значимую группу, носящую название «экспертов социальных сетей». Ими становятся взрослые люди, которые начинают учить других взрослых людей, как можно использовать Facebook, чтобы что-то продавать или оказывать влияние на других. Эксперты часто страдают манией величия и называют себя «ниндзя социальных сетей» или «цифровыми пророками». Старайтесь любой ценой избегать контактов с этими людьми, поскольку это может привести к ухудшению вашего состояния.

Лечение. Согласно результатам исследования принстонских ученых, со временем эпидемия лихорадки Facebook пойдет на спад, потому что постепенно у нас с вами выработается иммунитет к ее соблазнам. Авторы исследования пишут следующее: «Информация распространяется

посредством коммуникативных контактов между различными людьми, которые делятся ей друг с другом. В конце концов, переносчики этой информации теряют к ней интерес, что можно расценивать как развитие “иммунитета” к этой информации». Коротко говоря, Facebook становится скучным и немодным. Спасибо тебе, наука ***(Facebook как инфекционное заболевание // Хартии’97 (http://charter97.org/ru/news/2014/1/26/84914/). – 2014. – 26.01).***

Маніпулятивні технології

На YouTube появился ролик, являющий собой, по словам автора, видеобомбу МВД о беспределе на Евромайдане.

В комментариях к видео сообщается о том, что ни «Интер», ни другие украинские телеканалы так и не решились показать правду глазами и объективами видеокамер правоохранителей, выполнявших присягу.

По словам сотрудника «Беркута», цитируемого автором ролика, «у нас в СМИ все фабрикуют и несут полную ложь, а из милиции и “Беркута” сделали каких-то фашистов». Вся пресса, утверждает сотрудник «Беркута», куплена.

«Никто не показывал поломанные руки и ноги, сотни пробитых шлемов правоохранителей», – отмечает он.

«14 декабря великий манипулятор С. Шустер шустро и наотрез отказался показать в прямом эфире именной программы “Шустер live” оперативное видео МВД. Что скрывал от зрителей С. Шустер? Теперь читатели могут стать зрителями и увидеть наконец-то видео, кадры из которого, наотрез, отказался показывать С. Шустер. Слабонервным не смотреть!» – говорится в подводке к видео ***(На YouTube сбросили видеобомбу от МВД // From-UA. Новости Украины (http://www.from-ua.com/news/69bbf01c262bf.html). – 2014. – 17.01).***

***

16 січня Верховна Рада прийняла закон, у пояснювальній записці до якого йдеться про те, що соціальні мережі в Інтернеті використовуються як високотехнологічний інструмент для розпалювання ворожнечі на соціальному, національному, політичному та мовному ґрунті.

«Там, усе частіше лунають заклики до нетерпимості, ворожнечі, ненависті та насильницької зміни влади та конституційного ладу. Нерідко під виглядом самоорганізації громадян Інтернет використовується для маніпулювання ззовні, у результаті чого відбувається істотне зростання конфліктності, жорстокості, безжальності та насильства серед населення, що призводить до зниження рівня моральності та системного заподіяння шкоди законним правам та інтересам громадян і суспільству, інтересам держави в цілому», – йдеться у пояснювальній записці до законопроекту Колесніченко-

Олійника.

У ній також зазначається, що в соціальних мережах формуються групи, якими надаються детальні інструкції для виготовлення з підручних засобів речовин і предметів, що дають змогу наносити максимальні тілесні ушкодження під час масових заворушень ***(«Регіонали» законодавчо оголосили соцмережі поза законом // Мукачево.net (http://www.mukachevo.net/UA/News/view/86577-Регіонали-законодавчо-оголосили-соцмережі-поза-законом). – 2014. – 16.01).***

***

МТС и «Киевстар» признали, что не контролируют собственные сети мобильной связи.

Мобильный оператор «МТС Украина» никак не причастен к массовой рассылке сообщений участникам акций протеста в центре Киева. Об этом «Капиталу» заявила начальник отдела связей с общественностью компании В. Рубан.

Она заверила, что рассылка производилась с помощью оборудования, которое не принадлежит оператору МТС. В настоящее время оператор ищет пути предотвращения подобных рассылок в будущем.

Напомним, что в ночь с 20 на 21 января 2014 г. абоненты компании «МТС Украина», которые находились на улице Грушевского в Киеве, а также на близлежащих улицах получили SMS с номера 111, содержащие один и тот же текст: «Уважаемый абонент, вы зарегистрированы как участник массовых беспорядков». Согласно действующему законодательству, участие в массовых беспорядках влечет ответственность в виде лишения свободы на срок от пяти до восьми лет, а в некоторых случаях – до 15 лет.

Ранее информацию о своей причастности к аналогичной рассылке опровергли представители компании «Киевстар». «В соответствии с действующим законодательством мы строго придерживаемся условий конфиденциальности информации об абонентах, их номерах телефонов и местонахождении», – говорится в сообщении оператора на странице в социальной сети Facebook.

Представители «Киевстар» утверждают, что оборудование для осуществления таких рассылок (так называемые «пиратские станции») используется злоумышленниками. «Но как оператор мы не имеем технической возможности увидеть деятельность таких станций», – сообщили представители «Киевстар».

Сколько абонентов получили соответствующие SMS, пока не известно ***(МТС и «Киевстар» признали, что не контролируют собственные сети мобильной связи // Укррудпром (http://www.ukrrudprom.ua/news/MTS_i_Kievstar_priznali_chto_ne_kontroliruyut_sobstvennie_seti_m.html). – 2014. – 21.01).***

***

Информация в социальной сети способна распространяться со скоростью лесного пожара: пользователю проще сразу нажать лайк или «поделиться», чем проанализировать содержимое. В ситуации, которая сейчас сложилась в Киеве, сети вроде Facebook и «ВКонтакте» наряду с полезными функциями оповещения часто становятся «рассадником» «фейков», а также питательной средой для информационных вбросов, пишет AIN.UA (http://ain.ua/2014/01/23/509984).

С. Дидковский, PR-стратег «Ашманов и партнеры Украина» сформулировал для AIN.UA простые правила, с помощью которых можно отличить настоящую новость от поддельной, а также рассказал, по какой схеме работают информационные «вбросы».

Существует пять пунктов, по которым настоящую новость можно отличить от «фейка»:

1. Новость должна быть основана на официальном заявлении какой-то стороны. Например, на основе пресс-релиза чиновника или бизнесмена, в идеале – подкрепленного его подписью и печатью. Первоисточником новости должна быть официальная информационная площадка этой стороны (сайт или газета).

2. Сайт или страница в социальной сети, опубликовавшие новость, должны иметь свою историю. То есть, если вы впервые видите некий сайт со странным названием, на котором размещена «сенсационная новость», то нет оснований ему доверять.

3. Использование в новости в качестве источника информации «анонима» дает основания считать ее «фейком».

4. Если новость написана «со слов очевидца», нужно, во-первых, подтвердить его существование, идентифицировать его – для начала хотя бы в соцсетях. Если нет, удостовериться иными способами: сделать запрос автору материала, в котором упомянут свидетель событий. Ведь очевидец, предоставляя информацию, становится публичным человеком. Во-вторых, проверить квалификацию этого пользователя. Например, директор интернет-провайдера с большей вероятностью может знать о тотальном отключении Интернета, чем студент-гуманитарий.

5. Если новость размещают с помощью «ботов», то нет оснований ей доверять. Наряду с ботами часто используют проплаченных «авторов» в социальных сетях, которые говорят заготовленными меседжами, и у которых сотни разных аккаунтов. Они должны вступать с пользователями в дискуссии, иногда провоцировать нужную реакцию.

Как распознать бота?

– Странные имя и фамилия (Аристарх Суровый или Региональный Бандерлог).

– Отсутствие активности в профиле (нет истории коммуникации с другими людьми, подтверждающими реальность человека).

– Излишняя назойливость в распространении информации (спам в комментариях в социальных сетях и блогах, состоящий из однотипных слов и ссылок на некую статью).

– Боты никогда не отвечают на личные сообщения и комментарии.

Информационный «вброс» реализуется так:

1. Определяется «общий враг» и противопоставляемая ему социальная группа (те люди, поведение которых нужно смоделировать).

2. Создается набор понятных для социальной группы меседжей. Каждый меседж должен быть бинарным, то есть, «мы хорошие, а он (враг) – плохой». Меседжи должны быть основаны на непонимании между врагом и группой и изолированностью между социальной группой и врагом. Они, как правило, ориентированы на эмоциональное восприятие, с минимальной рациональной составляющей.

3. Выбирается пул информационных каналов – сайтов, блогов, форумов, социальных сетей – для распространения меседжей.

4. Выбираются лидеры общественного мнения, которые готовы стать первоисточниками для распространения меседжей. Они должны быть представителями социальной группы.

С помощью ботов максимально широко распространяется информация во всех местах, где есть представители социальной группы. «Именно боты впоследствии поддерживают градус интереса, являясь генераторами слухов. Сама механика распространения слуха подразумевает, что в процессе передачи (из уст в уста) слух обрастает дополнительными деталями (домыслами) уже с помощью самих участников группы», – говорит С. Дидковский.

Впоследствии группа, которая восприняла «вброс», принимает любую информацию против общего врага как правдивую ***(Как распознать ботов, фейки и «вбросы» в социальной сети – советы эксперта // AIN.UA (http://ain.ua/2014/01/23/509984). – 2014. – 24.01).***

***

Соціальна мережа «Одноклассники» заблокувала можливість додати посилання на матеріал про Майдан. Про це на своїй сторінці у Facebook написав відомий російський блогер І. Варламов.

Він написав, що не може розмістити посилання на матеріал про події у Києві під назвою «Временное перемирие на Майдане…» у соціальній мережі «Одноклассники». Він також додав, що ніхто інший також не може його опублікувати.

Соціальна мережа «Одноклассники», що була створена у 2006 р., є одним із найбільш відвідуваних сайтів російськомовного сегмента Інтернету ***(«Одноклассники» заблокували посилання на пост блогера Іллі Варламова про Майдан // Медіаграмотність (http://osvita.mediasapiens.ua/material/27064). – 2014. – 24.01).***

Зарубіжні спецслужби і технології «соціального контролю»

В Украине могут начать блокировать сайты за нарушение авторского права.

Государственная служба интеллектуальной собственности Украины в Проекте Закона Украины «О внесении изменений в некоторые законодательные акты по защите авторского права и смежных прав в сети Интернет» предложила довольно противоречивые изменения, об этом сообщает общественная организация «Викимедиа Украина».

Как сообщает пресс-служба организации, обеспокоенность вызывает тот факт, что предлагаемые изменения возлагают на сервисные службы, которые предоставляют услуги по размещению веб-сайтов, обязательства блокировать доступ к ним без необходимости доказательства нарушения авторских прав в суде.

Основанием для такого блокирования, согласно предложенным изменениям, является лишь заявление о нарушении авторских прав на веб-сайте, поступившее в сервисную службу, если в течение трех дней владелец сайта не предоставил письменного ответа на это заявление. При этом достоверность информации, изложенной заявителем в заявлении, не проверяется, и достаточно нотариально заверенного скриншота такой веб-страницы.

«Подобные нормы создают опасность злоупотребления использования таких процедур лицами, которые могут быть недостаточно осведомлены в законах об авторском праве, в частности в отношении свободных лицензий, или иметь целью заблокировать доступ к определенному веб-ресурсу.

Неопределенность понятия «владелец сайта» и требование использования цифровой подписи или заверения нотариусом физической подписи лица создает реальные угрозы для функционирования интернет-сообществ, которые работают по принципу добровольного участия людей в наполнении, поддержании и организации работы сайта», – прокомментировал новые законодательные инициативы член правления ОО «Викимедиа Украина» Ю. Булка.

Любой пользователь может сам разместить в сети информацию нарушающую авторские права, написать жалобу на такое содержание с нотариально заверенным скриншотом, и требовать прекращения доступа к популярному энциклопедическому ресурсу. Более того, любой ресурс можно будет заблокировать, если на нем будет ссылка на сайт, где размещены материалы, нарушающие авторские права ***(В Украине могут начать блокировать сайты за нарушение авторского права // Finance.Ua (http://news.finance.ua/ru/~/1/0/all/2014/01/13/316629B). – 2014. – 13.01).***

***

Терористична ісламістська організація Al-Shabaab заборонила користуватися Інтернетом населенню зон Сомалі, що перебувають під її контролем. Про це повідомили «Репортери без кордонів» (RSF).

Бойовики висунули ультиматум усім провайдерам Сомалі, які забезпечують доступ до світової мережі, – у 15-денний термін відключити сервіси. Проти тих, хто не виконає цю заборону, передбачено санкції. «Кожна компанія чи особа, які нехтуватимуть цим наказом, вважатиметься колабораціоністською. Ставлення до неї визначатиметься законами шаріату», – застерігають бойовики Al-Shaab.

Репортери без кордонів розцінили дії ісламістської міліції як «безпрецедентний наступ проти свободи інформації», що має на меті «знищити інформаційну платформу та будь-які комунікації», «відрізати захоплені території від решти Сомалі та світу, приректи їх на мовчання». «Особливу тривогу викликає те, – наголошує організація, – що Al-Shabaab вважає мобільний Інтернет знаряддям порушення приватного життя у той час, як для нас доступ до Інтернету – це фундаментальне право, закріплене Об'єднаними Націями».

Стратегія Al-Shabaab, яка фігурує у списку RSF «Хижаків за свободою інформації» (les Prйdateurs de la libertй d'information), не нова. Це контроль населення, методом позбавлення його інформації. Вона визначається також військовими поразками. Їх в останні два роки ісламістські бойовики зазнали від урядової армії, яку підтримує військовий контингент Африканського Союзу.

«Репортери» нагадують, що раніше бойовики Al-Shabaab захопили місто Бараве та вимагали від його мешканців здати місцевій владі телевізори. Сомалійці широко користуються Інтернетом, особливо у смартфонах. Однак ісламісти вважають його знаряддям шпигунства ***(Ісламісти Al-Shabaab оголосили війну Інтернету // Телекритика (http://www.telekritika.ua/svit/2014-01-12/89200). – 2014. – 12.01).***

***

Х. Вэйфан, один из наиболее известных «публичных интеллектуалов» континентального Китая, 31 декабря простился со своим блогом на «Сина Вэйбо». Таким образом число крупных политических мыслителей, участвующих в онлайн-дебатах в китайских социальных сетях, сократилось еще больше.

«В прошлом году я наблюдал за тем, как знакомые блогеры уходят один за другим, и не мог не почувствовать огорчения, – написал он в своем микроблоге 31 декабря. – Пришло время закрыть этот блог. До свидания», – заключил он.

Х. Вэйфан, преподаватель права в Пекинском университете, по телефону сообщил South China Morning Post, что ему «не давали покоя» постоянные

оскорбления и ругательства, оставляемые леваками в его микроблоге.

На блог Х. Вэйфана подписано более 1,1 млн человек. В последнее время все больше выдающихся лидеров общественного мнения, известных как «публиные интеллектуалы», переходит в режим молчания из-за войны с инакомыслием, развязанной правительством. Решение Х. Вэйфана прекратить участие в онлайн-дебатах лишь подтверждает эту тенденцию.

После ряда арестов в августе, Верховный народный суд КНР постановил, что любая клеветническая запись в Интернете, которую опубликуют на своих страницах более 500 пользователей или которая будет прочитана более 5 тыс. раз, может быть основанием для заключения автора под арест.

Некоторые видные комментаторы, такие как венчурные предприниматели Ч. Бицюнь и В. Гунцюань, в результате были взяты под стражу. Другие, как историк Ч. Лифань, лишились своих учетных записей.

К своей прощальной записи Х. Вэйфан прикрепил изображение Т. Юаньмина, поэта древности, ушедшего с правительственной службы в знак протеста против царившей там коррупции. Являясь одной из публичных фигур, подписавших Хартию-08 лауреата Нобелевской премии мира Л. Сяобо, он не раз призывал к укреплению роли конституции и проведению политических реформ.

«Коммунистическая доктрина неизбежно ведет к рабству, потому что она лишает людей права на свободное мышление и выражение мыслей – и эти проблемы так и не были разрешены должным образом», – сказал Х. Вэйфан в своем октябрьском интервью нашему изданию.

Сотни интернет-пользователей выразили сожаление по поводу его решения покинуть социальные сети. «Как много умао потеряют свою работу с уходом Х. Вэйфан?» – спросил с иронией один из них, намекая на состоящих на службе у правительства левых авторов, нападающих в Интернете на «публичных интеллектуалов», подобных Х. Вэйфану ***(Боэлер П., Чжоу Л. Выдающийся мыслитель Хэ Вэйфан говорит «прощай» дискуссиям в Интернете (South China Morning Post, Гонконг) // ИноСМИ.ru (http://inosmi.ru/world/20140113/216477895.html). – 2014. – 13.01).***

***

Агентство національної безпеки (АНБ) США таємно встановило приблизно на 100 тис. комп’ютерів по всьому світу спеціальне програмне забезпечення, що дає змогу отримувати доступ до них, а також спрощує вчинення кібератак. Про це повідомила 14 січня електронна версія американської газети «Нью-Йорк таймс».

Згідно з документами, наданими газеті колишнім співробітником ЦРУ Е. Сноуденом, а також інформації, отриманій виданням від офіційних осіб США та експертів у галузі комп’ютерних програм, АНБ, зокрема, використовувало секретну технологію, яка дає змогу «зламати» навіть ті комп’ютери, які не підключені до Інтернету. У такий спосіб, за відомостями

газети, активно користуються в АНБ з 2008 р. в рамках програми «Квантум» (Quantum). Він передбачає використання радіохвиль, які випускаються спеціальними мініатюрними пристроями, зокрема, що підключаються до комп'ютера через USB-порт.

«Технологія, заснована на використанні радіохвиль, допомогла вирішити одну з найбільших проблем, що стояли перед американськими розвідувальними службами, – проникнення в ті комп'ютери, які противники, а також деякі партнери США, намагалися зробити невразливими для шпигунства або кібератак», – вказує газета.

«У більшості випадків пристрої, що випускають радіохвилі, повинні бути фізично підключені шпигуном, виробником (комп'ютерного обладнання) або ж користувачем, якій нічого не підозрює», – підкреслює газета.

Вона також вказує, що використовувані АНБ програми показали свою ефективність в проникненні в комп'ютерні мережі, використовувані російськими військовими, мексиканською поліцією і наркокартелями, торговими організаціями Євросоюзу, а також різними структурами в КНР, Саудівській Аравії, Індії та Пакистані.

«Новим у цьому випадку є те, наскільки потужними і витонченими інструментами для проникнення в комп'ютери і мережі володіє розвідувальне агентство (АНБ), – вказав експерт американського Центру стратегічних і міжнародних досліджень Е. Льюіс.

Частина цих технологій була доступна вже деякий час, проте поєднання методів проникнення в комп'ютери і мережі з метою установки програм, а також використання для цього радіохвиль, надало Сполученим Штатам небачені раніше можливості» ***(ЗМІ: Спецслужби США встановили шпигунські програми на 100 тис. комп'ютерів у світі // Західна інформаційна корпорація (http://zik.ua/ua/news/2014/01/15/zmi_spetssluzhby_ssha_vstanovyly_shpygunski_programy_na_100_tys_kompyuteriv_u_sviti_452892). – 2014. – 15.01).***

***

Агентство национальной безопасности (АНБ) США перехватывало до 200 млн SMS-сообщений в день по всему миру, пишет газета The Guardian со ссылкой на документы, переданные журналистам бывшим сотрудником АНБ Э. Сноуденом. В результате обработки текстовых сообщений АНБ получало сведения о местоположении абонентов и номерах кредитных карточек. Какой-либо конкретной цели перехват сообщений, вероятно, не имел.

Для перехвата текстовых сообщений использовалась программа Dishfire. Она отвечает за сбор любой доступной с абонентского устройства информации. В частности, в Агентство национальной безопасности передавались данные о перемещении абонентов сотовых сетей, об их туристических планах, телефонных книгах и денежных переводах. При этом перехвату подлежали сообщения даже с телефонов тех людей, которые никогда не подозревались в

каких-либо незаконных действиях.

Ранее сообщалось, что АНБ использовало специальное радиооборудование для заражения компьютеров и перехвата информации с них. В общей сложности были заражены по меньшей мере 100 тыс. компьютеров по всему миру, которые могут быть объединены в сеть для организации кибератаки. В большинстве случаев установка оборудования в компьютер-жертву осуществлялось агентом АНБ или производителем.

Между тем, президент США Б. Обама намерен ограничить программу АНБ по отслеживанию телефонных звонков. В первую очередь ограничения коснутся правил слежки за телефонными переговорами иностранцев ***(Спецслужбы США перехватывали 200 миллионов SMS в день // InternetUA (http://internetua.com/specslujbi-ssha-perehvativali-200-millionov-SMS-v-den). – 2014. – 17.01).***

***

Медіа-експерт, юрист Т. Шевченко допускає, що в результаті принятих 16 січня законів влада може заборонити соціальну мережу Facebook. Таку думку він озвучив на прес-конференції, передає кореспондент «Страйку».

«Я не виключаю, що за цим законом (закон, що стосується обмеження ЗМІ. – Ред.) достаньо одного дня, щоб заборонити Facebook в Україні, як він заборонений в Туркменістані, як влада перед виборами в Таджикістані зробила це рік тому, через те, що в таджицьких медіа почали активно обговорювати відео, де були зняті розкоші одного з родичів президента на розкішному весіллі…Тому за цим законом, без суду – один день і Facebook заборонений», – пояснив експерт.

Водночас Т. Шевченко наголосив, що існують способи обійти це рішення, заходячи на Facebook через додатки на смартфоні. «Але основне рішення може бути ухвалене», – додав він.

Однак, експерт вважає, що свободу слова таким чином не спинити і все одно люди будуть знаходити інші можливості спілкування в Інтернеті ***(Влада може заборонити Facebook // Страйк UA – Первый социальний портал (http://www.socportal.info/news/vlada-mozhe-zaboroniti-facebook-ekspert). – 2014. – 20.01).***

***

Російський депутат із Санкт-Петербурга В. Мілонов запропонував ввести штрафи за створення фальшивих акаунтів у соціальних мережах.

Згідно з його проектом закону, за фейкові акаунти передбачаються штрафи від 5 до 10 тис. р. Водночас, за даними «Фонтанки», максимальний розмір штрафу для юросіб становитиме 2 млн р.

Крім того, в ініціативі В. Мілонова передбачено покарання за заклики до створення фальшивих акаунтів у соцмережах – до 5 млн р. для юросіб.

Необхідність введення закону В. Мілонов пояснив тим, що деякі піартехнологи можуть безкарно створювати акаунти від імені посадових осіб і поширювати через них неправдиву інформацію.

«Сьогодні в терористичній діяльності використовуються не тільки бомби, але й інформаційні бомби. Від фейкових акаунтів поширюється різна інформація, і якщо там немає закликів, наприклад, до насильства, такі автори залишаються в числі хуліганів», – акцентував В. Мілонов.

Зазначимо, що з аналогічною пропозицією депутат уже виступав у серпні 2013 р. Тоді він говорив про необхідність введення відповідальності за поширення в соцмережах неправдивої інформації, але до закону справа не дійшла ***(В Росії збираються штрафувати за створення фейкових акаунтів у соцмережах // ТСН.ua (http://tsn.ua/nauka_it/v-rosiyi-zbirayutsya-shtrafuvati-za-stvorennya-feykovih-akauntiv-u-socmerezhah-330015.html). – 2014. – 17.01).***

***

Ученые из Университета Абердина в Шотландии обнаружили, что попытки законодательно ограничить пользователей в социальных сетях изменяют их поведение, но не нарушает структуры сети и возможность распространения информации. Исследование опубликовано в журнале Europhysics Letters, кратко о нем можно прочитать на сайте Phys.Org

Объектом исследования стали канадские пользователи Twitter во время студенческих протестов вначале 2012 г. Недовольство, вызванное резким повышением стоимости обучения в колледжах, привело к забастовке, в которой участвовало около 75 % всех студентов в Квебеке. Канадские власти, пытаясь остановить протесты, приняли «Специальный закон 78». Среди прочего, он обязывал организаторов массовых мероприятий сообщать о них властям как минимум за восемь часов до начала и предусматривал большие штрафы за распространение информации о несогласованных мероприятиях.

Ученые проанализировали, как менялось поведение пользователей Twitter до и после принятия закона 18 мая 2012 г. Оказалось, что закон значительно поменял поведение пользователей – рост сообщений с «протестными» хэштегами перешел в падение, хотя общее число сообщений было выше, чем до принятия закона. Кроме того, общение стало более кластеризованно: пользователи опасались нового закона и предпочитали общение в узких группах.

Однако, указывают авторы, все это не изменило общей структуры социальной сети и ее безмасштабной природы. Студенты по-прежнему могли обмениваться информацией через наиболее популярных пользователей, которые выступали в роли ключевых узлов сети.

Ученые не впервые исследуют поведение социальных сетей во время тех или иных протестов. Так, анализ микроблогов сторонников движения «Захвати Уолл-Стрит» показал, что даже после спада протестной активности пользователи стали чаще обсуждать экономические вопросы. Недавно другая

группа исследователей определила с помощью подобного анализа активности американских пользователей Twitter основные центры генерации обсуждаемых тем в США.

В России поправки, внесенные президентом 8 июля 2012 г., разрешают распространение информации о массовых мероприятиях только «с момента их согласования» ***(Социальные сети оказались устойчивы к репрессивному законодательству // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/sotsialnye_seti_okazalis_ustoychivy_k_repressivnomu_zakonodatelstvu). – 2014. – 22.01).***

***

Многие уверены, что они за ними не следят. Напрасно, ведь большинство из нас сегодня так или иначе, на работе или дома, используют компьютеры.

При посещении многих веб-страниц вам сразу сообщат IP-адрес компьютера, а заодно расскажут, в какой стране и в каком городе вы находитесь. Большинство людей не считают нужным «шифроваться» при помощи специальных программ, маскируя свой IP. Таким образом, отследить местоположение конкретного пользователя в конкретный момент времени достаточно просто.

Но как установить соответствие – то есть узнать, что именно этот посетитель заходил на любимый форум или сайт, например, с турецкого IP-адреса, а теперь пользуется немецкими IP? Нужно выбрать учетную запись в Интернете, которая принадлежит лично человеку, и установить корреляцию. Наиболее простое решение – проследить, с каких IP-адресов пользователь заходит на свой почтовый аккаунт. Уж в него-то обычно никого не пускают, кроме прямого владельца.

Однако отслеживание IP-адреса – далеко не единственный способ присмотреть за пользователем в Сети. Федеральная налоговая администрация Бельгии даже не скрывает, что приглядывает за профилями граждан через популярные в этом государстве социальные сети – Facebook, Netlog и др.

И хотя официально полученные таким путем данные использовать нельзя, но можно неофициально. Например, гражданин похвастался дорогим автомобилем. Налоговая сопоставит с официальными доходами владельца данные о стоимости автомобиля и местах отдыха. Просматривается даже стоимость покупок на eBay – это тоже свидетельствует о реальных доходах.

Что уж говорить о личных сведениях и заметках, которые многие из нас публикуют в социальных сетях? Многие, не задумываясь, оставляют там свой домашний адрес, номер телефона, место работы и т. д.

Приложение Foursquare предлагает пользователям указывать свои перемещения в реальном времени, и многие охотно пользуются этой «прекрасной возможностью». По фотографиям человека и местам, которые он посещает, можно составлять его характеристику: хобби, уровень дохода, наличие машины, загородного дома и пр. Словом, если человек активен в

социальной сети, и кому-то вздумается собрать о нем информацию, это существенно облегчит задачу.

Мобильные телефоны – тот еще кладезь информации. Тем более часто мы сами, еще раз подчеркну – сами, отдаем эту информацию! Храним в телефоне маршруты передвижения, телефоны, адреса друзей, а если это смартфон, то и электронную почту, и т. д.

Когда многие из нас устанавливают приложения, очень часто мы даже не задумываемся о том, какие права просит у нас то или иное приложение. Вспомните некогда популярное приложение Angry Birds. Зачем ему нужны наши координаты? Причем они отслеживаются, даже если приложение не запущено.

Неприкосновенность личной жизни – уже давно фикция. Как с этим жить? Да как обычно. Если вы кому-то нужны, за вами будут смотреть. И ничего вы с этим не сделаете.

Впрочем, есть небольшое утешение: следить за всеми – нереально. Потому расслабьтесь и получайте удовольствие. «Улыбайтесь, вас снимают!» ***(Интернет-приватности нет, и никогда не будет // Николаевский Обозреватель (http://obzor.mk.ua/nikolaevskie-novosti/6915-internet-privatnosti-net-i-nikogda-ne-budet.html). – 2014. – 26.01).***

***

В российском сегменте анонимной сети Tor нашли узлы, способные перехватывать интернет-трафик и отслеживать активность пользователей в Facebook. Узлы были обнаружены в ходе эксперимента, проведенного учеными из шведского университета в Карлстадте (Karlstad Studentkar Karlstads Universitet).

Для проведения эксперимента был разработан специальный сканер, способный выявлять в Tor подозрительные узлы. В общей сложности за четыре месяца исследователями удалось собрать информацию по всем существующим в анонимной сети узлам (их около тысячи). После окончания эксперимента код сканера выложили в открытый доступ.

В итоге потенциально опасными оказались 25 внешних узлов. 18 из них имели российский IP-адрес. При этом все российские узлы и еще один, располагавшийся на территории США, по мнению исследователей, принадлежали к одной сети и управлялись одной группой хакеров. В основном все они были нацелены на сбор информации о посещении пользователями конкретных ресурсов, а не на массовую слежку за их действиями. Например, злоумышленниками отслеживались заходы на Facebook. В то же время, как говорится в исследовании, за российским поисковиком Mail.ru и социальной сетью «ВКонтакте» слежки не обнаружено.

Как отмечают авторы эксперимента, эффективность работы обнаруженных узлов не представляет серьезной угрозы для пользователей Tor. «Чаще всего, человек будет направляться на тот узел, пропускная способность

которого выше. У “испорченных” узлов такая способность невысока. Вероятность попадания на них пользователя крайне мала», – пояснили ученые.

С другой стороны, принцип, по которому работают узлы (подмена подписи в SSL-сертификатах) не является чем-то уникальным для сети Tor. Подобные методы могут, к примеру, использоваться и для отслеживания интернет-активности устройств, подключенных к открытым сетям Wi-Fi.

Анонимность в сети Tor достигается благодаря тому, что подключение к тому или иному ресурсу идет через цепочку промежуточных серверов. Таким образом, определить IP-адрес и местоположение использующего Tor человека становится довольно сложно. Благодаря своей анонимности Tor пользуется популярностью у интернет-активистов, хакеров, а также пользователей, живущих в странах, контролирующих и фильтрующих интернет-трафик. Кроме того, в так называемой скрытой зоне Tor (Tor Hidden Services) располагаются центры управления ботнетами (сетями зараженных компьютеров), сайты с порнографическим контентом и многочисленные ресурсы, предлагающие противозаконные товары. В частности, в такой зоне размещался закрытый в 2013 г. ФБР онлайн-рынок наркотиков Silk Road ***(В российском сегменте сети Tor нашли следящие за Facebook узлы // InternetUA (http://internetua.com/v-rossiiskom-segmente-seti-Tor-nashli-sledyasxie-za-Facebook-uzli). – 2014. – 22.01).***

***

Американская компания CrowdStrike включила Россию в список стран, активно занимающихся шпионажем на глобальном рынке. По данным аналитиков, российская хакерская группировка Energetic Bear виновна в атаках на 23 страны мира, включая США и государства Европы. Используя уязвимости в Windows XP, хакеры крадут информацию, которая способствует укреплению России на международной арене.

Калифорнийская компания CrowdStrike, специализирующаяся на технологиях защиты информации, назвала Россию одним из главных агрессоров в мировом киберпространстве. В частности, в компании сообщили о хакерской группировке Energetic Bear, виновной в атаках на энергетический сектор США, Европы, Турции, Японии и Китая.

Сооснователь и технический директор компании CrowdStrike – бывший вице-президент McAfee по исследованию угроз безопасности Д. Альперович (Dmitri Alperovitch). Подробности о заявлении CrowdStrike опубликовала газета The Washington Post.

В общей сложности жертвами Energetic Bear стали десятки частных компаний и госведомств в 23 странах мира. Характер целей и способы проведения атак говорят о том, что группировка связана с российскими государственными структурами. По данным исследователей, Energetic Bear функционирует с августа 2012 г.

Как рассказал А. Мейерс, вице-президент CrowdStrike, хакеры Energetic

Bear охотятся за информацией, которая может быть полезна в политической и дипломатической деятельности, так или иначе связанной с энергоресурсами.

На компьютеры в чужих государствах хакеры проникают с помощью вирусов, распространяемых через веб-сайты, которые посещают потенциальные жертвы – сотрудники зарубежных предприятий и организаций.

После того как жертва заходит на веб-сайт, на компьютер загружается вредоносное программное обеспечение. Используя уязвимости в операционной системе Microsoft Windows XP, оно предоставляет хакерам удаленный доступ к системе, после чего они получают возможность загрузки ценной информации.

Ситуация усугублена тем фактом, что с 8 апреля 2014 г. Microsoft планирует прекратить дальнейшее обновление Windows XP. Эта система по-прежнему установлена примерно на 20 % персональных компьютеров во всем мире.

«Россия является источником самых заметных интернет-атак», – говорится в отчете CrowdStrike. В компании, тем не менее, признаются, что не располагают конкретными доказательствами своих утверждений. Все, что они имеют, – это свидетельство связи командно-контрольных центров ботнетов с серверами, расположенными в России.

В любом случае это одно из первых публичных заявлений, в котором в проведении кибератак обвиняют Россию. Ранее, как правило, аналогичные претензии адресовались Китаю, отмечает The Washington Post.

Помимо России и Китая, в список главных агрессоров в киберпространстве вошли Сирия и Иран.

«Новый отчет представляет собой нечто большее по сравнению с традиционными отчетами о кибер-угрозах, – заявил Д. Альперович. – Мы сфокусировались на том, что наиболее важно – враге, – а не на вирусах, которые они создают. Мы считаем, что гораздо важнее знать врага в лицо, чем заниматься обнаружением вредоносного кода» ***(Россию обвинили в глобальном кибершпионаже // InternetUA (http://internetua.com/rossiua-obvinili-v-globalnom-kibershpionaje). – 2014. – 23.01).***

Проблема захисту даних. DOS та вірусні атаки

Разработана система оценки наиболее подходящего времени для нанесения кибердудара с использованием скрытых уязвимостей в компьютерных программах. Модель идеальной кибератаки приводится в статье, опубликованной американскими исследователями в журнале PNAS.

Эффективность атак на компьютерные системы потенциального противника авторы работы рассмотрели на примере так называемых эксплойтов – скрытых уязвимых мест в коде программ и операционных систем. Их модель основана на учете двух основных параметров: вероятности, что

эксплойт не будет обнаружен до его применения, и времени, в течение которого уязвимость можно будет использовать уже после атаки, пишет NewsOboz.org со ссылкой на Lenta.ru.

Влияние этих факторов является взаимоисключающим, поскольку использование никому не известной уязвимости можно отложить, а хорошо замаскированный эксплойт лучше применить сразу, чтобы дольше иметь доступ к системам противника.

Примером успешного использования скрытной уязвимости авторы работы назвали внедрение вируса Stuxnet на компьютеры иранских ядерных объектов в 2010 г. Вирус помешал работе центрифуг для обогащения ядерного топлива. Stuxnet успешно работал в течение 17 месяцев и, по мнению исследователей, был запущен как только появилась такая возможность для достижения максимального результата.

Предполагаемый ответ Ирана, в свою очередь, стал образцом поспешного использования недостаточно хорошо замаскированного эксплойта. Вирус поразил десятки тысяч рабочих станций саудовской нефтяной компании Saudi Aramco, но был замечен и удален в течение четырех дней.

В 2013 г. стало известно, что Агентство национальной безопасности США скупало данные об уязвимостях интернет-сайтов, которые можно использовать для несанкционированного доступа к компьютерам ***(Американские ученые разработали модель идеальной кибератаки // NewsOboz (http://newsoboz.org/it_tehnologii/amerikanskie-uchenye-razrabotali-model-idealnoy-kiberataki-15012014014500). – 2014. – 15.01).***

***

Официальные ресурсы украинской греко-католической церкви атакуют неизвестные хакеры, об этом на своей странице в Facebook сообщил советник УГКЦ отец И. Яцив, сообщает радио «Свобода». «Мы удостоились еще одной “чести”. На ресурсы УГКЦ происходят DOS-атаки. Наши сайты недоступны. 6000 одновременных подключений», – написал И. Яцив.

Об атаке он сообщил еще 15 января поздно вечером, но и по состоянию на утро 16 января сайт www.ugcc.org.ua остается недоступным. Напомним, 13 января глава Украинской греко-католической церкви Блаженнейший Святослав сообщил о письме из Министерства культуры Украины, в котором заместитель министра Т. Кохан сообщает УГКЦ о «нарушении требований законодательства Украины о свободе совести и религиозных организациях» и добавляет, что это «может служить основанием для возбуждения перед судом вопроса о прекращении деятельности соответствующих религиозных организаций» ***(Советник УГКЦ заявляет, что сайт церкви атакуют хакеры // 112.ua (http://112.ua/obshchestvo/sovetnik-ugkc-zayavlyaet-chto-sayt-cerkvi-atakuyut-hakery-10888.html). – 2014. – 16.01).***

***

По сети стремительно расползается новость о найденной дыре в системе восстановления пароля социальной сети «ВКонтакте», введя номер мобильного телефона можно получить имя и аватар человека, зарегистрировавшегося под этим номером в социальной сети.

Воспользоваться этой «телефонной книгой» элементарно:

1. Заходим на мобильную версию сайта m.vk.com.
2. Жмем «Забыли пароль?».
3. Вводим номер телефона.
4. Получаем имя и аватар.

Иногда надо ввести капчу.

Дело за малым – пока дыра активна отправить самую большую базу телефонных номеров России и СНГ ***(Дыра «ВКонтакте»: утечка персональных данных пользователей // InternetUA (http://internetua.com/dira-vkontakte--utecska-personalnih-dannih-polzovatelei). – 2014. – 16.01).***

***

Прес-служба Партії регіонів заявляє, що 16 січня офіційний партійний сайт зазнав масової хакерської атаки. Про це йдеться в заяві прес-служби.

«Таким примітивним чином у день ухвалення Верховною Радою найважливішого для країни документа – Державного бюджету на 2014 р. – наші політичні опоненти намагаються обмежити право доступу користувачів Інтернету і представників мас-медіа до достовірної та оперативної інформації», – переконані у ПР.

Прес-служба Партії регіонів звертає увагу на те, що дії хакерів порушують Конституцію України.

«На цей час ми докладаємо всіх зусиль для усунення наявних проблем. Однак певний час через DDoS-атаки в роботі сайту можливі збої», – додає ПР ***(Сайт Партії регіонів атакують хакери // Телекритика (http://www.telekritika.ua/kontekst/2014-01-16/89340). – 2014. – 16.01).***

***

Миллионы Twitter-совместимых приложений, применяющих в работе данные Twitter, должны будут шифровать их коммуникации с интерфейсом Twitter API.

Это позволит повысить безопасность и поддерживать целостность данных. В кратком сообщении в блоге Twitter говорится, что система принудительного шифрования коммуникаций заработала с 14 января и все API-функции должны исполняться через SSL-протокол или через его дальнейшее развитие – протокол TLS, сообщает CyberSecurity.

«Подключение к API через SSL позволяет создать безопасный коммуникационный канал между нашими серверами и вашим приложением.

Это значит, что никакие закрытые данные не могут быть перехвачены неавторизованным агентом, находящимся посередине коммуникационного канала», – пишет в блоге Twitter Л. Киприани, специалист по коммуникациям Twitter.

Он напомнил, что о принудительном шифровании было впервые объявлено еще в декабре.

Интернет-компании Facebook и Google начали шифровать API еще в 2011 г.

Согласно статистике, на сегодня более миллиона приложений зарегистрированы на использование API-функций Twitter. Сама сеть Twitter предлагает различные услуги через API, в том числе индивидульные ленты сообщений, агрегаторы, анализаторы трендов и др. В компании говорят, что запрос данных у Twitter в большинстве случаев ранее производился через простые HTTP-запросы, тогда как теперь обязательно применение HTTPS.

Разработчики программного обеспечения на популярных языках веб-разработки, таких как Python, PHP и Ruby, должны будут работать с системными библиотеками, которые управляют SSL-инициализацией ***(Twitter начинает шифровать данные по API // proIT (http://proit.com.ua/news/internet/2014/01/16/125844.html). – 2014. – 16.01).***

***

Как выяснили эксперты в сфере информационной безопасности из Microsoft, троян Sefnit, модификация которого стала причиной всплеска трафика в сетях анонимизатора Tor в октябре прошлого года, до сих пор представляет угрозу для пользователей.

Напомним, что получивший название Mevade ботнет (создан на базе Sefnit) использовал сервис для передачи данных с инфицированных систем на C&C-серверы злоумышленников. При этом количество зараженных пользователей достигало 4 млн человек.

В настоящее время Microsoft предпринимает активные усилия для того, чтобы демонтировать данный ботнет. Среди прочего эксперты компания добавили сигнатуры угрозы в свои антивирусные решения для Windows.

Вместе с тем в компании подчеркивают, что несмотря на удаление вируса на зараженной системе все еще остается установленным Tor версии 0.2.3.25, в котором отключена функция автоматического обновления. Таким образом, в случае обнаружения опасных брешей в данной программе ее пользователи могут вновь пострадать.

В настоящее время, по данным Microsoft, в Tor 0.2.3.25 не обнаружено каких-либо уязвимостей, позволяющих удаленное выполнение кода ***(Троян Sefnit – угроза для пользователей даже после удаления // InternetUA (http://internetua.com/troyan-Sefnit---ugroza-dlya-polzovatelei-daje-posle-udaleniya). – 2014. – 14.01).***

***

Зловмисники зламали аккаунт С. Власенка у Twitter.

Прес-служба партії «Батьківщина» повідомляє, що влада продовжує провокації проти представників опозиції.

21 січня зламано сторінку в соціальній мережі Twitter захисника лідера опозиції Ю. Тимошенко С. Власенка.

С. Власенко повідомив, що сторінкою не користується вже кілька років і просить журналістів і громадськість не реагувати на фальшиві повідомлення у Twitter, які нібито надходять від його імені й до яких він не має жодного відношення.

Прес-служба також нагадує, що це не перший випадок, коли зловмисники від влади намагаються захопити сторінки представників опозиції в соціальних мережах. У листопаді про захоплення сторінки в Facebook повідомляла прес-секретар Ю. Тимошенко М. Сорока ***(Аккаунт С. Власенка у Твіттері – зламали!? // JeyNews (http://jeynews.com.ua/news/d0/81442). – 2014. – 21.01).***

***

20 січня на хостинг провайдера «Телекритики» компанії DreamLine було здійснено DDoS-атаку. Про це компанія-провайдер повідомила ІТ-відділу каналу «1+1».

DDoS-атака тривала близько 2 год. Сайти «Телекритика», tsn.ua й групи «1+1 медіа», які мають хостинг у провайдера DreamLine, час від часу не завантажувалися.

Провайдер DreamLine запевняє, що робить усе можливе, щоб відновити повноцінну роботу інтернет-видань ***(На провайдера «Телекритики» і ТСН здійснюється DDoS-атака // Телекритика (http://www.telekritika.ua/rinok/2014-01-20/89494). – 2014. – 20.01).***

***

Согласно отчету компании Prolexic Technologies, начиная с 4 квартала 2013 г., мобильные приложения стали чаще использоваться при проведении DDoS-атак в корпоративном секторе.

«Превосходящее количество мобильных устройств и написанных для них приложений, которые используются при проведении DDoS-атак, стало ключевым моментом в изменении правил игры, – отмечает С. Чоли, президент Prolexic. – Вирусописатели теперь получили могущественный инструмент, для использования которого требуются минимальные навыки. Учитывая тот факт, что мобильные устройства очень легко могут использоваться при проведении такого типа атак, в 2014 г. мы ожидаем всплеск активности хакеров именно в этом сегменте».

Согласно данным отчета, собранным в ходе отражения ряда атак на клиентов Prolexic по всему миру, в 2013 г. мобильные устройства

использовались в проведении DDoS-атак на крупные финансовые корпорации. К примеру, аналитики компании установили, что пользователи устройств под управлением Android стали жертвами инструмента AnDOSid, который способен отправить огромное количество HTTP POST-запросов.

По словам эксперта, использование мобильных устройств при проведении атак усложняет исследования. «Дело в том, что мобильные сети используют огромное количество прокси-серверов, поэтому нельзя при помощи аппаратного обеспечения заблокировать IP-адрес источника атаки, не затронув легитимный трафик, – отметил С. Чоли. – Более того, высокая популярность мобильных устройств позволяет злоумышленнику активно проводить DDoS-атаки. Чтобы понять масштабы угрозы, достаточно проанализировать статистические данные по количеству мобильных устройств в мире» ***(Мобильные приложения используются для проведения DDoS-атак // InternetUA (http://internetua.com/mobilnie-prilojeniya-ispolzuuatsya-dlya-provedeniya-DDoS-atak). – 2014. – 18.01).***

***

Компания Microsoft в этом году несколько раз подвергалась успешной атаке хакерами из группировки «Сирийская электронная армия». Они взломали Twitter-аккаунты Skype и Xbox, блоги Skype и Microsoft, электронную почту сотрудников Microsoft, а 21 января дефейснули блог Office.

В начале января сирийцы получили доступ к Twitter-аккаунту и блогу Skype. Под аккаунтом Skype хакеры разместили запись, в которой призвали кого-то (вероятно, Microsoft) перестать шпионить за людьми, а под своим аккаунтом выложили в открытый доступ номер телефона С. Балмера с предложением поблагодарить его за слежку.

Чуть позже хакеры разместили твит с призывом к пользователям отказаться от почтовых служб Hotmail и Outlook, поскольку Microsoft якобы собирает данные о своих пользователях и продает их властям.

Спустя две недели сирийцы взломали сайт microsoft.com, блог Microsoft, Twitter-аккаунт Xbox и учетные записи нескольких сотрудников компании. Взлом почты, как призналась Microsoft, производился банально: злоумышленники разослали письма со ссылкой на троян, подождали, пока кто-нибудь перейдет по ней и завладели аккаунтами. Ничего интересного они там не нашли, но пообещали продолжить атаку.

21 января хакеры совершили очередной взлом – жертвой стал официальный блог Office. Никакой смысловой нагрузки, кроме сообщения, собственно, о взломе он не нес.

Цели сирийцев становятся все более и более туманны, но хакеры показывают одну важную вещь – взломать можно все, даже одну из самых крупных корпораций в мире. Можно не сомневаться, что взломы продолжатся ***(Microsoft беззащитна перед хакерами // InternetUA (http://internetua.com/Microsoft-bezzasxitna-pered-hakerami). – 2014. – 22.01).***

***

Крупнейшая в мире соцсеть Facebook позволяет узнать имя и аватар пользователя по номеру телефона – для этого достаточно ввести этот номер в строку логина и нажать на ссылку «Забыли пароль?».

Ранее в сообществе habrahabr.ru появилась информация, что при вводе мобильного номера в систему восстановления пароля в соцсети «ВКонтакте» можно получить имя и аватар человека, который зарегистрировался под этим номером. В результате злоумышленники могут создать базу данных телефонных номеров и имен пользователей. В настоящее время действие этой функции ограничено – следующим шагом после ввода номера соцсеть требует указать фамилию пользователя, и только после этого отображает его имя и аватар.

Аналогичная функция восстановления пароля по номеру телефона есть и на Facebook, но эта соцсеть сразу же выдает полное имя и аватар пользователя. Даже если имя не настоящее, потенциальный злоумышленник может воспользоваться поиском по картинке, который поддерживают Google, «Яндекс» и другие поисковики. Также Facebook предлагает три способа для восстановления пароля – отправить ссылку на e-mail, отправить SMS с кодом на мобильный номер, получить код на смартфон.

Работа этой функции не затронет пользователей Facebook, которые не привязали номер телефона к аккаунту – эта опция в соцсети необязательна. В свою очередь, «ВКонтакте» с 2011 г. ввела регистрацию по номеру мобильного телефона. Однако если злоумышленник знает электронный адрес пользователя Facebook и введет его в строку восстановления пароля, ему также будет доступна информация об имени и аватар.

Как сообщал Digit.ru, это уже не первый спорный момент с системами восстановления паролей в соцсетях. В прошлом году стало известно, что, зная адрес электронной почты пользователя и факт наличия у него аккаунтов во «ВКонтакте» и Facebook, можно узнать номер его телефона. После выявления этой информации «ВКонтакте» скрыла большую часть номера пользователя, чтобы избежать утечки данных ***(Facebook позволяет узнать имя и аватар пользователя по номеру телефона // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_pozvolyaet_uznat_imya_i_avatar_polzovatelya_po_nomeru_telefona). – 2014. – 21.01).***

***

Российские специалисты предупредили о распространении через Facebook и другие каналы трояна, маскирующегося под обновление к Adobe Flash Player. Зловред скачивает на компьютер жертвы дополнительные плагины, которые отображают рекламу в браузерах.

Специалисты по информационной безопасности обнаружили новую

троянскую программу Trojan.Zipvideom, которая в настоящее время активно распространяется в Интернете. Она попадает на компьютер жертвы под видом обновления для плагина Adobe Flash Player.

Как сообщает российская компания «Доктор Веб», если пользователь соглашается на установку обновления, на его компьютер загружается первый компонент трояна – приложение FlashGuncelle.exe. Процесс установки маскируется под процесс установки обновления к Adobe Flash Player.

Далее FlashGuncelle.exe загружает с сервера злоумышленников на компьютер жертвы оставшиеся компоненты трояна. Их цель заключается в установке вредоносных плагинов к браузерам Mozilla Firefox и Google Chrome.

Опасность трояна заключается в том, что загружаемые им плагины мешают свободному просмотру сайтов, демонстрируя рекламу, а также имеют возможность скачивать на компьютер жертвы другое нежелательное программное обеспечение.

Установлено, что при посещении сайтов популярных социальных сетей (Twitter, Facebook, Google+, YouTube, «ВКонтакте») эти плагины загружают Java-скрипты сомнительного назначения.

Одним из каналов распространения трояна является соцсеть Facebook. В ней ссылку на вредоносный файл содержат сообщения массовых рассылок. Одна из таких рассылок была отправлена в начале 2014 г.

Чтобы избежать заражения Trojan.Zipvideom, пользователям рекомендуется скачивать обновления программ и другой софт только из официальных источников, а также использовать антивирус, который блокирует установку вредоносных файлов.

Подробные сведения о происхождении трояна «Доктор Веб» не раскрывает, но сообщает о своем предположении, что автор программы говорит на турецком языке ***(В сети появился троян, замаскированный под Adobe Flash Player // InternetUA (http://internetua.com/v-seti-poyavilsya-troyan--zamaskirovannii-pod-Adobe-Flash-Player). – 2014. – 22.01).***

***

Традиционный ежегодный отчет Cisco с обзором рынка кибербезопасности рисует очень мрачную перспективу на 2014 г. Судя по всему, взлом Target и других торговых сетей США – это только начало.

В настоящее время количество уязвимостей в программном обеспечении и векторов угроз возросло до рекордного уровня за все время измерений (с 2000 г.). По оценке Cisco, в мире не хватает примерно 1 млн квалифицированных специалистов по безопасности. Это главная причина, по которой компании продолжат страдать от взломов и утечек информации. Проще говоря, хакеры-злоумышленники превосходят их интеллектуально.

Одна из главных тенденций последнего времени – увеличение сложности кибератак. Преступники объединяются в группы с узкой специализацией каждого участника, они хорошо финансируются и обладают необходимыми

ресурсами для нанесения серьезного экономического ущерба. На руку им играет и усложнившаяся компьютерная инфраструктура, в которую теперь входят разнообразные мобильные платформы и облачные сервисы.

Злоумышленники начали понимать, что взлом инфраструктурных сервисов дает большую выгоду, чем атака непосредственно на серверы жертвы. Поэтому все чаще встречаются случаи, когда хакеры получают контроль над хостинговыми платформами, нейм-серверами и дата-центрами с целью завладения богатыми ресурсами, которые можно получить через них.

Самым распространенной формой вредоносных программ в 2013 г. стали трояны универсального назначения, которые упоминаются в 27 % сообщений об атаках. На втором месте – атаки drive-by и фреймы с загрузкой наборов эксплоитов (23 %). По прежнему главным языком программирования, который эксплуатируют злоумышленники, остается Java. За прошлый год Java-эксплоиты стали причиной 91 % сообщений о взломах (Indicators of Compromise), по статистике компании Sourcefire ***(Java используется в 91 % кибератак // InternetUA (http://internetua.com/Java-ispolzuetsya-v-91--kiberatak). – 2014. – 22.01).***

***

Разработчики вредоносного ПО нашли новый хитрый способ проникновения на пользовательские компьютеры с целью отображения рекламы в веб-браузере. Они покупают расширения у их авторов и изменяют их код. Пользователи не всегда сразу догадываются, почему они стали видеть больше рекламы, чем прежде.

Разработчики AdWare, вредоносного ПО, несанкционированно распространяющего рекламу, нашли новый способ проникновения на компьютеры пользователей – посредством расширений для веб-браузера Google Chrome, сообщает Ars Technica.

Они обращаются к авторам расширений для браузера Google Chrome и покупают разработку. После этого они модифицируют код расширения и добавляют в него показ рекламы. При этом «попасть» на компьютер пользователя достаточно просто – как правило, у большинства обновление расширений выполняется автоматически.

Одним из расширений, через которое распространители рекламы смогли проникнуть на пользовательские компьютеры, стало Add to Feedly, написанное Э. Агарвалом. По его словам, к нему на почту пришло письмо с предложением купить расширение за четырехзначную сумму. Думать долго не пришлось – учитывая, что он потратил на создание расширения всего около часа, предложение оказалось крайне выгодным. Получив оплату по PayPal, он благополучно передал свою разработку.

Спустя месяц пользователи Google Chrome с установленным расширением Add to Feedly стали видеть рекламу на каждой просматриваемой ими странице, причем нажатие на ссылки стало приводить к перенаправлению

на сайты рекламодателей.

Распространители рекламы воспользовались расширениями, которые пользователи скачивают в Google Web Store.

Благодаря достаточно большой пользовательской базе Add to Feedly, насчитывающей около 30 тыс. человек, покупатель расширения стал мгновенно получать прибыль с размещения рекламы.

Другим расширением, ставшим инструментом в руках недобросовестных распространителей рекламы, стал Tweet This Page. Проверка магазина Google Web Store позволила выяснить, что указанная модификация была проведена над несколькими плагинами.

Особенностью веб-браузера Google Chrome является автоматическое обновление. Оно устроено таким образом, что пользователь всегда работает над наиболее свежей версией браузера.

Такая философия распространяется и на дополнения. При установке пользователь соглашается с автоматическим обновлением плагина, после чего каждая новая версия доставляется на компьютер автономно, без постороннего вмешательства.

Примечательно, что пользователи не сразу понимают, в чем дело и что стало причиной увеличения объема рекламы на страницах. Некоторые думают, что причиной стал вирус, однако антивирусные программы не находили ничего подозрительного. Чтобы запутать пользователя, покупатели расширений включают отображение рекламы спустя несколько дней после установки плагина ***(Google Chrome стал распространителем вредоносного ПО // InternetUA (http://internetua.com/Google-Chrome-stal-rasprostranitelem-vredonosnogo-po). – 2014. – 20.01).***

***

Злоумышленники распространяют банковского троянца под видом установки мобильного мессенджера WhatsApp на персональный компьютер пользователя, говорится в блоге российской компании «Лаборатория Касперского».

Согласно сообщению, злоумышленники организовали новую спам-рассылку писем по электронной почте, в которых говорится, что мобильный мессенджер WhatsApp теперь можно установить на ПК пользователя, однако тот, кто пытается установить это приложение, на самом деле скачивает себе на ПК банковского трояна.

Эксперты «Лаборатории Касперского» получили спам-сообщение на португальском языке, в котором говорится, что «наконец-то приложение WhatsApp стало доступно на ПК и что у получателя уже есть 11 приглашений от друзей в его учетной записи». Если пользователь нажмет на ссылку в письме для скачивания приложения, то попадет на взломанный сервер, расположенный в Турции, а затем его перенаправят на облачный сервис Hightail (бывший Yousendit), где ему будет предложено скачать троянец, который в системе

выглядит как 64-битный инсталляционный файл для скачивания.

На самом деле, отмечают эксперты, это стандартное 32-битное приложение, которое удовлетворительно (по шкале VirusTotal) распознаётся антивирусными продуктами. После запуска приложения оно загружает на ПК пользователя нового банковского троянца. Этот зловред скачивается с сервера в Бразилии и плохо распознаётся антивирусами – три из 49 по шкале VirusTotal. Иконка троянца делает его похожим на MP3-файл, поэтому многие пользователи могут кликнуть по ней, тем более что файл весит 2,5 Мб. Чтобы затруднить анализ вредоносной программы, в новый троянец включены некоторые противоотладочные функции, а сама программа написана на языке Delphi, отмечается в сообщении.

После запуска троянец отправляет отчет в принадлежащую киберпреступникам консоль статистики заражений. Украденная информация пересылается через локальный порт 1157, когда он открыт. Кроме того, зловред загружает на компьютер другое вредоносное программное обеспечение ***(Вредоносное ПО рассылается под видом приложения WhatsApp для ПК // InternetUA (http://internetua.com/vredonosnoe-po-rassilaetsya-pod-vidom-prilojeniya-WhatsApp-dlya-pk). – 2014. – 23.01).***

***

Сервис Instagram за несколько месяцев стал очень популярен. Им пользуются даже чаще, чем популярными социальными сетями типа «ВКонтакте» и Facebook.

Недавно компании Symantec стало известно, что пользователи популярного сервиса ради лайков и большого количества подписчиков готовы «поделиться» с другими своим логином и паролем. Дело в том, что существует специальное предложение InstLike, которое помогает заполучить желанные «сердца». Тем самым аккаунты людей, которые передали свои личные данные этому приложению, становятся похожи на роботов, потому что они автоматически ставят лайки и подписываются на страницы других людей. Контроль со стороны людей в таком процессе отсутствует полностью.

Адрес накрутчика instlike.com он же likefol.com.

Создатели такого приложения, как InstLike, заверяют своих пользователей, что нужные голоса люди получат бесплатно, от них ничего не требуется. Но компания Symantec считает совсем иначе. Разработчики InstLike должны использовать Instagram API для доступа к личным данным своих пользователей, но вместо этого они просто запрашивают пароль с логином напрямую у пользователей Instagram.

Компания Symantec в ходе своих исследований выяснила, что аккаунты пользователей приложения InstLike автоматически подписывались на чужие страницы и ставили лайки незнакомым людям, хотя для этого необходимо согласие со стороны самих владельцев аккаунтов.

Если у вас есть такое приложение, то вам следует не просто его удалить,

но и поменять аккаунт в Instagram. Компания Symantec еще раз предупреждает всех, кто активно пользуется различными приложениями: никогда не нужно делиться своей личной информацией, ведь доступ к данным должен происходить только по средствам специальных официальных протоколов авторизации. В таком случае вы будете защищены от утери личных данных, а значит, вашей виртуальной безопасности ничего не будет угрожать ***(«Лайки» не всегда позитивны… // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/layki_ne_vsegda_pozitivny). – 2014. – 23.01).***

***

Новое вредоносное программное обеспечение, заражающее мобильные устройства на Android через Windows-ПК, было обнаружено антивирусными специалистами. Оно ориентировано, главным образом, на разработчиков программного обеспечения. А. Невилл, специалист по ИТ-безопасности Symantec, говорит, что вредонос использует нетипичную двухшаговую схему атак для перехода из Windows в Android-устройства.

«Он начинает работать как троянец, когда попадает на Windows-машину и создает там новый сервис. Позже он ориентируется на Android-устройства, подключаемые к USB-портам. Он использует дебаггинг-мост для размещения троянца Fakebank на Android-устройствах», – говорит А. Невилл.

Fakebank – это известный троянец, созданный для кражи финансовых данных, причем в оригинале он нацелен на некоторые корейские банкинг-системы. Если таковые будут найдены, то троянец попросит пользователя установить обновленние, при этом фактически нотификатор ведет на вредоносный код псевдо-банкинга. Помимо этого, у троянца есть возможности по удаленному SMS-мониторингу, что отражает сложную сущность современных банковских приложений.

«Атака использует довольно сложный комплекс действий. Так как вредонос использует Android Debug Bridge, данный код требует активации через USB. Вместе с тем такой подход существенно ограничивает сферу использования троянца, а основная аудитория троянца – разработчики приложений», – говорит А. Невилл ***(Новый Android-троян попадает в смартфон через Windows // InternetUA (http://internetua.com/novii-Android-troyan-popadaet-v-smartfon-cserez-Windows). – 2014. – 25.01).***

***

Хакеры придумали коварный способ доставки вредоносного ПО на Android. Ф. Шиллер, старший вице-президент корпорации Apple, недавно опубликовал отчёт, согласно которому 99 % всех вредоносных программ для мобильных операционных систем создано для атаки на Android-устройства. Как правило, большинство вредоносных программ загружается через Интернет под

каким-либо благовидным предлогом, при этом персональный компьютер в атаке не задействован. Однако Symantec, компания по производству программного обеспечения в области информационной безопасности и антивирусов, отмечает подъем активности нового вида угроз, которые устанавливают на смартфон или планшет поддельную версию Google Play при подключении девайса к компьютеру под управлением Windows. Важным условием является включенный на смартфоне режим отладки по USB. Этот режим обычно используется разработчиками, однако простые пользователи могут самостоятельно включить его для получения Root или перепрошивки устройства.

После установки поддельного Google Play, который внешне ничем не отличается от настоящего, поведение программы может различаться. В Корее, например, был замечен троян, который при поиске программы для интернет-банкинга выдавал подмененные результаты. В результате поддельная программа отсылала данные о банковских картах создателю трояна. Для устранения риска подвергнуться заражению подобными программами Symantec рекомендует убедиться в том, что на вашем устройстве отключен режим отладки по USB, а также не советует подключать смартфон к неизвестным компьютерам ***(Хакеры придумали коварный способ доставки вредоносного ПО на Android // Aspekty.net (http://aspekty.net/2014/hakeryi-pridumali-kovarnyiy-sposob-dostavki-vredonosnogo-po-na-android/). – 2014. – 26.01).***

***

В ближайшем будущем целью хакеров и создателей вирусов могут стать очки дополненной реальности (такие как Google Glass), игровые консоли, охранные системы, автомобили, телевизоры, холодильники с подключением к Интернету и другие технические новинки, постепенно входящие в нашу жизнь. Об этом говорится в отчете, подготовленном экспертами компании ESET.

Так, в случае с автомобилями киберпреступники смогут взломать бортовой компьютер и получить информацию о маршруте передвижения. Кроме того, уже проводились эксперименты по удаленному управлению системами автомобиля – речь идет о запуске двигателя, открытии дверей и даже отключении тормозов.

В свою очередь, «умные» телевизоры Smart TV теоретически позволяют следить за их хозяевами через встроенные камеры. Также многие телевизоры позволяют осуществлять платежи при помощи встроенных интернет-кошельков крупных платежных систем. Перехват таких данных возможен и мало чем отличается от традиционной кибератаки на персональный ПК или смартфон. Наконец, многие телевизоры по инициативе самих производителей передают информацию о том, какие каналы смотрит пользователь.

Одной из целью хакеров могут стать «умные дома», утверждают специалисты ESET. По их мнению, «даже холодильник может содержать персональные данные владельца, на которые всегда найдется покупатель».

Эксперты отмечают, что подобная информация никак не защищена, поскольку антивирусов для холодильников пока не существует. Кроме того, многие предметы «умного дома» связаны через Интернет с ноутбуком или планшетом. Благодаря этому бытовая техника может стать «черным ходом» для заражения ПК или мобильного устройства.

Что касается игровых консолей, то они интересуют киберпреступников с точки зрения кражи личных данных, таких как логины и пароли пользователя в соцсетях и других сервисах ***(Хакеры готовятся атаковать «умные дома», машины и телевизоры // InternetUA (http://internetua.com/hakeri-gotovyatsya-atakovat--umnie-doma---mashini-i-televizori). – 2014. – 25.01).***