СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(22.09–5.10)

2014 № 18

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(22.09–5.10)
№ 18

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

© Національна бібліотека України
імені В. І. Вернадського, 2014

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Социальная сеть «Одноклассники» открыла у себя новый проект под названием «Достижения». Суть проекта заключается в том, чтобы повысить активность пользователей сети. Те из участников, которые окажутся наиболее социально активными, получат от организаторов проекта подарки.

Попасть на страницу проекта можно в горизонтальном меню, кликнув на кнопку «Еще». Там можно увидеть информацию о порядке присуждения наград и о самих наградах. Авторы проекта говорят, что категории в этом проекте будут еще добавляться.

Для того, чтобы проявить свою социальную активность, пользователь должен разместить у себя на странице фотографию или видеоролик. Заработанные наградные очки впоследствии можно будет потратить на сетевых «Аукционах» ***(Соцсеть «Одноклассники» открыла новый проект «Достижения» // IT Expert (http://itexpert.org.ua/rubrikator/item/38332-sotsset-odnoklassniki-otkryla-novyj-proekt-dostizheniya.html). – 2014. – 22.09).***

***

В Інтернеті з’явився сервіс, що допомагає непопулярним фото в Instagram отримати лайки. Додаток No Likes Yet акумулює в собі усі фото з Instagram, які не отримали жодного лайка і допомагає виправити цю ситуацію, повідомляє Wired.

Щоб розпочати користування No Likes Yet, слід авторизуватися за допомогою Instagram-акаунту. Після цього ресурс відображає фото зі всього світу, фото самого автора або ж дає змогу знайти фото без жодного лайка в певному профілі.

Таким чином можна зробити комусь приємно, вважають автори нового сервісу. Вподобати власні фото за його допомогою неможливо.

Додаток розробили Т. Хеттлер, Т. Мідян та Д. Сумарна, які живуть у Нью-Йорку та працюють у сфері реклами та дизайну. Ідея сервісу виникла у авторів після того, як вони помітили, що Instagram підписує фото без лайків фразою «Лайків поки що немає» (No Likes Yet) ***(В Інтернеті з’явився сервіс, що допомагає непопулярним фото в Instagram отримати «лайки» // Громадська організація «Телекритика» (http://osvita.mediasapiens.ua/material/34790). – 2014. – 22.09).***

***

У социальной сети «Одноклассники» сменится генеральный директор. Руководитель «Одноклассников» и вице-президент Mail.ru Group И. Широков покидает компанию, сообщает НТВ.

Уже с 1 октября во главе «Одноклассников» встанет А. Федчин, который ранее занимал должность технического директора соцсети.

И. Широков пробудет с Mail.ru Group до конца 2014 г. – все это время он будет передавать дела.

К. Чабаненко, представитель Mail.ru Group: «Сейчас мы обсуждаем с И. Широковым возможное сотрудничество по другим направлениям».

Сам И. Широков отметил, что, возможно, продолжил свое сотрудничество с интернет-компанией, однако по большей части хочет сконцентрироваться на своих международных проектах, пишут «Ведомости».

И. Широков возглавлял «Одноклассников» последние четыре года. При нем доходы соцсети возросли более чем в 10 раз. По мнению некоторых специалистов, И. Широков – один из лучших на сегодняшний день российских интернет-менеджеров ***(«Одноклассники» осиротели // Индустриалка (http://iz.com.ua/mir/53654-odnoklassniki-osiroteli.html). – 2014. – 25.09).***

***

В Интернете появилась и набрала популярность новая социальная сеть под названием Ello, позиционирующая себя, как полностью свободная от рекламы альтернатива Facebook. 25 сентября ресурс, существующий пока только в виде бета-версии, открыл ограниченную регистрацию по приглашениям.

О проекте Ello ещё в середине марта одним из первых сообщило издание BetaBeat. Тогда создатели ресурса привлекли внимание СМИ, разместив сети манифест с призывами к пользователям перестать быть продуктом в руках рекламщиков и маркетологов, «отслеживающих и продающих каждый статус, каждого друга и каждый лайк».

Как говорилось в манифесте, социальные сети должны быть не очередным способом обмана и манипуляции над людьми, а полезным, простым и удобным инструментом в руках всех, кто их используют.

Реализовать эти заявления на практике в Ello обещали создав анти-Facebook без рекламы и отслеживания пользовательских действий – бесплатную и открытую для всех соцсеть, зарабатывающую исключительно на продаже пользователям премиальных функций и дополнительных возможностей «за несколько долларов».

Бета-версия новой социальной сети запустилась в конце сентября. Внутри сайт выглядит как упрощённый и переработанный гибрид Google+, ленты Twitter и блогохостинга Tumblr.

Зарегистрировавшись, пользователь может заполнить профиль и начать добавлять друзей. Они отображаются в левой части страницы в виде небольших кругов с аватарками. Всех друзей можно разделить на две категории – «Друзья» (Friends) и «Шум» (Noise).

Правая часть страницы отведена под ленту новостей, состоящую из записей, фотографий и статусов, опубликованных другими пользователями. Каждую из записей можно комментировать, оставляя её автору упоминания

при помощи символа @ как в Twitter. Также Ello поддерживает публикацию ссылок и фотографий.

Практически сразу новый ресурс привлек к себе внимание западного ЛГБТ-сообщества, ранее часто высказывавшего недовольство политикой Facebook в свой адрес и сталкивавшегося с регулярными блокировками и удалением публикуемого активистами «взрослого» контента.

Изначально правила пользования Ello запрещали публикацию порнографии и эротических материалов. Однако затем текст обновили, добавив в него уточнение, что в некоторых случаях откровенные записи будут считаться допустимыми.

За первые сутки количество запросов на получение инвайта в соцсеть выросло с нескольких сотен до нескольких тысяч в час. Создатели проекта сообщили журналистке Fast Company Р. Харманки, что по состоянию на вечер 25 сентября ежечасно получали около 34 тыс. запросов на регистрацию на сайте.

Резкий рост популярности Ello породил в онлайн-магазине eBay множество лотов, на которых пользователи пытаются продать через Интернет приглашения на сайт. Стоимость инвайтов колеблется от 190 р. до 38 тыс.

Соцсеть Ello является проектом дизайнера П. Будница. Разработка ресурса ведётся на деньги компании Fresh Tracks Capital, весной вложившей в стартап 435 тыс. дол. По заявлениям сооснователей сайта и его инвесторов, их главная задача – изменить ценности IT-индустрии и доказать, что при большом количестве пользователей реально построить соцсеть, успешно функционирующую без рекламы и маркетинговых манипуляций ***(Новая соцсеть привлекла тысячи пользователей обещанием стать «Facebook без рекламы» // IT Expert (http://itexpert.org.ua/rubrikator/item/38453-novaya-sotsset-privlekla-tysyachi-polzovatelej-obeshchaniem-stat-facebook-bez-reklamy.html). – 2014. – 26.09).***

***

Сервис персональных алкогольных рекомендаций Distiller превратился в полноценную социальную сеть для любителей виски.

Сеть работает с мобильным приложением, которое анализирует тысячи марок, учитывая их цену, рейтинг, тип, отзывы других пользователей, и выводит список позиций, лучше всего подходящих по вкусу и к конкретной ситуации.

Клиент Distiller для iPhone стал доступен для скачивания ещё в феврале 2014 г., однако только после выхода версии для Android любопытное приложение превратилось в полноценную социальную сеть.

Профили Distiller напоминают личные страницы в Twitter. Приложение поддерживает ленту новостей, список желаний, рейтинги, счётчик подписчиков и другие, характерные для социальных сетей функции.

Пользователи могут добавлять друг друга в друзья, оставлять рекомендации и делиться мнениями о том или ином бренде виски ***(Появилась мобильная социальная сеть для любителей виски // Блог Imena.UA (http://www.imena.ua/blog/distiller/). – 2014. – 25.09).***

***

Вторник, 30 сентября, стал последним днем работы первой социальной сети Google. Проект Orkut, который был сильно популярен в некоторых развивающихся странах, таких как Бразилия и Индия, признан коммерчески неуспешным, поэтому оказался свернут.

О намерении закрыть соцсеть Google объявила 30 июня. Скопировать личные данные из Orkut можно будет до 30 сентября 2016 г. через Google Takeout. Загруженные фотографии можно перенести в Google+.

Руководство американской компании поблагодарило верных пользователей и принесло извинения за закрытие сервиса, посоветовав пользоваться более популярными ресурсами. Этим начали давно заниматься бывшие участники Orkut.

В частности, после объявления о закрытии Orkut количество пользователей социальной сети «ВКонтакте» в Бразилии возросло на 2000 % всего за двое суток. Кроме того, мобильная версия сервиса обмена мгновенными сообщениями ICQ для платформы iOS стала самым популярным приложением в App Store среди бразильцев.

Сеть Orkut появилась около 10 лет назад и пользовалась неплохой популярностью в ряде стран, но с появлением Facebook проект Google не выдержал конкуренции, тем более сама интернет-корпорация начала развивать другую социальную сеть – Google+ ***(Первая соцсеть Google прекратила работу // InternetUA (http://internetua.com/pervaya-socset-Google-prekratila-rabotu). – 2014. – 30.09).***

***

Протестующие в Гонконге формируют свой собственный «частный Интернет», используя приложение для чатов, чтобы общаться, несмотря на правительственное ограничение доступа к некоторым социальным сетям и сбои в работе систем сотовой связи.

Только за 24 часа после запрета около 100 тыс. человек в Гонконге загрузили приложение FireChat. Этот сервис обмена сообщениями стал самым популярным продуктом в гонконгском магазине приложений Apple App Store.

Китайские органы цензуры заблокировали Instagram и некоторые поисковые слова на Weibo, китайском аналоге Twitter, чтобы помешать появлению в Китае фотографий десятков тысяч протестующих в Гонконге. Мобильные сети в тех местах Гонконга, где происходят протесты, перегружены.

Разработанное стартапом Open Garden из Сан-Франциско приложение FireChat базируется на технологии «ячеистой сети» и использует Bluetooth для того, чтобы передавать сообщения с одного смартфона на другой через телефоны других пользователей FireChat. Таким образом увеличивается расстояние, которое можно охватить чатом.

Приложение изначально разрабатывалось для использования в самолетах и поездах, где плохое соединение с Интернетом ограничивает коммуникацию.

К. Далиголт, вице-президент по продажам и маркетингу Open Garden, сказал, что протестующие создали сотни чатов, чтобы предупреждать друг друга о действиях полиции или угрозе использования водометов. 30 сентября, после напряженного противостояния, в котором полиция применила слезоточивый газ, правительство Гонконга отозвало полицейских с улиц, где остались лишь мирные протестующие.

FireChat можно использовать для того, чтобы один человек, подсоединенный к Интернету, давал возможность выходить в Интернет другим пользователям. Приложение также позволяет обмениваться сообщениями вне Интернета, поскольку вся сеть чатов работает офлайн. «Это только видимая часть айсберга, так как мы не видим обмена сообщениями, происходящего «без подключения», – сказал К. Далиголт.

Последний раз взлет популярности приложения наблюдался в Ираке, когда правительство в июне ограничило доступ к Интернету. Тогда за неделю приложение загрузили 40 тыс. человек, хотя в Ираке нет App Store ***(«Частный интернет» набирает обороты // InternetUA (http://internetua.com/castnii-internet--nabiraet-oboroti). – 2014. – 1.10).***

***

В соцсети «ВКонтакте» обновился фоторедактор. Теперь в нем можно не только накладывать фильтры, но и настраивать различные параметры фотографии, такие как изменение уровня экспозиции, контраста, насыщенности и резкости фото. Они изменяются при помощи ползунков.

Также можно воспользоваться автоматической коррекцией, которая анализирует изображение и на основе этого настраивает контраст и баланс белого. В отличие от Instagram, использовать в фоторедактор «ВКонтакте» одновременно фильтры и настройку параметров нельзя.

Количество фильтров в новой версии увеличилось с семи до 15 штук. Можно также регулировать их интенсивность с помощью ползунка. При помощи фоторедактора также можно кадрировать, размывать, поворачивать снимок и накладывать на него надписи.

Социальный фотосервис Instagram, который принадлежит соцсети Facebook, запустил аналогичные обновления в июне 2014 г. В Instagram тоже можно настраивать экспозицию, контраст, насыщенность и резкость, и совмещать это с фильтрами. Возможность регулировать интенсивность фильтра во «ВКонтакте» появилась раньше, весной 2013 г. ***(Фоторедактор***

«ВКонтакте» продолжил копировать Instagram // InternetUA (http://internetua.com/fotoredaktor--vkontakte--prodoljil-kopirovat-Instagram). – 2014. – 2.10).

***

Пользователь Facebook сербский студент и фотограф А. Симик заметил, что социальная сеть тестирует новую функцию «Слайд-шоу поездки» (Trip Slideshow). Об этом он сообщил изданию The Next Web.

После поездки А. Симика в Грецию, приложение Facebook на его iPhone создало слайд-шоу из фотографий, сделанных во время путешествия.

По сообщению А. Симика и других пользователей Facebook в Twitter, новая функция создает слайд-шоу автоматически, не требуя никаких действий со стороны пользователя.

Опция Trip Slideshow работает на основе того же принципа, что и Year In Review, которую крупнейшая социальная сеть рекламирует в конце каждого года. Только вместо «лучших моментов» – отобранных Facebook фото и постов, пользователь получает скомпилированные в слайд-шоу фото последней поездки.

Журналисты издания TNW отправили запрос о комментарии по поводу полученной информации в пресс-службу Facebook, но пока не получили ответа ***(Facebook тестирует функцию «Слайд-шоу поездки», которая компилирует фото недавних путешествий // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_testiruet_funktsiyu_slayd_shou_poezdki_kotoraya_kompiliruet_foto_nedavnih_puteshestviy). – 2014. – 2.10).***

***

Компания Facebook извинилась за проведения социальной сетью исследований психологического состояния пользователей. Об этом говорится в письме, опубликованном главным инженером Facebook М. Шрепфером в блоге компании.

В своем письме М. Шрепфер объяснил, что любые исследования Facebook предназначаются для улучшения продуктов и услуг, которые предоставляет социальная сеть. Однако руководство компании не ожидало, что публикация результатов их экспериментов вызовет негодование пользователей.

Речь идет об исследовании, связанном с эмоциональной окраской постов, попадающих в ленту. В 2011 г. Facebook манипулировал новостными фидами более чем 600 тыс. пользователей, чтобы выяснить, каким образом позитивные и негативные эмоции распространяются через социальные сети.

По словам М. Шрепфера, компания пересмотрела методику своих исследований и поменяла их структуру. В частности, в программу образования инженеров соцсети были включены тренинги, посвященные

корректным исследованиям, а результаты текущих экспериментов размещены на специальной странице.

При этом М. Шрепфер подчеркнул, что компания продолжает верить в исследования, так как они помогают делать Facebook лучше ***(Facebook извинился за проведение исследований психологического состояния пользователей // Четверта Влада (http://4vlada.net/mass-media/facebook-izvinilsya-za-provedenie-issledovanii-psikhologicheskogo-sostoyaniya-polzovatele). – 2014. – 3.10).***

***

Новая социальная сеть Ello смогла привлечь к себе внимание пользователей своей жёсткой политикой в отношении спама и ботов – такие аккаунты в качестве наказания получали перманентный бан. Но не прошло и недели с момента запуска, как пользователи стали замечать резкое увеличение числа спамных аккаунтов. Доходит до того, что примерно каждые 10 мин пользователям приходят запросы на дружбу от «интернет-экспертов» вроде @fitness4all

Ello позиционирует себя как абсолютно некоммерческую сеть «для людей», и её правила направлены против скриптов, написанных для автоматического добавления в друзья сотен пользователей. Такой метод спамеры постоянно используют, чтобы создавать рекламные площадки в социальных сетях наподобие Ello или Tumblr.

В компании говорят, что они ещё пока не придумали, как бороться с ботами и спамом в автоматическом режиме. «Жалобы от пользователей – это единственный способ удаления спамных аккаунтов на сегодняшний день. Но мы работаем над ускорением процесса» – заявляют разработчики.

Но не только простые пользователи стали жертвами действий спамеров. В Ello так же стали появляться страницы ведущих брендов и знаменитостей, которые на самом деле были созданы спамерами. Видимо это делается с расчётом дальнейшей продажи этих страниц самим брендам, когда те придумают, как использовать Ello в своих маркетинговых целях.

Несмотря на то что Ello всё ещё находится в бета-версии, она уже наводнена людьми, пытающимися сделать на ней деньги.

Возможно, разработчики не ожидали такого развития событий, поэтому ручной способ борьбы со спамом до сих пор является единственным решением проблемы. Остаётся надеяться, что разработчики смогут что-нибудь придумать в кратчайшие сроки – иначе Ello, так же как и другие социальные сети, попросту утонет в спаме ***(Социальная сеть Ello оказалась наводнена ботами и спамерами // InternetUA (http://internetua.com/socialnaya-set-Ello-okazalas-navodnena-botami-i-spamerami). – 2014. – 3.10).***

***

Социальная сеть LinkedIn анонсировала изменения в пользовательском соглашении, которые вступят в силу 23 октября этого года. В двух словах их общий смысл можно выразить так: «Вы – владелец своего контента».

Эти изменения особенно актуальны, учитывая специфику пользовательских соглашений других социальных сетей. Например, Facebook оставляет за собой право использовать размещенный вами контент по своему усмотрению и не планирует отказываться от этой практики, несмотря на многочисленные скандалы и возмущение пользователей.

Итак, чем LinkedIn планирует порадовать нас уже меньше чем через месяц?

Вы являетесь собственником контента, опубликованного вами в соцсети. И это не может измениться.

Если вы удаляете что-то из LinkedIn, права социальной сети на эти материалы заканчиваются. Но LinkedIn не может контролировать, что делают другие пользователи с вашим контентом до того, как вы его удалите. Например, кто-то из пользователей мог скопировать вашу презентацию в свой блог до того, как вы удалили ее с LinkedIn. Естественно, в подобных случаях социальная сеть не несет ответственности.

У LinkedIn нет эксклюзивных прав на контент пользователей. Так что вы можете размещать его на других площадках по своему усмотрению.

LinkedIn не лицензирует и не продает пользовательский контент третьим лицам (рекламодателям, издателям, сайтам и т. д.) без разрешения пользователей.

LinkedIn не вносит изменения в контент пользователей. Но иногда социальной сети требуется перевести его, настроить форматирование или провести другие технические изменения, чтобы материал адекватно выглядел на сайте ***(LinkedIn возвращает права на контент пользователям // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_vozvraschaet_prava_na_kontent_polzovatelyam). – 2014. – 3.10).***

***

Сегодня с полос профильных СМИ и лент в Facebook и Twitter не сходит одно и то же слово – Ello. Интернет-пространство заполонили черные безглазые смайлы, и сложно себе представить, что вся эта истерия крутится вокруг очередной новой соцсети. Да, она без рекламы. И да, она закрытая, а, как известно, люди больше всего хотят туда, куда их не пускают. Но все-таки – что в ней такого особенного, что шум вокруг нее не утихает уже несколько недель? Внештатному автору VentureBeat Р. Черриеру удалось внедриться в Ello – и вот что он рассказал после 48 часов, проведенных на сайте, пишет AIN.UA (http://ain.ua/2014/10/03/543195).

«Чем Ello так сильно отличается от других соцсетей?

В основном, таймингом. В целом она не очень-то отличается от Facebook или Twitter: вы можете менять аватар, обложку, обновлять статус, делиться фотографиями, добавлять друзей. Но (и это реальное но!) здесь нет рекламы. И это обещание – что вы сможете общаться с друзьями не отвлекаясь на спонсированные посты, приглашения в игры, нескончаемую Facebook-рекламу, интегрированную в приложения – стало причиной того, что все так хотят проникнуть сюда и посмотреть, что да как.

Что я думаю по этому поводу?

Это определенно новый опыт. Очевидно, что они позиционируют себя анти-фейсбуком, но беда в том, что у Facebook ушло много времени и денег на то, чтобы стать удобной для пользователей. Быть новым, другим – круто, но долго на этом не продержишься без понятного и удобного интерфейса. Есть моменты, из-за которых можно с ответственностью заявить, что Ello пока в бете и здесь хватает багов, над которыми надо поработать. Также есть нехватка функций, в частности недостает блокировки пользователей и мобильного приложения.

Впрочем, администрация обещает, что скоро станут доступны новые функции:

“Скоро в ассортименте:
блокировка пользователя
пометка запрещенного контента
аудио-интеграция с Soundcloud
приватные аккаунты
мультимедиа
улучшенный мобильный интерфейс
репосты
центр уведомлений
онлайн/офлайн маркировка
закладки в ленте
смайлы
видео-интеграция с YouTube, Vimeo, Instagram, Vine
приватный мессенджер
автоперепосты в другие соцсети
приложения на iOS и Android”

Однако, не все так плохо. Простота интерфейса очень линейная, а лента чрезвычайно изменчива. Здесь нет ограничения по количеству символов, как в Twitter, можно публиковать GIF-картинки и делать прочие веселые штуки, которых нельзя делать в Facebook. Есть несколько интересных вещей вроде инструмента Ello Facemaker, с помощью которого можно поставить себе на фотографию вместо лица лого Ello, скрыв таким образом свою личность или просто в поддержку нового сайта. Такое можно делать и без регистрации на сайте.

Если бы мне пришлось оценивать эту соцсеть, я бы сказал, что она незакончена. Здесь имеется несколько хороших идей, но есть и очень много к чему стремиться. И то, куда она идет – это самое интересное.

Она действительно может выжить без рекламы?

Скорее всего – нет. Ello получила венчурные инвестиции в марте в размере 435 тыс. дол. Венчурные инвесторы – это вам не бекеры с Kickstarter, они дают деньги не ради добра. Разумеется, на создателей Ello будут давить, требуя делать деньги и для себя, и инвесторов, и это может изменить направление движения компании.

Один из вариантов, как они могли бы этого избежать – предложить пользователям какие-то “особые функции” за небольшую единоразовую плату. И хотя это показывает, как стартаперы пытаются “думать по-другому”, чтобы предотвратить появление рекламы на сайте, тяжело представить, чтобы эта модель была способна генерировать достаточно прибыли и при этом удержать пользователей, учитывая, что у них есть готовые бесплатные аккаунты в других соцсетях. Не забывайте, что Facebook изначально тоже была бесплатной, с лозунгом “прежде всего продукт”.

Стоит присоединиться?

Дело ваше. Для начала придется получить приглашение, но я сомневаюсь, что это будет так уж сложно. Все зависит от того, чего вы хотите от социальной сети. Вы можете пройти через все эти треволнения напрасно. За успех Ello придется долго и тяжко сражаться, и сложно представить, что при этом она умудрится остаться свободной от рекламы и ненависти.

Но пока она именно такая. И это что-то» ***(Мои впечатления после 48 часов на Ello – история одного счастливчика // AIN.UA (http://ain.ua/2014/10/03/543195). – 2014. – 4.10).***

***

Крупнейшая в мире социальная сеть, Facebook, планирует экспансию в сфере здравоохранения. Об этом Reuters рассказали на условиях анонимности три источника, знакомых с ситуацией.

Одно из направлений, которое намерены развивать в соцсети – онлайновые группы поддержки для пациентов, страдающих от тех или иных заболеваний. Там они могли бы обмениваться опытом борьбы с недугами, обсуждать эффективность различных методов терапии и т. д. Еще одна группа разработчиков в Facebook создает приложения, призванные предотвращать заболевания, заставляя пользователей изменить свой образ жизни.

По словам источников Reuters, представители соцсети в последние месяцы провели ряд встреч с медиками и предпринимателями от здравоохранения. Полученная в ходе встреч информация используется в создании специального подразделения для исследований и разработок,

касающихся «приложений для здоров'я». Пока, впрочем, Facebook находится на стадии сбора идей.

С одной стороны, медицинские сообщества и приложения помогли бы Facebook повысить активность пользователей. С другой – в бесценную для рекламодателей копилку данных Facebook о том, кто у пользователя в друзьях и каковы его интересы, могли бы добавиться и сведения о здоровье. В этом отношении инициатива соцсети наверняка вызовет у многих неоднозначную реакцию. Поэтому рассматриваются различные подходы, в том числе запуск первого «здорового» приложения от имени другой компании, без упоминания роли Facebook в его разработке ***(Facebook хочет позаботиться о здоровье пользователей // InternetUA (http://internetua.com/Facebook-hocset-pozabotitsya-o-zdorove-polzovatelei). – 2014. – 5.10).***

***

Компания Twitter, владеющая одноименной сетью микроблогов, планирует инвестировать 10 млн дол. в Массачусетский технологический институт (MIT), специалисты которого помогут построить новую платформу для онлайн-общения людей на темы гражданских и политических вопросов.

Указанная сумма, по информации портала PC World, будет вложена в лабораторию Laboratory for Social Machines (LSM), входящую в состав MIT. Ее сотрудники, как сообщается, получат неограниченный доступ к общей базе всех существующих твитов, сделанных со дня начала работы этого проекта, то есть с 2006 г.

Все необходимые данные специалисты получат от компании Gnip, занимающейся анализом различной информации. С апреля текущего года она полностью принадлежит Twitter. MIT предстоит нелегкая работа по «просеиванию» всех твитов, выявлению среди них тех, что затрагивают гражданские и политические темы и нахождению между ними очевидных и неочевидных связей. Конечная цель данного исследования пока не разглашается, но известно, что Twitter собирается создать совершенно новую платформу для общения, предварительно выявив и собрав воедино шаблоны работы нынешних социальных сетей и проектов.

Twitter начнет сотрудничество с MIT в рамках собственного проекта Twitter Data Grants, который подразумевает открытие полного доступа к твитам ряду крупных учебных заведений и исследовательских центров. Проект был запущен в феврале этого года, и в апреле стало известно, что в этом ключе Twitter будет сотрудничать с шестью учреждениями, расположенными на четырех континентах. MIT стал одним из них. Упомянутые 10 млн дол. будут переводиться на его счета в течение пяти лет ***(Twitter инвестирует $10 млн в Массачусетский технологический інститут // InternetUA (http://internetua.com/Twitter-investiruet--10-mln-v-massacsusetskii-tehnologicseskii-institut). – 2014. – 5.10).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Служба безпеки України відкриває свої офіційні сторінки в соціальних мережах Facebook та Twitter. Про це повідомляє прес-центр СБУ.

«Віримо, що наші сторінки стануть не тільки джерелом оперативної інформації про роботу Служби, а й майданчиком для професійної дискусії щодо питань безпеки, які є особливо актуальними в наш час», – наголосив радник голови Служби безпеки України М. Лубківський ***(У Facebook та Twitter з'явились офіційні сторінки СБУ // Чернівці Таймс (http://times.cv.ua/2014/09/23/u-facebook-ta-twitter-zyavylys-ofitsijni-storinky-sbu/). – 2014. – 23.09).***

***

Радник міністра внутрішніх справ, кандидат у народні депутати від партії «Народний фронт» А. Геращенко оголосив про ініціативу «Стоп Підкуп», яка покликана виявити та покарати всіх нечесних кандидатів, які підкуповують виборців.

«Я зареєстрував у Facebook групу – "Стоп Підкуп", куди пропонується повідомляти про всі факти підкупу та інші порушення на виборах. Повідомлення про підкуп можуть відкрито відображатися в хроніці сторінки "Стоп Підкуп" і будуть відкриті для всіх виборців, а також для представників ЗМІ, правоохоронних органів, організацій, які проводять моніторинг виборів», – повідомив А. Геращенко.

Крім того, повідомлення можна слати на пошту stop.podkup@gmail.com або в приват групи «Стоп Підкуп».

«Усі повідомлення будуть перевірятися співробітниками міліції і за ними буде відповідна правова реакція. Для цього міністр МВС А. Аваков підписав відповідне розпорядження, яке зобов'язує співробітників міліції реагувати на скарги, пов'язані з підкупом та іншими порушеннями на виборах, і уважно моніторити всі ЗМІ з цього питання», – зазначив А. Геращенко.

При цьому радник міністра МВС закликав «всіх патріотично налаштованих громадян, які не терплять несправедливості і корупції, додаватися до групи, а потім через сторінку "Стоп Підкуп" координувати свої дії з правоохоронними органами для виявлення негідників, які організовують підкуп голосів виборців» ***(У Facebook створили групу для скарг про підкуп виборців // LB.ua (http://ukr.lb.ua/news/2014/09/25/280616_facebook_sozdali_gruppu_zhalob.html). – 2014. – 25.09).***

***

В соц-сетях проект «АЙ ЛАВ КРЕМЕНЧУГ» открывает новую рубрику «Выборы2014». Соответствующее сообщение содержится на официальных страницах общественного движения в социальных сетях. «АЙ ЛАВ КРЕМЕНЧУГ открывает новую рубрику “Выборы2014”, в которой мы будем делиться информацией о кандидатах от Кременчуга по 146 и 150 округах. Просим вас в свою очередь присылать нам любую информацию, компромат, фотографии, ссылки о наших кандидатах. Кременчужане должны сделать осознанный выбор!» – написано на странице движения.

В настоящее время там же разыскиваются фотографии двух официально зарегистрированных кандидатов в нардепы. Странно, кандидаты есть, а фотографий НЕТ! Социальные сети на сегодняшний день являются наиболее доступным источником информации и обмена данными среди пользователей. Мы будем внимательно следить за проектом, в котором наверняка появится что-то интересное о кандидатах от Кременчуга.

Ссылки на официальные страницы общественного движения «АЙ ЛАВ КРЕМЕНЧУГ»:

vk.com/ay_lav

facebook.com/ay.lav.Kremenchug

odnoklassniki.ru/ay.lav ***(В соц-сетях стартовал новый проект «АЙ ЛАВ КРЕМЕНЧУГ за честные выборы!» // Кременчуг Today (http://kremenchugtoday.com.ua/news.php?id=36142&year=2014&today=22&month=09). – 2014. – 22.09).***

***

Керівництво Facebook направило представникам Національної ради України з питань телебачення і радіомовлення, які просили відсторонити російського громадянина від керування українським сегментом соцмережі, відповідь на їх звернення.

«Facebook не має представництв ні в Росії, ні в Україні. Наша міжнародна штаб-квартира розташована в Дубліні, в Ірландії. Там працюють співробітники з різних країн, які надають об’єктивну підтримку користувачам Facebook з України», – цитує відповідь прес-служби компанії «Капітал».

У повідомленні соцмережі також підкреслюється, що вона працює по ряду внутрішніх правил, які є стандартними. І саме згідно з цими правилами соцмережа і розглядає кожне звернення.

«Наприклад, ці стандарти передбачають, що ми не дозволяємо користувачам знущатися над людьми або поширювати повідомлення, повні ненависті. Якщо користувачі бачать на Facebook те, що може суперечити даними правилами, ми заохочуємо їх повідомляти нам про це», – підкреслюють у соцмережі.

При цьому зазначається, що до складу команди мережі входять представники різних країн, які забезпечують неупереджено реалізацію

стандартів спільноти Facebook ***(Facebook спростував інформацію, що українським сегментом керує росіянин // INSIDER (http://www.theinsider.ua/politics/542b00b9b7a23/). – 2014. – 30.09).***

***

Як і під час будь-якої вагомої революції чи хвилі протестів за останні п’ять років, Twitter посідає важливе місце в комунікації між учасниками протестів та трансляції всього, що відбувається. Адміністрація сервісу вирішила поділитися даними щодо того, як Twitter використовувався на початку протестного руху в Гонконгу.

У пікові дні – наприклад ввечері 28 вересня – учасники гонкогських протестів відправляли понад 700 записів на хвилину.

Найпопулярнішим хештегом революції став #Hongkong ***(Twitter випустив інтерактивну візуалізацію протестів у Гонконгу // UkrainianWatcher (http://watcher.com.ua/2014/10/01/twitter-vypustyv-interaktyvnu-vizualizatsiyu-protestiv-u-honkonhu/). – 2014. – 1.10).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Сервис микроблогов Twitter представил существенно переработанный инструмент персонального тематического ретаргетинга Tailored Audiences.

В обновлённом инструменте был улучшен функционал управления аудиториями пользователей; появилась возможность привязки к инструменту номеров мобильных телефонов или ID пользователей мобильных устройств; усовершенствовались возможности таргетинга на «похожие аудитории» на ads.twitter.com . В частности, разработчики добавили возможность исключать из списка различные категории пользователей: к примеру, тех, кто переходил на сайт рекламодателя по определённым ключевым словам, видел телерекламу бренда и т. д.

«Чтобы расширить охват, вы можете использовать информацию о покупателях и формировать похожие аудитории среди пользователей мобильных устройств. Теперь мы поддерживаем ID мобильных пользователей Apple iOS и Google Android. Это значит, что теперь вы получаете возможность таргетировать рекламу на пользователей мобильных устройств, которые совершали какие-либо целевые действия в ваших приложениях или просматривали информацию о вашем продукте. Мы также интегрировали эту функциональность в Ads API», – сообщается в блоге Twitter .

Сам инструмент Audience Manager стал более функциональным и удобным, что заметно облегчило процесс создания сегментов

пользовательских аудиторий, отслеживания статистики по ним и оценки их потребительского потенциала рекламодателями.

В случае, если пользователь не желает, чтобы за ним следили, он может указать это в настройках конфиденциальности, деактивировав пункт «Реклама подбирается индивидуально и основана на информации от рекламных партнёров».

Впервые о том, что Twitter тестирует дополнительную возможность в функционале инструмента Tailored Audiences, стало известно в январе 2014 г. Новинка позволяет использовать e-mail-адреса пользователей, ранее посетивших сайт рекламодателя, и регистрационные данные в Twitter для формирования баз потенциальных клиентов и партнёров. Сам же формат персонализированной рекламы Tailored Audiences был запущен по всему миру в конце 2013 г.

В июне текущего года Twitter представил специальный тег, который позволит рекламодателю отслеживать cookies и таргетировать рекламу на пользователей сервиса микроблогов, ранее посетивших его веб-сайт. Новые возможности ретаргетинга позволяют транслировать пользователям рекламный контент, основываясь на понимании того, чем конкретно они интересовались на веб-сайте рекламодателя ***(Twitter заметно обновил инструмент ретаргетинга Tailored Audiences // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zametno_obnovil_instrument_retargetinga_tailored_audiences). – 2014. – 23.09).***

***

С 22 сентября количество рекламных постов в группах во «ВКонтакте» ограничивается пятью публикациями в сутки, минимум два из которых должны быть размещены через биржу «ВКонтакте», – сообщается в официальном разделе, описывающем правила работы сообществ.

Администраторы подписывают петицию против решения «ВКонтакте»: несогласны с новыми правилами работы уже 300 групп с суммарным количеством подписчиков около 40 млн пользователей, сообщает один из авторов петиции И. Грицкевич, представляющий сообщество DLMA SociaL o Бизнесе.

В тексте петиции говорится, что результатом новых правил станет падение эффективности «отдачи от рекламных постов, так как они затеряются в куче спама на стене (с нынешним лимитом в 200 постов в день). В связи с этим уменьшатся заказы на рекламу, от чего пострадают как владельцы пабликов и нанятые администраторы, так и владельцы «ВКонтакте».

Для разрешения конфликта администраторы предлагают ограничить количество разрешенных постов с 200 до 50 в сутки и расширить количество разрешенных ссылок на другие сообщества до 15 (включенных в лимит 50 постов в сутки), либо вовсе не ставить лимит на рекламу.

Но в администрации не планируют менять правила снова.

«Изменения правил не планируется. В данном случае наше решение связано с тем, чтобы разгрузить ленты пользователей от мусора и сделать посты их друзей и добросовестных сообществ с качественным контентом более заметными», – пояснил Cossa.ru пресс-секретарь «ВКонтакте» Г. Лобушкин.

Тем не менее, Г. Лобушкин добавил, что в социальной сети в настоящее время обсуждается вопрос снижения лимита постов в сообществах в сутки. По словам компании, решение о введении новых правил никак не связано с покупкой акций «ВКонтакте» компанией Mail.Ru Group ***(«ВКонтакте» ограничил рекламу в сообществах, администраторы готовят протест // IT Expert (http://itexpert.org.ua/rubrikator/item/38367-vkontakte-ogranichil-reklamu-v-soobshchestvakh-administratory-gotovyat-protest.html). – 2014. – 23.09).***

***

Рекламодатели осознали, что именно они приносят деньги Facebook, и массово уходят из социальной сети. Компании перераспределяют свои ресурсы в пользу менее крупных площадок вроде LinkedIn, пишет sostav.ru.

Представитель агентства признался изданию AdWeek, что клиенты бегут из Facebook, и число таких рекламодателей «впечатляет». На клиентов повлияла статистика: менеджер по соцсетям сообщил о сильном падении охвата аудитории в течение последних 16 месяцев. Провал связан с алгоритмом EdgeRank, который формирует новостную ленту пользователей.

Рекламодателей не устраивает то, что Facebook полностью контролирует контент и не позволяет влиять на него. По словам аналитика Forrester Н. Эллиота, компании признают непригодность крупнейшей соцсети для маркетинговой деятельности. Новой целью компаний является привлечение пользователей на официальные сайты. По данным Jun Group, в 2012–2013 гг. доля кликов, ведущих на сайты брендов, удвоилась с 28 до 57 %, а доля кликов на Facebook упала с 31 до 10 %.

Соцсеть М. Цукерберга неоднократно критиковали за работу EdgeRank. Как признавались маркетологи, алгоритм постоянно занижает охват, чтобы рекламодатели платили за продвижение постов ***(Рекламодатели бегут из Facebook // Media бізнес (http://www.mediabusiness.com.ua/content/view/40745/126/lang,ru/). – 2014. – 23.09).***

***

Популярная соцсеть для мобильных телефонов и планшетов Instagram объявил о начале размещения рекламы в лентах пользователей.

Компания обещает вводить рекламу постепенно и ненавязчиво, однако отмечает, что не может обойтись без этого непопулярного шага – в

следующем году Instagram планирует выйти на самоокупаемость, а значит, должен начать зарабатывать деньги.

Instagram обещает, что рекламные публикации будут максимально похожи на обычные пользовательские фотографии, и сначала реклама будет приниматься от тех компаний, которые уже самостоятельно ведут свои корпоративные ленты ***(Instagram начинает размещать рекламу в лентах пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/instagram_nachinaet_razmeschat_reklamu_v_lentah_polzovateley). – 2014. –23.09).***

***

Социальная сеть Facebook заключила соглашение с платежной системой Stripe для создания кнопки «Купить» на своем сайте.

Данная кнопка позволит пользователям соцсети покупать товары, представленные в рекламе на сайте, не покидая его.

Информацию о сделке подтвердили представители Stripe.

Stripe позволяет быстро совершать мобильные платежи, при этом пользователю необходимо ввести платежные данные только один раз. Компания уже сотрудничает с Twitter, Apple и Alipay (системой платежей от Alibaba) ***(Facebook создаст систему покупок товаров в соцсети // InternetUA (http://internetua.com/Facebook-sozdast-sistemu-pokupok-tovarov-v-socseti). – 2014. – 28.09).***

***

Французская банковская группа Banque Populaire Caisse d'Epargne готовится запустить функцию денежных переводов посредством Twitter.

Воспользоваться сервисом смогут клиенты любого французского банка. Для денежных транзакций потребуется только банковская карта и аккаунт в Twitter, к которому она будет привязана.

Достаточно будет отправить всего лишь один твит без указания реквизитов банковского счета, обозначив только сумму перевода, деньги будут списаны с карты и отправлены адресату.

Нововведение будет доступно на территории Франции со следующего месяца ***(В Twitter'е появится возможность переводить деньги // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_twitter_e_poyavitsya_vozmozhnost_perevodit_dengi). – 2014. – 29.09).***

***

Только 5 % американских взрослых пользователей Интернета совершили покупку в социальной сети, например Facebook, Twitter или Pinterest. Об этом свидетельствует опрос Harris Poll для DigitasLBi за август 2014 г.

Согласно исследованию, мотивацией к покупкам через социальные платформы могут стать лучшие меры безопасности. 42 % пользователей

заявили, что они будут более склонны сделать покупку через социальные сети, если они будут знать, что их кредитная информация была защищена. 38 % опрошенных завершили бы сделку, если бы были уверены, что информация об их покупке не распространится.

Треть респондентов были бы более склонны совершить покупку стоимостью ниже 25 дол., и последующие ответы указывают, что расходы определенно имеют влияние на использование кнопки «купить». Большинство говорит, что цена играет большую роль в их решении купить что-то на сайте социальных сетей.

Несмотря на то что многие пользователи нуждаются в приватности и безопасности социальных покупок, около четверти респондентов заявили, что не могут удержаться от покупок в социальных сетях, даже если это означает, что бренд будет знать их историю покупок.

eMarketer ожидает, что число американских пользователей социальных сетей увеличится на 4,5 % в этом году и составит 173,2 млн. Это представляет 68,5 % интернет-пользователей и 54,3 % населения, а также большую аудиторию для розничной торговли, стремящейся к социальной коммерции.

Кнопка «Купить», которая позволяет пользователям Facebook приобрести товары из объявлений или сообщений в новостной ленте, все еще находится в стадии испытаний ***(Всего 5 % американских взрослых пользователей интернета покупают в социальных сетях // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/vsego_5_amerikanskih_vzroslyh_polzovateley_interneta_pokupayut_v_sotsialnyh_setyah). – 2014. – 2.10).***

***

Социальная сеть Facebook объявила о запуске рекламной платформы Atlas, призванной усилить конкуренцию с лидером рынка онлайн-рекламы – компанией Google.

Платформа Atlas существовала ранее и принадлежала Microsoft до тех пор, пока в феврале 2013 г. ее не приобрела Facebook. С тех пор инженеры крупнейшей в мире соцсети занимались ее модернизацией и в итоге переделали платформу практически полностью, с нуля переписав ее код.

Особенность Atlas, на которой Facebook многократно сделала акцент на презентации в Нью-Йорке и на официальном сайте, заключается в «человеко-ориентированности». Во всем потоке декстопного и мобильного трафика Atlas следит за поведением конкретного человека. То есть если, например, пользователь нашел какой-то товар в Интернете с помощью мобильного телефона и затем сел за ноутбук, чтобы его купить, для платформы это будет один и тот же человек, хотя и обезличенный.

«Atlas предлагает человеко-ориентированный маркетинг, помогая рекламодателям достигать потребителей вне зависимости от устройства, платформы и издателя», – рассказал глава Atlas Э. Джонсон.

Проблема современного интернет-маркетинга, утверждают в Facebook, в отсутствии возможности задействовать те же механизмы таргетинга на мобильных устройствах, что и на настольных ПК. В частности, речь идет о куках (cookies) – фрагментах данных, которые создаются на локальном устройстве удаленным сервером и служат для хранения статистики и предпочтений пользователя.

«На мобильных устройствах куки не работают. Поэтому продавать таргетированную рекламу сложнее. И непросто определить, был ли в конечном счете товар приобретен, так как для покупки пользователь может воспользоваться другим устройством», – пояснил Э. Джонсон. Atlas, по его словам, лишена этого недостатка, так как цепляется за человека, с какого бы устройства он ни выходил в сеть.

В компании не раскрывают информацию о том, как именно они отслеживают потребителя. Как пишет Wall Street Journal, при каком-либо акте взаимодействия пользователя с рекламой, размещенной в сети Atlas, данные об этом взаимодействии отправляются в аккаунт пользователя на Facebook. Таким образом, аккаунт в Facebook служит связующим звеном при использовании устройств различного типа.

В Facebook уверены, что особенность Atlas увеличит мировые расходы на мобильную рекламу. «Платформа изменит рынок мобильной рекламы, – приводит слова представителя Facebook газета WSJ. – Потребители стали проводить больше времени за мобильными устройствами, нежели за десктопами. Но рекламодатели не спешат тратить на мобильную рекламу из-за отсутствия механизмов таргетинга. Теперь этому сегменту развиваться ничто мешать не будет».

Помимо кросс-платформенности, Atlas был наделен полностью новым интерфейсом и расширенными аналитическими инструментами.

Первым клиентом Facebook, согласившимся использовать платформу Atlas, стало рекламное бюро Omnicom, обслуживающее свыше 5 тыс. клиентов во всем мире, включая известные мировые бренды.

С запуском Atlas в новом формате, будучи второй по величине игрок рынка интернет-рекламы Facebook сможет усилить конкуренцию с занимающей лидирующую позицию Google. По данным eMarketer, компании Facebook принадлежит 6 % мирового рынка интернет-рекламы, включая мобильную рекламу. Тогда как Google – 32 %. В то же время новая платформа рождает новые вопросы, связанные с безопасностью персональных данных: что именно о пользователе будет собирать Facebook и насколько надежно сможет хранить эти сведения?

В 2013 г., согласно eMarketer, Google занял 41,5 % мирового рынка мобильной рекламы, при этом по сравнению с 2012 г. его доля сократилась (в 2012 г. – 49,8 %). Доля Facebook в прошлом году составила около 16 %, увеличившись почти вдвое (с 9 %) по сравнению с 2012 г. ***(Рекламная сеть Facebook научилась отслеживать людей при смене устройств интернет-доступа // ProstoWeb***

(http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/reklamnaya_set_facebook_nauchilas_otslezhivat_lyudey_pri_smene_ustroystv_internet_dostupa). – 2014. – 3.10).

***

Как известно, социальная сеть Pinterest недавно объявила о запуске нового функционала для рекламодателей, связанного с возможностью отслеживания конверсий и усовершенствованным таргетингом. Нововведения направлены на улучшение понимания того, как продвигаемые пины влияют на бизнес. Также стало известно, что рекламные пины станут более релевантными.

Издание TechCrunch сообщило новые детали запускаемого функционала.

Согласно информации издания, в результате нововведений рекламодатели смогут добавить отслеживающий пиксель к продвигаемым пинам, чтобы собрать информацию об их производительности. Пиксель на сайте рекламодателей поможет им понять соотношение пинов и конверсий и определить, какие покупатели пришли после просмотра или нажатия на ссылку в продвигаемом пине рекламодателя.

Эти изменения позволят брендам, использующим Pinterest в качестве рекламной площадки, лучше измерять эффективность рекламы в социальной сети. Они смогут определить не только пины, которые поощряют пользователей перейти по ссылке, и на основе которых затем подсчитываются конверсии, но и тех пользователей, которые стали покупателями после всего лишь просмотра продвигаемых пинов. Эти данные будут включены в отчеты по эффективности, а также будут использованы для показа интересных материалов пользователям.

Кроме того, рекламодатели смогут предоставить Pinterest «хэш» (анонимный шифр) или другие идентификаторы, типа e-mail адресов клиентов, которые позволят ему связать эту информацию с пользователями и сделать продвигаемые пины более релевантними ***(Pinterest запускает новый функционал отслеживания конверсий и улучшает таргетинг // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_zapuskaet_novyy_funktsional_otslezhivaniya_konversiy_i_uluchshaet_targeting). – 2014. – 3.10).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Сотрудник центра цифровой журналистки при Колумбийском университете в США К. Силверман разработал программу, демонстрирующую, что слухи и различные материалы, основанные на неподтверждённых фактах и фейковых источниках, получают в социальных сетях большее распространение, чем статьи с последующим опровержением. Об этом 29 сентября сообщает The New York Times.

Программа К. Силвермана получила название Emergent. Софт способен проводить анализ того, как проходит вирусное распространение новостного контента в Интернете и подсчитывать, сколько раз пользователи делятся той или иной статьёй за определённый период времени.

Изучив с её помощью десятки появлявшихся в СМИ инфоповодов, специалист пришёл к заключению: статьи, безоговорочно утверждающие, что какой-то слух является правдой, всегда получают в Twitter, Facebook и Google+ больше лайков и репостов, чем заметки, утверждающие, что появившийся слух – это всего лишь фейк.

Этот вывод К. Силверман проиллюстрировал графиком, который показывает распространение в соцсетях новости о женщине с тремя грудями, привлекшей в конце сентября внимание многих мировых СМИ. Опровержения этой истории появились в прессе практически сразу, однако стали активно распространяться в Twitter и Facebook только спустя двое суток.

Судя по данным Emergent, даже после появления доказательств того, что новость является фейком, количество лайков и репостов у записей, доказывавших, что женщина с тремя грудями действительно существует, продолжило расти.

С помощью программы похожий тренд можно обнаружить и при анализе большинства других новостных материалов. Например, слухи о готовящемся корпорацией Microsoft поглощении фирмы Mojang (поздее подтвердились) распространялись быстрее, чем сама новость о сделке.

Данные американского специалиста подтверждаются и статистикой новостей на TJournal. 23 сентября на сайте вышла новость о пользователях 4chan, анонсировавших массовый слив интимных фотографий актрисы Э. Уотсон. Статья собрала около 500 лайков во «ВКонтакте» и почти 100 «шэров» в Twitter и Facebook. Материал о том, что история оказалась пиар-ходом, придуманным SMM-агентством, опубликованная на следующей день, распространялась значительно слабее, получив около 250 отметок «Мне нравится» во «ВКонтакте» и всего 27 лайков в Facebook.

В мае TJournal рассказал о планах Apple встроить датчики пульса и давления в наушники EarPods. Новость публиковалась со ссылкой на британскую газету The Guardian, нашедшую информацию об этом в сервисе Secret. Анонсированная в соцсетях статья собрала почти две с половиной тысячи просмотров и около 115 лайков. Её опровержение, появившееся через пять дней, незначительно побило оригинал по количеству лайков в соцсетях, однако при этом материал всё равно набрал почти на тысячу просмотров меньше ***(Исследование: Фейковые новости в соцсетях популярнее их опровержений // InternetUA (http://internetua.com/issledovanie--feikovie-novosti-v-socsetyah-populyarnee-ih-oproverjenii). – 2014. – 3.10).***

***

Четверть пользователей Facebook назвали самыми раздражающими сообщения, содержащие хвастовство. О этом сообщает Lenta.ru со ссылкой на The Independent. Опрос на тему эмоций в соцсети провел британский ритейл-портал PromotionalCodes.

Многие интернет-юзеры также негативно отозвались о друзьях, размещающих романтические посты о своих вторых половинках. Сентиментально настроенные люди в Facebook раздражают 26 % респондентов.

На третьем месте оказались те, кто любит жаловаться на жизнь в соцсети – такие юзеры вызывают недовольство 22 % опрошенных.

Любители слишком часто обновлять онлайн-статусы не по душе 19 % респондентов. В немилости также оказались любители животных и фанаты фитнеса.

Издание не уточняет количество опрошенных пользоваталей соцсети.

Ранее в июле 2014 г. самым раздражающим типом фото в соцсетях были признаны «релфи» – автопортреты с любимым человеком ***(Названы самые раздражающие типажи пользователей «Фейсбука» // InternetUA (http://internetua.com/nazvani-samie-razdrajauasxie-tipaji-polzovatelei--feisbuka). – 2014. – 2.10).***

Маніпулятивні технології

22 вересня ціла низка українських ЗМІ поширила новину про те, що Facebook запроваджує абонентську плату за користування своїм сайтом. Звісно ж, новина виявилася фейком.

Кожен із сайтів, що опублікували фейк – а серед них опинилося навіть Громадське ТБ, посилається на новину The National Report. Видання як доказ наводить слова М. Цукерберга, де він нібито підтверджує встановлення плати за соцмережу – у розмірі 3 дол. на місяць. Оригінал новини назбирав уже

понад 140 тис. шерів, а сам сайт час від часу не витримує напливу трафіка – всі хочуть дізнатися, чи дійсно Facebook запроваджує абонентську плату.

В якості підтвердження слів М. Цукерберга, National Report також навело слова «експертів», які обґрунтовують, чому 1,4 млрд користувачів повинні платити за доступ до Facebook і наскільки вигідним це буде для самої соцмережі: в час економічної кризи та нестачі доходів від реклами, навіть якщо 2/3 користувачів почнуть платити, Facebook зможе заробити на цьому ***(Facebook не буде платним: українські ЗМІ знову поширили фейк // UkrainianWatcher (http://watcher.com.ua/2014/09/22/facebook-ne-bude-platnym-ukrayinski-zmi-znovu-poshyryly-feyk/). – 2014. – 22.09).***

***

У відповідь на активне використання бойовиками «Ісламської держави в Іраку та Сирії» (ISIS) соціальних мереж мусульмани всього світу запустили власну інтернет-кампанію проти злочинів цієї організації, повідомляє Mashable.

Активісти вигадали і почали активно використовувати у соцмережах хештег #NotInMyName (англ. «Не від мого імені»). Він має на меті нагадати світові, що ISIS не репрезентує їхню релігію.

Кампанію у соціальних медіа 10 вересня запустила базована в Лондоні Фундація активної зміни (Active Change Foundation).

«Вбивство невинної людини не має виправдання у жодній релігії чи світогляді, – каже Х. Кадір, засновник the Active Change Foundation, нагадуючи про обезголовлення бойовиками ISIS британських та американських громадян. – Ці терористи несправжні мусульмани, вони не практикують справжніх вчень ісламу (миру, милосердя та співпереживання) і є ворогами всього людства».

За останній тиждень хештег #NotInMyName використали понад 46 тис. разів.

Нагадаємо, що в серпні терористи опублікували відео, на якому обезголовлюють американського журналіста Д. Фоулі. На початку вересня у такий самий спосіб було вбито іншого журналіста С. Сотлоффа. 13 вересня з'явилося аналогічне повідомлення про британського громадянина Д. Хейнеса ***(Мусульмани запустили масштабну кампанію у соціальних медіа проти ISIS // «Медіаграмотність» (http://osvita.mediasapiens.ua/material/34880). – 2014. – 25.09).***

***

У зв'язку зі збільшенням активності інтернет-тролів у Польщі було порушено кілька кримінальних справ. Про це повідомляє видання «Новый регион» із посиланням на польський тижневик Do Rzeczy.

Розслідування веде Агентство внутрішньої безпеки Польщі, але поки що не повідомляє жодних подробиць. Хоч поки що нема загрози появи «зелених чоловічків» на польській території, триває пропагандистська війна

РФ із рештою світу за допомогою Інтенету, нагадує Do Rzeczy. У Польщі наразі активно обговорюють «Кремлівську армію тролів» та називають її «тінями Путіна».

«Новый регион» пише, що вони спамлять західні медіа, дублюючи офіційну російську пропаганду, а також нападають на тих, хто несхвально висловлюється про путінський режим.

Ідеться, зокрема про базовані у Польщі організації, наприклад Польський слов'янський комітет на чолі з Б. Тейковськийм. Активісти цієї організації підтримують дії Москви на території України та прагнуть до створення слов'янської держави. Підтримують подібні ідеї і члени Спільноти Дружби Польщі та Росії. Вони публікують у соцмережах матеріали, що дискредитують дії польського уряду в Україні. Поширенням проросійської інформації займаються також радіо Glos Rosji та журнал Obserwator Polityczny ***(У Польщі почали розслідування у зв'язку з діяльністю «кремлівських тролів» // «Медіаграмотність» (http://osvita.mediasapiens.ua/material/35087). – 2014. – 2.10).***

Зарубіжні спецслужби і технології «соціального контролю»

Із соціальної мережі Facebook видалили групу «Груз-200 из Украины в Россию», яка викривала факти російського вторгнення, повідомляла про померлих солдатів. Про це поінформувала засновниця групи, російська правозахисниця Є. Васильєва на своєму сайті.

У своїй заяві вона розкритикувала дії російських модераторів соціальної мережі. «Що і треба було довести: російські модератори Facebook більше реагують на ботів та порожні акаунти, звідки йдуть скарги, ніж на реальних учасників своєї соціальної мережі», – написала Є. Васильєва.

Правозахисниця зазначила, що адміністраторів «Груз-200 из Украины в Россию» повідомили не просто про блокування групи, а про її видалення.

«Виходить, що російські адміністратори Facebook самі порушили правила, встановлені головним офісом».

Відразу ж після видалення групи активісти створили нову групу із аналогічною назвою та закликали користувачів соцмережі скаржитися до адміністраторів з метою відновлення попереднього ресурсу.

Раніше Є. Васильєва повідомляла, що кількість російських військових, які загинули у війні проти України перевищила 3,5 тис.

Станом на 10:00 за Київським часом 24 вересня група залишається недоступною ***(Facebook видалив групу «Груз-200 из Украины в Россию» // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/34848). – 2014. – 24.09).***

***

Роскомнадзор заблокував українську соціальну мережу Politiko.ua через статтю про корупцію в судовій системі.

Як повідомив Watcher автор соцмережі Д. Лисенко, рішення № 2-3923/2014 про блокування сайту було винесене Автозаводським районним судом м. Тольятті Самарської області ще влітку, проте адміністраторів сповістили лише зараз. Д. Лисенко висловив здивування тим фактом, що сайт було заблоковано за статтю про корупцію в українській судовій системі – яким чином вона має відношення до Росії – невідомо. За його словами, це просто привід для того, щоб заблокувати ще один український ресурс на території Росії.

Виконувати рішення Роскомнадзору і видаляти «заборонений» матеріал Politiko не збирається ***(Роскомнадзор заблокував українську соціальну мережу // UkrainianWatcher (http://watcher.com.ua/2014/09/22/roskomnadzor-zablokuvav-ukrayinsku-sotsialnu-merezhu/). – 2014. – 22.09).***

***

Корпорация Apple сделала официальное заявление, в котором объявила, что операционная система iOS 8 исключает возможность получения органами государственной власти данных о владельцах iPhone или iPad.

Ключи шифрования больше не будут храниться на серверах Apple. Как сообщается, получить удалённый доступ к информации будет невозможно даже по распоряжению суда.

Компания изменила систему шифрования данных таким образом, что доступ к массиву пользовательских данных, который хранится на смартфоне или планшете, может получить только непосредственный владелец устройства.

Однако новая система шифрования может стать проблемой уже для пользователей iOS 8: теперь если владелец забудет код доступа к своему устройству, обращаться в службу технической поддержки Apple станет бесполезно.

Единственным выходом из ситуации потери кода доступа будет удаление данных и полный сброс настроек.

В то же время Apple по-прежнему доступна личная информация пользователей в «облачном» хранилище iCloud, и компания может предоставить официальным лицам все «облачные» данные, если будет предъявлен соответствующий запрос ***(Apple официально назвала iOS 8 непроницаемой для шпионажа //Блог Imena.UA (http://www.imena.ua/blog/apple-protected-ios-8/). – 2014. – 22.09).***

***

ФБР глубоко обеспокоено шифрованием пользовательских данных в iOS 8 и Android L.

Недавно компании Apple и Google практически одновременно анонсировали существенные изменения в политике конфиденциальности, в соответствии с которыми доступ к кладезю пользовательских данных, хранящихся на мобильных устройствах под управлением ОС iOS 8 или Android L, не смогут получить ни сами компании, ни госорганы. Свои опасения по поводу предпринятых Apple и Google мер по обеспечению конфиденциальности данных пользователей на недавней пресс-конференции выразил новый руководитель Федерального бюро расследований США (ФБР) Д. Коми, сообщает «ITC».

По мнению господина Д. Коми, новые меры безопасности, касающиеся шифрования данных, которые не по силам обойти даже правоохранительным органам подвергают потребителей потенциальным опасностям того или иного рода.

Данный комментарий имеет прямое отношение к недавним изменениям в политике конфиденциальности Apple и Google, которые делают невозможным доступ к огромным объемам пользовательских данных для правительства или других правоохранительных органов.

Хоть Д. Коми и понимает необходимость обеспечения неприкосновенности частной жизни потребителей, с учетом данных защитных мер, решаемые ранее с помощью соответствующего судебного разрешения чрезвычайные ситуации, становятся недосягаемыми для полиции. Д. Коми сравнивает неспособность получить доступ к хранящимся на смартфоне данным, имея на руках соответствующее судебное разрешение, с ситуацией, когда невозможно открыть запертые двери при расследовании уголовного дела о похищении ребенка.

Господин Коми также сообщил, что ФБР в настоящее время ведет переговоры с компаниями Apple и Google, чтобы выяснить, почему они рекламируют свои продукты именно таким образом, а также получить более ясное представление о работе технологи ***(ФБР недовольна жесткой политикой конфиденциальности Apple и Google // InternetUA (http://internetua.com/fbr-nedovolna-jestkoi-politikoi-konfidencialnosti-Apple-i-Google). – 2014. – 28.09).***

***

Оптичні мережі поступово поширюються світом, і чим більше міст вони з’єднують, тим спокійніше почуватимуть себе користувачі. Адже шпигунам не вдасться легко зазирнути у їхнє приватне життя. На заваді цьому стануть закони фізики, а експерти кажуть, що з часом це може привести до появи глобального квантового Інтернету.

Увагу ЗМІ та людей до шпигування спецслужб привернули відомості від колишнього співробітника Агентства національної безпеки США (АНБ)

Е. Сноудена. Він відкрив методику їхньої роботи та показав необхідність створення нових захищених ліній пересилання даних. Однак дослідники зрозуміли це ще раніше і працювали над ними. «Навіть до одкровень Е. Сноудена ми вирішили, що назрівають якісь події, – каже працівник американської дослідницької організації Battelle Д. Хейфорд. – Тому ми почали шукати кращі способи обміну інформацією».

Вони запропонували технологію квантового розподілення ключів (QKD), яка передає фотони в певному стані для генерації безпечного криптографічного ключа. Останній потім можна відправити через звичайні канали зв'язку. Такий спосіб виявляється безпечнішим за звичайне шифрування, оскільки останнє спирається на складні математичні задачі. А їх хоча важко, проте можна вирішити, якщо мати достатньо потужні комп'ютери. При цьому будь-яка спроба перехопити квантовий ключ порушить стан фотонів, і про це дізнаються відправник з адресатом. Завдяки цьому вони не будуть використовувати викрадений пароль.

Подібні лінії з квантовим захистом вже з'єднали офіси Battelle в місті Колумбусі та Дубліні, відстань між якими становить 62 км. Це була перша подібна комерційна лінія, за якою з'явилася нова в Женеві. Її створили разом з організацією ID Quantique, яка продає технологію QKD та допомогла убезпечити вибори в Швейцарії у 2007 р. від злому.

Квантове шифрування поширюється

Локальні тестування нового способу шифрування пройшли успішно, і Battelle хоче перейти до масштабнішої перевірки. Для цього компанія хоче залучити місцеву оптоволоконну мережу в американському Дубліні. Якщо все пройде гладко, то наступним етапом стане під'єднання до захищеного квантами каналу офісу у Вашингтоні, відстань до якого становить понад 650 км.

На іншій стороні планети, у Китаї, учені також з'єднують новою технологією захисту міста. Наукова група Університету науки та технології в місті Хефей створили захищену QKD мережу, яка об'єднала п'ять комп'ютерів у Хефеї та три в місті Вуху за 150 км. При цьому мережа пройшла через місто Чаоху. «З точки зору покриття, – каже один з науковців, – це найбільша квантова мережа у світі».

Досягнення науковців Хефея скоро можуть втратити статус рекорду, адже до 2016 р. влада Китаю планує прокласти лінію у 2000 км між Пекіном та Шанхаєм. Однак така мережа буде досить дорогою, адже чим більше відстань між вузлами, тим нижча пропускна спроможність. Якщо вузли у Хефеї справлялися з передачею голосу в реальному часі, то на ділянці Хефей-Вуху можна було відправляти нові ключі не більше трьох разів на секунду.

Технологія QKD унеможливить прослуховування комп'ютерних мереж

Квантовий репітер на порятунок

Одним із способів вирішити проблему низької пропускної спроможності є встановлення пристрою під назвою квантовий репітер. Його

необхідно ставити кожні 100 км через фізичні обмеження квантової фізики. Однак проблема в тому, що такого гаджета ще не існує в природі, і замість нього використовують довірений вузол із квантовим шифруванням, що значно ускладнює та здорожує всю систему.

Поява квантового репітера, за словами науковців, стане проривом, який принесе QKD звичайним користувачам. Через дорожнечу обладнання в квартири продовжать прокладати мідні дроти, однак у містах з'являться центри шифрування, які записуватимуть сотні тисяч ключів на дисковий носій користувача. Останній потім можна використати для авторизації на сервісах Google, Amazon тощо.

Проблема метаданих

Незважаючи на захищеність, технологія QKD не ховає сам факт наявності каналу комунікації. Е. Сноуден казав, що спецслужби часто не читають зміст повідомлень, а просто збирають метадані – час, місце та ім'я людей у перемовинах. Цього досить, щоб встановити зв'язки між ними та відкрити зміст їхніх розмов без зазирання в тексти їхніх листів.

Фахівці QKD працюють над цим питанням. Наприклад, вони розробляють методи відправки крихітних порцій даних, пересилання яких майже неможливо засікти. Подібне стає можливим завдяки маскуванню квантового повідомлення під оптичний шум. Подібна ідея поки лише тестується в лабораторіях, однак з розвитком квантових мереж вона може перетворитись на основний спосіб відправки інформації в них ***(Квантовий Інтернет захистить від шпигунів // InternetUA (http://internetua.com/kvantovii--nternet-zahistit-v-d-shpigun-v). – 2014. – 23.09).***

***

Департамент юстиции США предложил внести поправку в п. 41 Федеральных правил уголовной процедуры страны, которая упростит внутренним правоохранительным органам доступ к компьютерам пользователей, пытающихся защитить свою анонимность при помощи сервиса TOR или других технологий, гарантирующих анонимность.

Согласно поправке, по запросу сотрудника правоохранительных органов или государственного обвинителя, мировой судья любого округа, где могли произойти события, связанные с совершенным преступлением, имеет право выдать ордер, разрешающий использование удаленного доступа для обыска устройств и конфискации копии информации, расположенной на электронных носителях.

В том случае, если поправка будет принята, правоохранительные органы смогут законным путем получить доступ к анонимному сервису TOR и, игнорируя государственные границы разных стран, использовать ресурсы сети Интернет для сбора экстерриториальных доказательств.

Как отмечает профессор права А. Гаппур, в 2002 г. уже возникала подобная ситуация, когда один из сотрудников ФБР получил доступ к

данным, которые хранились на серверах в Челябинске. Эта информация была использована в качестве доказательства на судебном процессе. Позже Служба федеральной безопасности России возбудила уголовное дело в отношении сотрудника ФБР за несанкционированный доступ к серверам, находящимся на территории РФ.

Речь в поправке идет о так называемых Методах исследования сети (Network Investigative Techniques), которые используются правоохранительными органами для наблюдения. Эти методы могут включать скрытую загрузку файлов, фотографий и электронных писем на сервер ФБР, использование микрофона или камеры устройства для сбора аудио-и видеоинформации, а также компрометации компьютера пользователя ***(Пользователи сервиса TOR могут стать главной мишенью ФБР // InternetUA (http://internetua.com/polzovateli-servisa-TOR-mogut-stat-glavnoi-mishenua-fbr). – 2014. – 23.09).***

***

Депутати Держдуми РФ розглянуть законопроект стосовно заборони в Росії дзвінків на мобільні телефони через Skype та інші аналогічні інтернет-сервіси. Про це повідомляють «Ведомости».

Автори законопроекту пропонують внести зміни до Закону «Про зв'язок» і зобов'язати всіх операторів під час встановлення з'єднання між абонентами відображати номер того, хто телефонує, без змін. Тих, хто порушуватиме це правило, хочуть позбавляти ліцензії.

У Skype та інших подібних інтернет-сервісах номер абонента автоматично замінюється на місцевий номер, перетелефонувати на який не можна. Таким чином, в разі прийнятті нового закону, дзвінки через IP-телефонію стануть нелегальними.

Депутати-автори ініціативи кажуть, що нинішня практика дзвінків через Інтернет небезпечна для людини та суспільства. Вони запевняють, що заміна номеру ускладнює роботу спецслужб та правоохоронців. Крім того, у Держдумі заявляють, що поширення інтернет-сервісів для IP-телефонії спричинює мільярдні втрати для російських операторів і що у зв'язку з цим недоотримує і бюджет ***(У Росії пропонують заборонити дзвінки зі Skype на російські мобільні номери // Медіаграмотність (http://osvita.mediasapiens.ua/material/34852). – 2014. – 24.09).***

***

Роскомнадзор отправил американским интернет-сервисам Facebook, Gmail и Twitter уведомления о необходимости зарегистрироваться в России в качестве организаторов распространения информации, пишет «Обозреватель» (http://obozrevatel.com/politics/62975-v-rossii-prigrozili-otklyuchit-facebook-gmail-i-twitter-v-sluchae-ih-otkaza-ot-registratsii.htm).

«ВКонтакте», сервисы «Яндекса» и Mail.Ru уже включены в соответствующий реестр, «Хабрахабр» – в процессе регистрации, пишут «Известия».

По словам замруководителя надзорного ведомства М. Ксензова, «всем направили уведомления и так или иначе заставим исполнить закон. Мы с ними тоже ведем консультации и пока специально не торопим».

«Если они не будут выполнять требования российского законодательства, к ним будут применены меры административного воздействия, – отметил М. Ксензов. – Эти три ресурса должны принять решение по поводу размещения своих дата-центров в России и по законам о блогерах. Они готовятся и хотят исполнять закон».

«Возможный штраф – не главное, – отмечает начальник юридического отдела Координационного центра национального домена сети Интернет С. Копылов. – Если сайты не зарегистрируются, Роскомнадзор имеет право направить второе требование об устранении нарушения, которое должно быть выполнено в течение 15 дней. В противном случае ведомство имеет право включить площадку в черный список, то есть заблокировать ее для российских пользователей сети» ***(В России пригрозили отключить Facebook, Gmail и Twitter в случае их отказа от регистрации // Обозреватель (http://obozrevatel.com/politics/62975-v-rossii-prigrozili-otklyuchit-facebook-gmail-i-twitter-v-sluchae-ih-otkaza-ot-registratsii.htm). – 2014. – 26.09).***

***

О подготовки к блокированию в России серверов Facebook, Twitter и Google Роскомнадзором пишет в своем блоге А. Носик – известный стартап-менеджер, журналист и общественный деятель. Далее следуют выдержки из его блога.

«Изначально планировалось, что они будут заблокированы во второй половине 2016 г., но на этой неделе депутаны срочно передумали, и приняли поправки, по которым срок отключения переносится на 1 января 2015 г. Но Роскомнадзор торопится создать предпосылки ещё быстрей.

Технология отключения – двухходовка. Сначала к зарубежным сервисам предъявляется заведомо неисполнимое требование о переносе всех пользовательских данных на площадки, подконтрольные ФСБ РФ. А потом за невыполнение этого требования их отключают. Вернее, от них отключают нас.

Зарегистрировавшись в Роскомнадзоре в качестве организатора распространения информации, такой сайт должен в течение шести месяцев хранить “на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет»”. За неисполнение данного требования грозит штраф: для юрлиц – до 500 тыс. р., – объясняют связисты.

Вам, может быть, кажется, что журналисты “Известий” упустили важный нюанс: чьи именно данные подлежат хранению на территории РФ. Идёт ли тут речь только о гражданах РФ, о русскоязычных пользователях Интернета во всём мире, или о лицах с любым гражданством, находящихся в момент передачи данных на территории России?

На самом деле, журналисты “Известий” в этом не виноваты. Конечно, они могли бы задать чиновнику Роскомнадзора этот интересный вопрос, и, может быть, даже его задали, только ответ им не разрешили печатать. Суровая правда состоит в том, что ответ в 97-ФЗ вообще никак не прописан. Не сделано никакой попытки ограничить юрисдикцию думских законов и легитимную сферу интересов ФСБ РФ – ни по критерию гражданства, ни по языку, ни по географии. Если читать 97-ФЗ в том виде, в каком он написан и принят, то там речь идёт вообще о любом приёме и передаче данных – американских и европейских, японских и канадских, израильских и новозеландских, без каких-либо ограничений.

Понятно, что исполнять этот закон в том виде, в каком он принят, никто не собирается. Задача изначально так не ставилась. Ещё за 10 дней до вступления закона в силу М. Ксензов из Роскомнадзора всем объяснил, что его ведомство не будет исполнять никакие положения этого закона, кроме избирательной политической цензуры.

“Мы не ставили и не ставим себе целью организовать поголовную перепись всех популярных русскоязычных интернет-пользователей. Это малоперспективное занятие, да и закон не об этом... Предусмотренный законом реестр блогеров, который Роскомнадзор начнет вести с 1 августа, создается не для того, чтобы производить статистические подсчеты... мы не видим особой необходимости в предварительной оценке количества пользователей, которые потенциально попадают в зону действия этого закона, – статистика сформируется в ходе правоприменительной практики и будет подвижной”.

Подвижность – это, пожалуй, основное качество российского правоприменения в нынешнем сезоне. На кого завтра покажут пальцем, к тому “подвижные” и придут. Но первоочередная задача – блокировать в России Facebook, Twitter и сервисы Гугла. Дума установила крайним сроком 1 января, но Роскомнадзор спешит управиться раньше.

Не знаю, с чем связана такая спешка, в любом случае, речь идёт пока лишь о той технологии отключения, которая легко преодолима с помощью прокси и VPN» ***(Отключение Facebook, Twitter и Google в РФ является средством избирательной политической цензуры, – российский блогер // IT Expert (http://itexpert.org.ua/rubrikator/item/38484-otklyuchenie-facebook-twitter-i-google-v-rf-yavlyaetsya-sredstvom-izbiratelnoj-politicheskoj-tsenzury-rossijskij-bloger.html). – 2014. – 28.09).***

***

Популярный сервис обмена фотографиями и видеозаписями Instagram частично заблокирован в материковом Китае после того, как некоторые пользователи разместили там фото с акций протестов в Гонконге, пишет «Обозреватель» (http://obozrevatel.com/politics/27164-vlasti-kitaya-zablokirovali-instagram-iz-za-protestov-v-gonkonge.htm).

Перебой в работе приложения наблюдается с вечера 28 сентября. Пользователи по-прежнему могут зайти на свои страницы, однако разместить фотографии и обновить ленту не удается.

Причиной такой блокировки, как отмечают ряд китайских новостных интернет-сайтов, стало размещение на днях некоторыми пользователями фото с акций протестов в Гонконге, которые продолжаются уже несколько дней. Демонстранты выступают за демократизацию избирательной системы в этом Специальном административном районе КНР. По официальным данным, в ходе столкновений пострадали свыше 40 человек ***(Власти Китая заблокировали Instagram из-за протестов в Гонконге // Обозреватель (http://obozrevatel.com/politics/27164-vlasti-kitaya-zablokirovali-instagram-iz-za-protestov-v-gonkonge.htm). – 2014. – 29.09).***

***

Агентство национальной безопасности США объявило о завершении разработки единой поисковой системы для спецслужб и разведывательных организаций.

Доступ к этому «Google для шпионов» есть у более чем двух десятков силовых структур, включая ФБР, ЦРУ и Управление по борьбе с наркотиками. От рядовых пользователей поисковая система ICREACH совершенно закрыта.

В базе системы содержатся миллиарды записей о частных сеансах связи иностранных граждан и миллионы записей, касающихся граждан США, к которым не были предъявлены какие-либо обвинения.

Среди данных на секретных серверах есть номера телефонов, уникальные номера SIM-карт, адреса электронной почты и прочее.

Вся эта информация может быть использована для отслеживания перемещений, составления списка родственников и знакомых, предсказания последующих действий, выяснения религиозной принадлежности и политических предпочтений отдельных лиц.

При помощи специальных маркеров пользователи системы могут искать информацию, связанную с определёнными людьми: можно быстро получить список телефонных номеров, по которым конкретный человек звонил за последний месяц.

Разработка системы ICREACH длилась с 2005 г. Её создание обусловлено необходимостью разведывательного сообщества иметь быстрый доступ к специальной информации ***(АНБ запустило «Google для шпионов»***

// Блог Imena.UA (http://www.imena.ua/blog/google-like-nsa-search/). – 2014. – 26.09).

***

Служба безопасности Украины выявила и остановила незаконную работу скрытых каналов международной связи.

Об этом сообщили на официальном сайте СБУ. В Киеве сотрудники СБУ пресекли незаконную деятельность преступной группы, которая при помощи специального программно-аппаратного комплекса вмешивались в телекоммуникационную сеть одного из операторов мобильной связи.

В СБУ сообщили, что незаконное оборудование размещалось в квартире одного из подозреваемых. Злоумышленники использовали технологию IP-телефонии чтобы получать заграничный телефонный трафик и, под видом локальных звонков, перенаправляли его на телекоммуникационную сеть Украинских мобильных операторов.

В сообщении сказано, что противозаконная деятельность нанесла ущерб мобильным операторам. Кроме того, создание скрытых каналов международной связи могло служить для передачи любой информации, в том числе – незаконной.

Незаконно действующее оборудование было изъято сотрудниками СБУ. Прокуратура возбудила уголовное производство по признакам состава преступления, предусмотренного ст. 361 Уголовного кодекса Украины (несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи). Ведутся следственные действия ***(СБУ остановила незаконные каналы международной святи // InternetUA (http://internetua.com/sbu-ostanovila-nezakonnie-kanali-mejdunarodnoi-svyazi). – 2014. – 28.09).***

***

Последние разработки превратили смартфоны iPhone от американской компании Apple в подлинные «шпионофоны», пишет газета The Daily Mail. Основанием для этого стали оценки одного из ведущих экспертов Великобритании в сфере компьютерных технологий, профессора Н. Шарки и активистов, борющихся за неприкосновенность частной жизни.

По оценке Н. Шарки, нынешние способности устройств отслеживать поведение людей стали «пугающими». Речь идет об интегрированных в последние версии операционной системы мобильных аппаратов Apple – iOS7, iOS8 – механизмах, фиксирующих любые перемещения владельцев управляемой данным программным обеспечением электроники. Записываются, в том числе, время прибытия и убытия, частота посещений. Издание описывает все это как «скрытую систему слежения».

«Это шокирует, – отметил Н. Шарки. – Каждое место, куда вы идете, где совершаете покупки, употребляете напитки, – все это записывается. Это просто мечта адвоката на бракоразводном процессе. Но что пугает меня, так

это то, насколько это секретно». В свою очередь репортер Daily Mail Б. Спенсер отметил, что программой, «тихо введенной Apple год назад», фиксируются «точное время, когда вы ушли на работу, где купили кофе и где предпочитаете заниматься шопингом».

Функция «Частые местоположения» установлена в последних версиях операционной системы от Apple автоматически. Чтобы ограничить сбор данных, требуется углубиться в настройки аппарата на пять уровней («именно поэтому об этом мало известно»), задействуя серию шагов. Требуется как очистить «историю» в данном разделе (она тут же отображается на карте – по городам и районам), так и отключить «Улучшение карт», после чего деактивировать «Частые местоположения», указывает издание.

Оно уточняет, что указанные шаги «не остановят сбор данных» – они просто перестанут сохраняться на карте. Чтобы прекратить процесс сбора придется выключать все «Услуги, связанные с местоположением» (Location Services), а это лишит владельца возможности пользоваться картографическими программами на устройстве.

Как настаивают в Apple, информация «покидает устройство» только с согласия владельца, пользующегося «улучшением картографических сервисов», добавило издание. Но профессор Н. Шарки предостерег, что, оказавшись «в чужих руках», такие сведения «могут оказаться мощным, а подчас и опасным (инструментом)». Активисты опасаются, что доступ к подобным данным – «покопавшись» в телефоне – могут получить, к примеру, начальник или ревнивая жена, либо же они могут оказаться изъяты полицией ***(Apple превратила iPhone в «шпионофон» // InternetUA (http://internetua.com/Apple-prevratila-iPhone-v--shpionofon). – 2014. – 29.09).***

***

Донецькі терористи зобов’язали місцевих інтернет-провайдерів обмежити доступ абонентів до низки українських ЗМІ. Про це повідомляють «Новости Донбасса».

Терористи заборонили новинні ресурси, які звинуватили в «поширенні завідомо неправдивих матеріалів і наклепу».

Зокрема, під заборону потрапили сайти місцевих ЗМІ, які не підтримують ідеї сепаратизму і політику терористів ***(У Донецьку бойовики заблокували низку українських сайтів // InternetUA (http://internetua.com/u-donecku-boioviki-zablokuvali-nizku-ukra-nskih-sait-v). – 2014. – 1.10).***

***

Соцсеть Facebook и видеосервис YouTube отказали китайским властям в удалении материалов экстремистского содержания. Об этом пишет tass.ru

«В рамках кампании по борьбе с материалами порнографического и экстремистского содержания» было обнаружено, что «на крупнейших сайтах Интернета, включая Facebook и YouTube, размещены видеоматериалы

движения «Восточный Туркестан». «Данные материалы призывают к джихаду и признаны экстремистскими», – приводит издание выдержки из доклада Китайского центра отчетности по нелегальной информации в Интернете. Facebook и YouTube приложили недостаточно усилий для удаления подобной информации», – подчеркивается в документе.

Китайские эксперты полагают, что размещение в Интернете подобных материалов способствует росту террористической активности. «Практически все террористы в Китае перед терактами просматривали видео- и аудиоматериалы экстремистского содержания. Правительству КНР необходимо усилить сотрудничество с электронными СМИ в этом направлении», – считает эксперт по борьбе с терроризмом Л. Вэй. Он признал, что добиться прогресса в данном направлении и получения согласия на удаление материалов будет непросто, ведь недовольство интернет-компаний Facebook и YouTube вызывает уже то, что доступ к их сервисам в Китае заблокирован.

Исламское движение «Восточный Туркестан» признано Советом Безопасности ООН террористической организацией. Оно выступает за отделение Синьцзян-Уйгурского автономного района (СУАР) от КНР. На ее счету ряд терактов в Синьцзяне, жертвами которых были как гражданские лица, так и военные ***(Facebook и YouTube отказали Китаю в удалении материалов с экстремистским содержанием // Медіа бізнес (http://www.mediabusiness.com.ua/content/view/40844/126/lang,ru/). – 2014. – 2.10).***

***

На закритому засіданні Радбезу Росії було прийнято рішення щодо підвищення інформаційної безпеки в російському сегменті Інтернету. Участь у засіданні брав і російський президент В. Путін.

За словами В. Путіна, влада не буде закривати доступ до Інтернету та ставити його на тотальний контроль. «Свобода ЗМІ, право громадян на отримання та поширення інформації – це базові принципи демократичної держави і суспільства і їх необхідно неухильно дотримуватися», – цитує його слова агенція ІТАР-ТАСС. Водночас В. Путін заявив, що сайти з незаконним контентом будуть закриватись.

Голова Мінкомзв'язку РФ М. Никифоров звітував з результатами дослідження літніх навчань, під час яких перевіряли російський сегмент Інтернету на предмет протидії інформаційним загрозам. Саме через цей звіт кілька тижнів тому низка ЗМІ заявили про можливість повного відключення Росії від зовнішнього Інтернету. М. Никифоров заявив, що Росія створить дублюючі елементи інфраструктури та працюватиме з іноземними партнерами для того, аби забезпечити стабільну роботу та захист від атак.

В. Путін у свою чергу заявив, що певні держави намагаються використати своє домінуюче положення в глобальному інформаційному

просторі для досягнення не лише економічних, а й військово-політичних цілей. Що саме за держави, він не уточнив.

Як пише РБК, результати літніх навчань засекречені, але думки щодо підсумків розділились: у владі вважають, що серйозної загрози не існує, а в Кремлі та спецслужбах навпаки, хочуть активно діяти на випадок можливих загроз ***(Путін розповів, що Росія робитиме з Інтернетом // InternetUA (http://watcher.com.ua/2014/10/02/putin-rozpoviv-scho-rosiya-robytyme-z-internetom/). – 2014. – 2.10).***

***

Держпідприємництво отримало на розгляд від Державної служби інтелектуальної власності України проект Закону «Про внесення змін до деяких законодавчих актів щодо захисту авторського права і суміжних прав у мережі Інтернет».

Законодавчі ініціативи у сфері Інтернету дозволять закривати сайти без рішення суду. Проект передбачає, що після отримання скарги від правовласника держслужба буде повідомляти провайдерів, що на певному ресурсі є піратський контент (при цьому достовірність інформації, викладеної заявником у заяві, не перевіряється, і достатньо нотаріально засвідченого скріншоту такої веб-сторінки. Тобто без будь-яких правових підстав). Протягом одного дня компанія повинна повідомити власника сайту про скаргу. Якщо той не вживатиме заходів з видалення піратського контенту або не подасть заперечення на претензію правовласника, провайдер буде зобов’язаний сам заблокувати або видалити контент. За невчасне блокування сайту провайдери нестимуть адмінвідповідальність (штраф до 17 тис. грн).

Через значну кількість суперечливих Конституції України, Цивільному кодексу України, вимогам міжнародно-правових актів змін, Держпідприємництво відмовило в погодженні цього документа.

Досвід більшості розвинутих країн світу демонструє, що блокування веб-сайтів зазвичай здійснюється за рішенням суду. Натомість, проектом пропонується наділити таким повноваженням навіть не органи державної влади (які в межах компетенції можуть обмежувати права особи чи позбавляти її цих прав у разі порушення законодавства), а суб’єктів господарювання, які надають послуги з доступу веб-сайту до мережі Інтернет.

Держпідприємництво категорично не погоджується із запропонованою редакцією та вважає, що єдиною підставою для блокування веб-сайту має бути належно аргументоване рішення суду. Відсутність будь-якої відповідальності заявника при позасудовому порядку блокування веб-сайтів дозволить узаконити механізм безперешкодного блокування «незручних» інтернет-ресурсів.

До того ж прийняття законопроекту у такій редакції:

– порушує право на поширення інформації власниками сайту і право користувачів сайту на доступ до інформації;

– сприяє зловживанню правом на звернення;

– запроваджує «презумпцію вини»: після звернення заявника сервісна служба може одразу, не перевіряючи суті претензій, блокувати адресу мережі Інтернет. Провайдер не з'ясовує вини власника сайту ***(Законодавчі ініціативи у сфері Інтернету дозволять закривати сайти без рішення суду // Бучанський Інтернет сайт (http://bucha.com.ua/?newsid=1151071944). – 2014. – 2.10).***

***

Госспецсвязи упрощает работу шпионам?

В прошлом месяце Кабмин наконец-то распорядился передать от «Укртелекома» в госсобственность выделенную телекоммуникационную сеть специального назначения (ТССН). С 1 ноября 2014 г. ее правопреемником станет Государственная служба специальной связи и защиты информации (ГСССЗИ).

Как мы уже писали, создание ТССН было одним из условий приватизации «Укртелекома». Согласно распоряжению Кабинета Министров Украины от 12 октября 2010 г., сеть для госорганов должны были построить в течение двух лет, на что из госбюджета выделили 231,6 млн грн. Однако во времена В. Януковича техническое задание на построение ТССН подменили. После подмены ТЗ, во время руководства ДСС ЗЗИ Л. Нетудыхатой, государство за сотни миллионов гривен получило «облачную отмазку» дельцов от власти и бывшего руководства «Укртелекома».

Теперь до 1 ноября «Укртелекому» предстоит придумать, как передать на баланс государства «облако», а Госспецсвязи – как перевести на облачные сервисы, в первую очередь, все силовые структуры страны. В дальнейшем с помощью ресурсов ТССН Госспецсвязи планирует «реабилитировать» Национальную систему конфиденциальной связи (НСКС), которая может обеспечивать связью Минобороны. Таким образом, в недалеком будущем пользователями «облаков» могут стать и украинские военные. Скорее всего, на этом цепочка не прервется, и в обязательном порядке «уйдут в облака» и все остальные госструктуры.

Помня историю Э. Сноудена, InternetUA решил разобраться, как сложившаяся ситуация отобразится на информационной безопасности страны.

Этим письмом руководство Госспецсвязи в очередной раз подтвердило нам, что верит в надежность облачных технологий, и не считает, что ТССН недостаточно защищена.

Однако большинство специалистов телеком-рынка не согласны с позицией госоргана. Мало кто верит и в то, что после передачи ТССН на баланс государства власть действительно начнет тратить средства на ее нормальное обустройство, а не обойдется «облаками». Никто не забыл и о том, что при проектировании сети спецназначения использовались не только

российские программные продукты, но частично и технические средства произведенные для Украины.

Председатель комиссии УСПП по вопросам науки и IT И. Петухов:

«На мой взгляд, данное постановление Кабмина весьма странное. Особенно учитывая тот факт, что вопрос технологии построения ВАТ "Укртелеком" так называемой "защищенной" ТССН обсуждается уже не один день и на всех уровнях, начиная от проверок СБУ и КРУ, заканчивая запросами народных депутатов и информацией в прессе.

После подмены ТЗ государство за сотни миллионов гривен получило "облачный" развод дельцов от власти и бывшего руководства "Укртелекома", а также легко контролируемую любыми спецслужбами мира сеть. На деле это выглядит следующим образом. За огромные деньги "Укртелеком" продал порты в своей транспортной DWDM-сети с последней милей до района. Да еще и подсадил государство на неплохое ежемесячное обслуживание и обеспечил себе миллионный доход за счет бюджета. И все бы хорошо, вот только Фонд госимущества пока не научился ставить на баланс «разноцветные» фотоны! Хотя «новоявленные» профессионалы из Кабинета министров могут их толкнуть на данный непродуманный шаг, и они совершат должностное преступление.

"Укртелеком" должен передать в государственные руки физическую сеть, а не "облако". Даже если представить себе, что "Укртелеком" отдаст ГСССЗИ пару волокон по всей стране, за свой счет установит всю необходимую аппаратуру и передаст ее в государственную собственность, то если не отдать места прохождения и установки данного оборудования (т. е. всю инфраструктуру, в том числе с кабельной канализацией электросвязи), то у частной компании "Укртелеком" останется беспрепятственный доступ ко всем критическим элементам ТССН, со всеми вытекающими последствиями. И мы все прекрасно знаем, кто именно стоит за "Укртелекомом" – Р. Ахметов и В. Янукович. И и какая же здесь секретность и защищенность? Кому мы отдаем правительственную сеть?!»

А. Кульчицкий, директор ДП «УкрМОТ»:

«Главный вопрос состоит в том, насколько эффективно может действовать собственник ТССН. Например, если в госсобственность перейдет кабельная канализация, как активно государство будет отрывать деньги от других направлений для ее обслуживания и эксплуатации? Сейчас она не оборудована ни сигнализацией, ни камерами наблюдения, и туда может попасть кто угодно. И я не уверен, что в случае ее передачи в руки государства что-то изменится.

Собственник должен обеспечить эффективную защиту кабелей спецсвязи от физического повреждения. Кто это лучше сделает – государство или частный бизнес, сказать сложно. А пока достаточно поднять несколько люков, бросить коктейль Молотова, и не будет ни Интернета, ни связи. Ни специальной государственной, ни обычной.

По поводу облачного решения. Без физической инфраструктуры обеспечить информационную безопасность специальной связи невозможно. Все прослушивается. Существует аппаратура, которая позволяет осуществлять перехват по оптике. Это легко сделать, имея физический доступ к кабелю. Оптические кабели должны находиться на балансе государственных структур. А чья должна быть канализация, вопрос спорный, так как ее часть вообще находится на балансе у частных операторов, которые сами же ее и строили.

При помощи шифрования вопрос защиты ТССН частично решается, но остается человеческий фактор. То есть ключ всегда можно получить другим путем, даже не имея доступа к инфраструктуре. Вот вам и эффект Э. Сноудена. Обеспечить сохранность ключей, когда к ним имеет доступ огромное количество людей, достаточно сложно. Если бы работу и обслуживание ТССН поручили роботам, тогда вопрос был бы снят. Но пока еще такого никто не придумал».

М. Пергаменщик, адвокат, старший юрист практики IT и меда права АО «Юскутум»:

«На сьогоднішній день в Україні відсутнє спеціальне правове регулювання “хмарних” технологій. Так, поняття “хмарних” технологій зустрічається в “Стратегії розвитку інформаційного суспільства в Україні”, схваленої розпорядженням КМУ № 386-р від 15.05.2013 р. та постановою КМУ № 397 від 17 травня 2012 р., але там навіть не розкривається його зміст.

З юридичної точки зору, діяльність у сфері “хмарних” сервісів може бути пов’язана з використанням об’єктів права інтелектуальної власності (об’єктів авторського права, комерційної таємниці тощо), обігом персональних даних (в т. ч. з транскордонною передачею персональних даних), і навіть з діяльністю, що підлягає ліцензуванню: використання засобів криптографічного захисту інформації і надання повноцінних телекомунікаційних послуг.

Така конструкція, як “продаж”, є характерною для речових відносин, де об’єктом продажу є матеріальна річ. Коли мова йде про “продаж технології”, то під цим зазвичай розуміють відчуження прав на комплекс об’єктів інтелектуальної власності із наданням різних супутніх послуг на підставі відповідного договору.

Що стосується обліку об’єктів інтелектуальної власності, то це питання регулюється Положенням (стандартом) бухгалтерського обліку 8 “Нематеріальні активи” та Порядком застосування типових форм первинного обліку об’єктів права інтелектуальної власності у складі нематеріальних активів.

До речі, статтею 8 Закону України “Про захист персональних даних” передбачено право суб’єкта персональних даних знати, хто є володільцем і розпорядником його персональних даних, а також фактичне місцезнаходження цих даних. Під поняттям “місцезнаходження” законодавець розуміє фактичну адресу зберігання носіїв інформації. Але

ключовою характеристикою “хмарних” технологій є те, що всі процеси відбуваються “в хмарі”, тобто зберігання і обробка даних відбувається одночасно в багатьох місцях, і дані можуть постійно мігрувати. В таких умовах сервіс-провайдеру буде важко повністю виконувати вимоги законодавства про захист персональних даних».

Также мы отправили официальный запрос в ВАТ «Укртелеком», в котором поинтересовались, сколько составит абонентская плата за ТССН для государственных учреждений ежемесячно за каждую точку доступа. На наш запрос (уже традиционно) не ответили, зато поспешили «оправдаться» на официальном сайте.

Остался один вопрос без ответа. Если через некоторое время секреты государства Украина по вине разработчиков или продажных исполнителей «уйдут» в руки врага (на которого уже работает Э. Сноуден) и произойдёт очередной «иловайскгейт», кто своей головой ответит за «передовую технологию»? ***(Госспецсвязи упрощает работу шпионам? // InternetUA (http://internetua.com/gosspecsvyazi-uprosxaet-rabotu-shpionam-3). – 2014. – 4.10).***

***

Государственная дума России окончательно одобрила законопроект, согласно которому вводятся тюремные сроки за публичные призывы к экстремизму с помощью Интернета, а также за финансирование экстремистской деятельности. За экстремизм в сети теперь можно угодить в тюрьму на пять лет, за финансовую помощь экстремистам суд имеет право наказывать шестью годами заключения. Поводом для уголовной статьи может стать репост или лайк провокационных записей в Интернете.

За финансирование группировок экстремистской направленности предполагаются: штрафы от 300 тыс. до 500 тыс. р.; лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет; обязательные работы на срок до 200 часов; исправительные работы на срок от одного года до двух лет; лишение свободы на срок до трех лет. Если преступление будет совершено с использованием служебного положения, максимальное наказание составит шесть лет тюрьмы.

Что касается Интернета, то меры по контролю за пользовательским контентом снова ужесточились. Отныне распространение в сети экстремистской информации – уголовно-наказуемая деятельность, при этом, судя по последним событиям, достаточно поставить лайк или сделать репост какого-либо подобного материала.

Так, наказание за публичные призывы к экстремизму в Интернете – принудительные работы или лишение свободы до пяти лет. Аналогичным образом дополняется и известная статья 282 («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства») – под нее теперь также будут подпадать соответствующие преступления, совершенные в информационном пространстве, например, в сети.

Также в МВД РФ разработали стратегию противодействия экстремизму в России до 2025 года. Ее цель – на фоне сохранения силовой составляющей борьбы с экстремистскими проявлениями «кардинально повысить эффективность противодействия радикальной идеологии, поставить надежные барьеры на путях ее проникновения в общественное сознание». Основной акцент в документе сделан на информационном подавлении «экстремистов». Для этого предложено вести мониторинг СМИ и Интернета и разработать новые способы «ограничения доступа» к вредной информации.

Стоит подчеркнуть, что принятый Госдумой закон, скорее всего, облегчит правоохранителям доказательство вины в таких случаях, как с оппозиционером Д. Бычковым, которого обвинили в призывах к терроризму за перепост картинки с пулями и комментарий в социальной сети «ВКонтакте». В Барнауле в настоящее время начинается процесс по этому делу, сообщает портал «ОВД-Инфо».

Добавим, что это не первая история, связанная с репостами записей. Так, в январе 2014 г. Сотрудники ФСБ задержали в здании Московского государственного университета им. М. В. Ломоносова доцента философского факультета В. Дмитриева из-за перепоста публикации в Интернете. Его заподозрили в экстремизме. По словам В. Дмитриева, в статье, которая была почти сразу удалена из общего доступа, речь шла о возможной смене власти в России. «Текст жесткий, но я его подавал теоретически, как возможный сценарий», – подчеркивал В. Дмитриев ***(Госдума России одобрила закон о тюремных сроках за лайки и репосты в интернете // InternetUA (http://internetua.com/gosduma-rossii-odobrila-zakon-o-tuaremnih-srokah-za-laiki-i-reposti-v-internete). – 2014. – 3.10).***

Проблема захисту даних. DDOS та вірусні атаки

Аргентинские хакеры атаковали официальные сайты Херсонщины.

Похоже, что работой чиновников Генической райгосадминистрации недовольны не только жители района. 23 сентября, при заходе на официальный сайт Геническої РГА мы попадали на страницу, на которой сообщалось, что сайт взломан хакерами из Аргентины, сообщает «Новый Визит».

На момент написания статьи, на сайте идет патриотический ролик о революции на Майдане, а также выложены материалы против российской агрессии в Украине. По состоянию на 9 часов 23 сентября сайт еще взломан. Судя из текста, хакеры хотят показать, что безопасность сайта также плоха, как политика бывшего Президента В. Януковича и Партии регионов, чьи люди оккупировали власть в Геническом районе.

При этом издание «Херсонцы» сообщает, что в ночь с 22 на 23 сентября была предпринята попытка незаконного вторжения в файловую

систему сразу нескольких сайтов органов власти и местного самоуправления Херсонской области, в результате которой была нарушена работа официального сайта Херсонского областного совета и ряда официальных сайтов районных администраций и местных советов области.

Ответственность за хакерскую атаку взяли на себя неизвестные злоумышленники из анонимной группы hackers argentinos, которые используют элементы символики известной преступной компьютерной группировки Anonymous.

Как сообщили специалисты коммунального предприятия Центр электронного самоуправления Херсонского областного совета, изначально компьютерной атаке подверглись сайты органов власти Генического района области, а затем уже была нарушена работа около десятка официальных сайтов органов власти и местного самоуправления Херсонской области.

Версий, почему именно не политические официальные сайты подверглись незаконному вторжению, рассматриваются разные – идет расследование ситуации. Специалисты КП «ЦЭС» уже подали соответствующие заявления в правоохранительные органы и работают над восстановлением работы сайтов, которые подверглись хакерской атаке ***(Аргентинские хакеры атаковали официальные сайты Херсонщины // ХЕРСОН Онлайн (http://khersonline.net/novosti/politika/29356-sayt-genicheskoy-raygosadministracii-vzloman-argentinskimi-hakerami.html). – 2014. – 23.09).***

***

После крупных презентаций и заявлений от компании Apple количество фишинговых писем, нацеленных на пользователей продуктов калифорнийской корпорации, значительно увеличилось. Как сообщает Internet Storm Center при институте SANS, в его распоряжении оказалось письмо, отосланное якобы от имени компании Apple.

Письмо предупреждает пользователя, что в течение 48 часов срок действия его учетной записи истечет. Для того чтобы сохранить доступ к своему аккаунту, жертве необходимо перейти по ссылке и ввести свои логин и пароль. В противном случае злоумышленники угрожают ограничить доступ пользователя к сервисам Apple.

Л. Зельцер из ZDNet также сообщил о получении фишингового письма. В нем указывалось, что кто-то изменил финансовые данные его учетной записи, и для восстановления доступа предлагалось перейти по ссылке. Она вела на веб-сайт под управлением уязвимой версии WordPress, который перенаправлял пользователя на страницу злоумышленников.

По словам Л. Зельцера, сообщение было оформлено в виде официального уведомления от Apple и было почти неотличимо от оригинала. Тем не менее, его внимание привлекло то, что в конце письма были указаны контактные данные офиса компании в Греции ***(Злоумышленники нацелились на пользователей Apple // InternetUA***

(http://internetua.com/zloumishlenniki-nacelilis-na-polzovatelei-Apple). – 2014. – 23.09).

***

Интернет-сервис бронирования туристических туров Viator, используемый приложением TripAdvisor, сообщил о возможной утечке персональных данных 1,4 млн клиентов. По предварительной оценке, скомпрометированными могут оказаться платежные данные 880 тыс. пользователей. Кроме того, в руках злоумышленников, вероятно, оказались адреса электронной почты и пароли еще 560 тыс. клиентов сервера.

Утечка данных оставалась незамеченной до тех пор, пока Viator не получил информацию извне о мошеннических транзакциях. Подобная ситуация имела место и в случаях с хищением реквизитов платежных карт Home Depot, Target, Neiman Marcus и др. Viator сообщает , что уведомление о незаконных платежах поступило 2 сентября от одной из процессинговых компаний, занимающихся обработкой электронных платежей.

Viator утверждает, что незамедлительно приняла исчерпывающие меры по расследованию инцидента, оценке масштабов ущерба и усовершенствованию защиты своей платежной системы. Есть основания полагать, что три или четыре цифровых защитных кода, которые наносятся на оборотную или лицевую сторону платежных карт, остались нескомпрометированными. Кроме того, поскольку Viator не сохраняет PIN-коды дебетных карт, владельцы этого вида платежных карт не пострадали.

По утверждению К. Бойда из Malwarebytes Labs, злоумышленники пока не опубликовали похищенные данные. Тем не менее, исключать подобную возможность нельзя, уверен специалист.

Хорошая новость заключается в том, что если данные клиентов до сих пор не задействованы в мошеннических транзакциях, то клиентам уже ничего не угрожает. Похищенные платежные данные не подлежат длительному хранению, поскольку обнаружить хищение и заблокировать карту – это лишь вопрос времени ***(Хакеры похитили персональные данные 1,4 млн клиентов Viator // InternetUA (http://internetua.com/hakeri-pohitili-personalnie-dannie-1-4-mln-klientov-Viator). – 2014. – 24.09).***

***

Подарки любят все, и мошенники ловко этим пользуются, причем действуют по давно известным несложным схемам. Так, после того как iPhone 6 поступил в широкую продажу, эксперты международной антивирусной компании Eset обнаружили новые кибератаки, маскирующиеся под массовые спам-рассылки в социальных сетях и электронной почте, а также вредоносные ссылки на eBay.

В частности, на Facebook массово рассылались посты о «розыгрыше iPhone 6». Желающим поучаствовать предлагалось установить специальное приложение, ответить на несколько вопросов и указать контактную информацию, включая номер телефона. Выполнив все условия, пользователь

попадал на страницу с сообщением об ошибке, по всему списку его друзей рассылался спам, а на номер мобильного подключались дорогостоящие платные услуги.

В другом случае мошенники продемонстрировали еще один, также давно известный подход. На eBay размещались объявления о продаже подержанных iPhone предыдущих поколений, содержащие ссылки на фишинговые страницы, созданные для хищения логинов и паролей.

По словам ИБ-эксперта компании М. Джеймса, подобные схемы действуют много лет и по-прежнему эффективны. «Пользователи прекрасно знают поговорку про бесплатный сыр, но продолжают переходить по подозрительным ссылкам или “расшаривать” посты мошенников в надежде на подарок. Просто задумайтесь – вы же вряд ли поверите тому, кто постучит в дверь вашего дома и предложит iPhone 6 в обмен на заполнение анкеты?!» – подчеркивает он ***(Злоумышленники используют iPhone 6 для похищения пользовательских даннях // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-iPhone-6-dlya-pohisxeniya-polzovatelskih-dannih). – 2014. – 25.09).***

***

Служба безпеки України попереджає, що проти українських громадян російські спецслужби проводять інформаційно-технічні атаки для взяття під контроль інформаційно-телекомунікаційних систем та персональних комп’ютерів.

Від імені Державної фіскальної служби України з електронних поштових скриньок kabminonline@minrd.gov.ua, nalogs_ki@minrd.gov.ua, nalogs@minrd.gov.ua та nalogs_ua@minrd.gov.ua розповсюджуються листи, які містять шкідливі віруси, повідомили Еспресо.TV у прес-центрі СБУ.

Встановлено, що ці електронні адреси не зареєстровані в Державній фіскальній службі України, при цьому вони мають доменне ім’я, подібне до офіційних електронних адрес органів державної влади України.

Такі «замасковані» повідомлення начебто мають актуальну для громадян інформацію про сплату податків на нерухоме майно. Для того, щоб спонукати отримувача відкрити прикріплений файл, у листі містяться погрози можливих санкцій – подання судових позовів, накладання арешту на зарплатну або пенсійну картку, нарахування пені на суму заборгованості.

Фахівці СБУ застерігають, що у додатках до електронних листів наявне шкідливе програмне забезпечення. При отриманні кореспонденції із цих електронних поштових адрес вірус уражає комп’ютерне обладнання та робить його підконтрольним зовнішньому впливу.

СБУ встановлює злочинців, які розсилали людям листи з комп’ютерними вірусами.

Радник голови СБУ М. Лубківський закликав громадян бути обережними і пильними.

«Звертаємо увагу, що повідомлення надсилаються російською мовою та містять юридичні терміни, властиві правовій системі саме Російської Федерації. Тобто російські спецслужби навіть не ховають “вуха”, або у них такі “фахівці”. Щоб не потрапити у пастку російських хакерів достатньо просто не відкривати такі листи».

Про протиправні кібератаки громадяни можуть повідомити за безкоштовним номером 0 800 501 482 або на електронну скриньку callcenter@ssu.gov.ua ***(В СБУ розповіли, як ідентифікувати електронні листи з вірусами, які розсилає українцям ФСБ // Espreso.tv (http://espreso.tv/news/2014/09/26/v_sbu_rozpovily__yak_identyfikuvaty_elektronni_lysty_z_virusamy__yaki_rozsylaye_ukrayincyam_fsb). – 2014. – 26.09).***

***

Новая модификация трояна BlackEnergy использовалась для атаки на государственные и коммерческие организации в Украине и Польше, сообщает Газета.Ru со ссылкой на экспертов антивирусной компании ESET.

В отличие от старых версий, новейший BlackEnergy используется для направленных атак. На это указывают используемые плагины, а также характер новой кампании и потенциальные жертвы – корпоративные пользователи в Украине и Польше.

«Мы изучаем эволюцию BlackEnergy и детально рассматриваем плагины трояна, обеспечивающие его работу, а также дополнительные возможности и функции, – заявил Р. Липовски, вирусный аналитик ESET. – Новейшие версии трояна, обнаруженные в сентябре этого года, демонстрируют, что он все еще крайне опасен. Особенно интересна последняя вредоносная кампания BlackEnergy, поскольку она может иметь отношение к текущей геополитической ситуации на востоке Украины».

В новейшей кампании по распространению BlackEnergy используются уязвимые лакуны в программах, а также методы социальной инженерии, фишинг и сочетание всех этих инструментов ***(Хакеры использовали троян BlackEnergy для DDoS-атак на Польшу и Украину // InternetUA (http://internetua.com/hakeri-ispolzovali-troyan-BlackEnergy-dlya-DDoS-atak-na-polshu-i-ukrainu). – 2014. – 26.09).***

***

Эксперты в области информационной безопасности обнаружили в программном обеспечении Linux новую уязвимость, которая может оказаться опаснее, чем найденная в апреле ошибка Heartbleed, сообщает Reuters со ссылкой на данные Департамента внутренней безопасности США.

Мишенью для хакеров, по словам специалистов, стало приложение под названием Bash, которое используется в Linux для управления командной строкой. Используя уязвимость, злоумышленники могут получить полный контроль над взломанной системой.

Ошибка в Bash, фактически открывающая хакерам доступ ко всем ресурсам компьютера-жертвы, обнаружена в системах Linux, которые устанавливаются как на домашние компьютеры, так и на интернет-серверы, а также в программных платформах Mac OS X.

По словам Т. Бердсли, руководителя отдела кибербезопасности в компании Rapid7, уязвимость в Bash получила максимальную оценку «10», что говорит о легкости ее использования для организации различных кибератак. «С помощью этой уязвимости злоумышленники потенциально могут проникнуть в операционную систему, внести в нее изменения и т. д.», – заявил Т. Бердсли.

Эксперт также подчеркнул, что администраторы любых систем, использующих Bash, должны немедленно загрузить обновление. При этом, по утверждению других специалистов, часть патчей, направленных на устранение ошибки, на самом деле ее не устраняют, а обновление безопасности для Mac OS X пока еще не создано. Пока корректные исправления не будут установлены, каждый подключенный к Интернету компьютер на Linux или Mac остается уязвимым для хакеров.

В настоящее время под управлением Linux работают, по разным оценкам, от 62 до 82 % всех серверов в Интернете (данные Security Space на февраль 2012 г.). Что касается домашних компьютеров, то Linux и Mac OS X установлены суммарно на 8,4 % компьютеров во всем мире. По состоянию на июнь 2013 г. к Интернету подключено 2,4 млрд устройств в различных странах ***(На сотнях миллионов компьютеров найдена опаснейшая уязвимость // InternetUA (http://internetua.com/na-sotnyah-millionov-kompuaterov-naidena-opasneishaya-uyazvimost). – 2014. – 26.09).***

***

Європейські регулятори поновили свій тиск на Google стосовно зміни її налаштувань приватності. Про це повідомляє BBC.

Такі претензії вперше були висунуті після того, як два роки тому контролюючі органи помітили з боку американської компанії порушення європейських правил. Одна з вимог до Google стосується того, що компанія має розповідати користувачам, яку саме інформацію вона збирає та з ким нею ділиться.

Google каже, що працює із регуляторами з метою «пояснити їм зміни політики приватності».

Суперечки розпочалися після того, як у березні 2012 р. Google об’єднала 60 своїх політик приватності в одну і почала змішувати дані з YouTube, Gmail та Google Maps. Користувачі при цьому не мали можливості відмовитися від якоїсь із опцій.

Хоча Google прямо не звинуватили у незаконних діях, їй закидали надання «неповних та приблизних» деталей та зростання «глибокої стурбованості стосовно захисту даних та поваги до Європейського права».

Як заявив агентству Reuters речник Google, компанія в перспективі хоче обговорити нові правила із європейськими регуляторами з питань приватності.

При цьому регулятори окремих країн (Італії, Франції, Іспанії, Німеччини, Великої Британії та Нідерландів) розпочали розслідування стосовно питань приватності у користувацькій політиці Google. У січні Франція оштрафувала Google на 150 тис. євро за невиконання правил стосовно приватності ***(Європейські регулятори закликають Google змінити правила щодо приватності // Osvita.MediaSapiens (http://osvita.mediasapiens.ua/material/34959). – 2014. – 28.09).***

***

Вскоре после обнаружения критической уязвимости ShellShock эксперты выявили ботнет, эксплуатирующий брешь. Исследователь по имени Инетт (Yinette) сообщила об найденном ботнете на своей странице в Github.

Эксперт компании Rapid 7 Д. Эллис написала в своем блоге о находке и детально описала уязвимость ShellShock. По ее словам, брешь может затронуть огромное количество устройств под управлением Linux. Тем не менее, далеко не все устройства могут оказаться зараженными.

Как объяснила Д. Эллис, для эксплуатации уязвимости хакеры должны иметь возможность отправить вредоносную переменную окружения программе, взаимодействующей с сетью и использующей Bash. По ее словам, больше всего подверженными этой бреши будут устаревшие веб-приложения со стандартной имплементацией CGI.

По словам эксперта, пока оценить степень угрозы невозможно. Тем не менее, факт того, что ботнет был обнаружен уже спустя несколько часов после публикации деталей ShellShock, вызывает значительные опасения.

Д. Эллис посоветовала установить исправление, выпущенное компанией Red Hat. Оно не устраняет уязвимость, но позволяет значительно уменьшить риск компрометации системы. В скором времени будет выпущена финальная версия обновления, которая окончательно исправит ShellShock ***(Обнаружен ботнет, эксплуатирующий уязвимость ShellShock // InternetUA (http://internetua.com/obnarujen-botnet--ekspluatiruuasxii-uyazvimost-ShellShock). – 2014. – 28.09).***

***

Экс-глава социальной сети «ВКонтакте» П. Дуров сообщил, что на серверы мессенджера Telegram идет мощная DDoS-атака.

«Никогда не видел такую мощную DDoS-атаку, какую мы имеем сегодня в Telegram. Раньше я уже сталкивался с подобной “мерзкой” атакой в период работы во “ВКонтакте”», – говорится в сообщении П. Дурова в Twitter.

Telegram позиционируется как «самый быстрый мессенджер в мире» для смартфонов, позволяющий обмениваться как текстовыми сообщениями,

так и файлами. С его помощью можно создавать групповые чаты (включающие до 200 участников), отправлять медиа-вложения и видео до полутора гигабайт. Аккаунт в Telegram привязан к номеру телефона.

В июне Telegram был признан самым быстрорастущим стартапом года: всего за несколько месяцев аудитория мессенджера набрала более 35 млн пользователей ***(Павел Дуров сообщил о мощной DDoS-атаке на мессенджер Telegram // InternetUA (http://internetua.com/pavel-durov-soobsxil-o-mosxnoi-DDoS-atake-na-messendjer-Telegram). – 2014. – 27.09).***

***

За период с апреля по июнь участники Антифишинговой рабочей группы (APWG) обнаружили порядка 128,4 тыс. сайтов-ловушек, созданных фишерами. Согласно статистике APWG, этот показатель немногим выше, чем в предыдущем квартале и второй по величине за последние два года. За отчетный период борцы с фишингом получили от пользователей около 171 тыс. уникальных отчетов о фишинговых рассылках.

Как и прежде, большинство обнаруженных сайтов-имитаций имели американскую прописку; в апреле-июне на долю США приходилось от 35,6 до 48 % таких находок. При этом больше половины фиш-сайтов были привязаны к TLD-зоне .COM; лидером среди региональных TLD остался бразильский домен, показатель которого, впрочем, остался неизменным (3 %).

Общее количество атакуемых брэндов за квартал уменьшилось с 557 до 531, при этом участники APWG отметили повышенный интерес фишеров к новым платежным веб-сервисам и службам, оперирующим криптовалютой.

«На сегодняшний день в 2014 г. обнаружен ряд новых мишеней, которые в 2013 г. не наблюдались, – заявил Г. Аарон, президент Illumintel и один из активных участников проводимых APWG исследований. – Фишеры атакуют новые сервисы онлайн-платежей, например, австрийский сайт безналичных платежей PayLife, базирующуюся в Гонконге альтернативную платежную систему Perfect Money, а также веб-сервис Payoneer, оказывающий разные виды финансовых услуг, в том числе по переводу денег и приему платежей с помощью предоплаченных пополняемых дебетовых карт MasterCard. Кроме того, наблюдается рост числа фишинговых атак на Bitcoin-сайты, в частности, на цифровые кошельки Blockchain и учетные записи обменника Coinbase».

Распределение мест во главе списка мишеней фишеров осталось прежним: на долю платежных сервисов во втором квартале пришлось 39,8 % атак, на финансы – 20,2 %, на розничную торговлю и сферу услуг 16,5 %.

Среди новых образцов вредоносных программ, обнаруженных участниками APWG из PandaLabs, по-прежнему преобладали троянцы, на долю которых в отчетный период пришлось 58,2 % опасных находок – заметно меньше, чем в первом квартале. Уменьшение «троянской» составляющей эксперты объясняют ростом экспансии PUP, потенциально

опасных программ, таких как шпионское ПО и программы показа рекламы (adware). PUP часто раздаются в связке с легальными программами, и невнимательный пользователь может загрузить их, вовсе того не желая. Одновременно APWG отметила заметный рост спроса на программы-упаковщики.

Экспансия PUP, по мнению APWG, послужила также одной из основных причин роста зараженности глобального компьютерного парка. В апреле-июне среднестатистический уровень составил 36,8 %, что значительно выше показателей за предыдущие кварталы. В разделении по странам чемпионом по степени заражения по итогам второго квартала оказался Китай (51,05 % местного парка), за ним следуют Перу и Турция (44,34 и 44,12 % соответственно). Россия в этом не почетном рейтинге заняла 6 место (42,89 %), пропустив вперед Боливию и Эквадор и обогнав Аргентину.

Основным хостером троянцев и даунлоадеров, используемых для фишинга, тоже являются США. В отчетный период на долю этой страны приходилось от 60 до 77 % ежемесячно фиксируемых вредоносных источников (IP-адресов) ***(APWG фиксирует рост числа фишинговых сайтов // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/09/29/more-phishing-registered.html). – 2014. – 29.09).***

***

В ходе трехмесячного наблюдения за специально разработанной приманкой исследователи обнаружили, что самое большое количество хакерских атак совершается из США, Китая и России.

Два эксперта по безопасности Д. Робертсон и Г. Мартин провели исследование, в ходе которого попытались выяснить, какое из государств совершает больше всего хакерских атак. Для этого исследователи разработали специальную online-приманку. К своему удивлению, специалисты обнаружили, что главным агрессором по проведению атак оказались США.

Приманкой, которую сконструировали исследователи, послужила поддельная промышленная компьютерная система, расположенная на территориях США, Великобритании, Амстердама, Бразилии, Токио и Сингапура. При этом система была уязвимой на всех этих локациях.

В течение трех месяцев исследователи наблюдали за ловушкой и выяснили, что самое большое количество хакерских атак было совершено из США (6000 тыс.), Китая (3500 тыс.) и России (более 2500 тыс.). Также значительное количество атак было нацелено из Франции и Нидерландов.

Как отмечают специалисты, в основном атаки были скорее разведывательными миссиями, в которых злоумышленники используют гораздо меньшее количество обфускации. Тем не менее, данный эксперимент опроверг представление о том, что Китай является лидером по проведению

хакерских атак и показал, что на самом деле, пальма первенства в этой сфере принадлежит США ***(США является лидером по проведению хакерских атак // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/09/29/a-decoy-computer-was-set-up-online-see-which-countries-attacked-it-the-most.html). – 2014. – 29.09).***

***

Редакція інформагентства «Центр журналістських розслідувань» у Сімферополі (Крим) повідомляє, що сайт втретє за вересень піддається потужним DDos-атакам. Наразі ресурс тимчасово недоступний, повідомляється на сторінці Центру в Facebook.

Нагадаємо, 2 вересня було зламано редакційну пошту «Центр журналістських розслідувань». 5 вересня на сайт інформагентства було здійснено потужні DDos-атаки. Тоді хостер був змушений тимчасово відключити сервер, розташований в Німеччині, і ресурс був недоступний декілька днів. 15 вересня DDos-атаки на «Центр журналістських розслідувань» повторилися.

Також співробітників інформагентства викликали для бесід в ФСБ і прокуратуру. «Кореспондент Є. Гаркуша був викликаний для "профілактичної бесіди" в Ялтинський відділ ФСБ, головний редактор видання В. Самар – в прокуратуру Сімферополя», – зазначали в Центрі ***(Сайт «Центр журналістських розслідувань» втретє за місяць зазнав потужних DDos-атак // «Телекритика» (http://www.telekritika.ua/kontekst/2014-09-30/98696). – 2014. – 30.09).***

***

«Доктор Веб» объявил об обнаружении сложного многофункционального бэкдора для Mac OS X. Вредоносное приложение было добавлено в вирусные базы под именем Mac.BackDoor.iWorm. Программа позволяет выполнять на инфицированном «маке» широкий набор различных команд, поступивших от злоумышленников. По данным компании, свыше 17 тыс. компьютеров Mac инфицированы данным троянцем.

В момент первого запуска Mac.BackDoor.iWorm сохраняет свои конфигурационные данные в отдельном файле и пытается прочитать содержимое папки /Library, чтобы получить список установленных в системе приложений, рассказали специалисты «Доктора Веб». Если «нежелательные» директории обнаружить не удается, бот получает с использованием нескольких системных функций наименование домашней папки пользователя OS X, от имени которого он был запущен, проверяет наличие в ней своего конфигурационного файла и записывает туда данные, необходимые ему для дальнейшей работы. Затем Mac.BackDoor.iWorm открывает на инфицированном компьютере один из портов и ожидает входящее

соединение, отправляет запрос на удаленный интернет-ресурс и ожидает поступления команд для последующего выполнения.

Троянец пытается установить соединение с командными серверами, перебирая в случайном порядке первые 29 адресов из полученного списка и отправляя запросы на каждый из них. Повторные запросы для получения нового перечня отправляются раз в 5 мин.

В процессе установки соединения с управляющим сервером, адрес которого выбирается из списка по специальному алгоритму, троянец пытается определить, не добавлен ли этот адрес в список исключений, и обменивается с ним специальным набором данных, по которым с использованием ряда сложных математических преобразований проверяется подлинность удаленного узла. Если проверка прошла успешно, бот отправляет на удаленный сервер номер открытого на инфицированном компьютере порта и свой уникальный идентификатор, ожидая в ответ поступления управляющих команд.

Mac.BackDoor.iWorm способен выполнять два типа команд: различные директивы в зависимости от поступивших бинарных данных или Lua-скрипты.

Собранная специалистами компании «Доктор Веб» статистика показывает, что в бот-сети, созданной злоумышленниками с использованием Mac.BackDoor.iWorm, на конец сентября насчитывалось 17 658 IP-адресов зараженных устройств. Наибольшее их количество – 4610 (что составляет 26,1 % от общего числа) приходится на долю США, на втором месте – Канада с показателем 1235 адресов (7 %), третье место занимает Великобритания: здесь выявлено 1227 IP-адресов инфицированных компьютеров (6,9 %) ***(«Доктор Веб» обнаружил ботнет из 17 000 компьютеров Mac // InternetUA (http://internetua.com/doktor-veb--obnarujil-botnet-iz-17-000-kompuaterov-Mac). – 2014. – 30.09).***

***

Учетные записи пользователей сервиса Snapchat были скомпрометированы неизвестными мошенниками в целях рассылки рекламных спам-сообщений. По данным администрации компании, несмотря на большое количество подверженных нападению пользователей, компьютерные сети службы не были скомпрометированы.

Напомним, что ранее, в январе этого года, Snapchat стал жертвой хакерской атаки, в результате которой произошла утечка учетных данных 4,6 млн человек. Кроме того, в руки злоумышленников попали телефонные номера пользователей.

В текущем заявлении представители социальной сети заявляют, что текущая атака стала возможной благодаря предыдущим инцидентам безопасности. Аферисты использовали в ходе нападения учетные данные пользователей сервиса, опубликованные на сторонних ресурсах.

«Для большинства пользователей уже налажена обратная связь, они получили уведомления о том, что их учетная запись была взломана», – следует из уведомления ***(Snapchat наводнили аферисты, рассылающие спам // InternetUA (http://internetua.com/Snapchat-navodnili-aferisti--rassilauasxie-spam). – 2014. – 1.10).***

***

Компания «Доктор Веб» обнаружила новую вредоносную программу, предназначенную для работы на смартфонах и планшетах под управлением ОС Android. Как сообщили CNews в «Доктор Веб», зловред представляет для пользователей весьма серьезную опасность, поскольку удаляет все имеющиеся на карте памяти данные, не позволяет прочитать входящие sms-сообщения, а также мешает нормальному общению в популярных программах-мессенджерах, блокируя их окна.

Новый Android-троян, внесенный в вирусную базу «Доктор Веб» под именем Android.Elite.1.origin, является представителем весьма редкого типа вредоносных программ, относящихся к классу программ-вандалов. Такие вредоносные приложения обычно создаются вирусописателями не для получения каких-либо материальных выгод, а для доказательства своих навыков программирования, выражения своей точки зрения на те или иные события, либо с целью развлечения или хулиганства. Часто подобные угрозы демонстрируют различные сообщения, портят пользовательские файлы и мешают нормальной работе зараженного оборудования. Именно так и действует новый Android-троян, который распространяется под видом популярных приложений, таких, например, как игры, рассказали в компании.

При запуске Android.Elite.1.origin обманным путем пытается получить доступ к функциям администратора мобильного устройства, которые якобы необходимы для завершения корректной установки приложения. В случае успеха троян приступает к немедленному форматированию подключенной SD-карты, удаляя все хранящиеся на ней данные. После этого вредоносная программа ожидает запуска ряда популярных приложений для общения.

Как только пользователь попытается запустить официальный клиент социальной сети Facebook, программу WhatsApp Messenger, Hangouts, либо стандартное системное приложение для работы с sms-сообщениями, Android.Elite.1.origin блокирует их активное окно, демонстрируя на экране изображение с текстом OBEY or Be HACKED. При этом данная блокировка сохраняется только для указанных программ и не распространяется на прочие приложения или операционную систему в целом, отметили в «Доктор Веб».

Чтобы еще больше ограничить доступ пользователя к инструментам «мобильного» общения, троян препятствует прочтению всех вновь поступающих sms-сообщений, для чего скрывает от своей жертвы все оповещения о новых sms. В то же время сами сообщения сохраняются и заботливо помещаются в раздел «Входящие», который, впрочем, остается недоступным из-за действующей блокировки.

При запуске Android.Elite.1.origin пытается получить доступ к функциям администратора мобильного устройства, которые якобы необходимы для завершения корректной установки приложения

Помимо форматирования SD-карты и частичной блокировки средств коммуникации, Android.Elite.1.origin с периодичностью в 5 с рассылает по всем найденным в телефонной книге контактам sms со следующим текстом: «HEY!!! [имя контакта] Elite has hacked you.Obey or be hacked». Кроме того, похожий текст отправляется в ответ на все входящие sms, поступившие с действующих мобильных номеров других пользователей: Elite has hacked you.Obey or be hacked.

Таким образом, счет мобильного телефона большинства пострадавших владельцев зараженных мобильных устройств может быть опустошен за считанные минуты и даже секунды.

Специалисты «Доктор Веб» не рекомендуют пользователям загружать приложения из сомнительных источников. Предоставлять доступ подобным приложениям к правам администратора мобильного устройства также не рекомендуется во избежание порчи файлов или иных негативных последствий ***(Троян-вандал для Android форматирует карту памяти и препятствует общению пользователей // InternetUA (http://internetua.com/troyan-vandal-dlya-Android-formatiruet-kartu-pamyati-i-prepyatstvuet-obsxeniua-polzovatelei). – 2014. – 1.10).***

***

Специалисты компании Barracuda Networks обнаружили новые образцы вредоносной программы-вымогателя CryptoWall, использующие цифровую подпись законного SSL-сертификата DigiCert. Образцы распространялись посредством атак по типу drive-by download. Суть атаки состоит в том, что вредоносное ПО рассылается через рекламные Flash-баннеры, с помощью которых веб-мастера хотят монетизировать свой сайт. При этом они сами могут не подозревать, что установленный на веб-странице баннер сделал их портал частью сети распространения вирусов.

По данным специалистов, злоумышленники атаковали порядка 15 тыс. ресурсов, в том числе сайт индийского издания Hindustan Times, а также порталы Israeli sports news и Web development community. В каждом из этих случаев вредоносная программа распространялась посредством рекламной сети Zedo.

Как поясняют эксперты Barracuda Networks, с помощью легитимной цифровой подписи злоумышленники пытались обойти средства защиты веб-сайтов. По сути своей, подход довольно сомнительный, поскольку такая практика широко распространена среди разработчиков вредоносного ПО, и многие антивирусные программы исключают возможность инфицирования подобным способом. Тем не менее, существует вероятность того, что с помощью цифровой подписи легитимного сертификата от надежного

разработчика, вредонос сможет обойти правила вайтлистинга некоторых приложений.

После успешного проникновения в систему CryptoWall посредством шифрования через алгоритм RSA 2048 зашифровывает все файлы и данные, а затем блокирует доступ пользователя к ним. Для получения доступа к зашифрованным файлам жертве предлагается уплатить выкуп, осуществляемый в Bitcoin через обеспечивающий анонимность браузер Tor.

На сегодняшний день нет абсолютно надежного способа восстановления зашифрованных CryptoWall файлов, кроме уплаты выкупа или использования не инфицированных резервных копий. Вместе с тем, эксперты не советуют идти на поводу у преступников, поскольку нет никаких гарантий, что пользователь получит ключ дешифрования, даже заплатив требуемую сумму ***(Обнаружены новые образцы программы-вымогателя CryptoWall // InternetUA (http://internetua.com/obnarujeni-novie-obrazci-programmi-vimogatelya-CryptoWall). – 2014. – 1.10).***

***

Исследовательская компания Lacoon Mobile Security выявила вредоносное приложение Xsser mRAT, нацеленное на пользователей iPhone и iPad. Троян передает sms-сообщения, контакты из адресной книги, географические координаты, учетные записи Apple ID, пароли и прочую информацию с мобильных устройств, подвергнутых процедуре джейлбрейка.

В настоящее время Xsser mRAT получил распространение в Китае. Эксперты отмечают, что таким образом китайское правительство осуществляет массивную кибератаку. В пользу предположения Lacoon свидетельствует тот факт, что атака совершается исключительно против гонконгских протестующих, а ее осуществляет крупная организация, понимающая китайский язык.

Xsser mRAT представляет собой значительную угрозу для джейлбрейкнутых устройств. Пользователи iPhone и iPad заражают свои устройства, перейдя по ссылкам, которые распространяют в социальных сетях. Троян запускает специальную службу launchd, которая обеспечивает возможность автоматической загрузки вредоноса.

По команде с управляющего сервера Xsser mRAT передает персональные данные владельца устройства. Создатели трояна могут получить широкий спектр информации, в том числе модель гаджета, версию операционной системы, MAC-адрес, номер телефона, IMSI и IMEI. В руки хакерам попадут также почтовые и короткие сообщения, фотографии, пароли из Связки ключей, логи звонков и т. д.

По словам экспертов, это наиболее совершенный iOS-троян среди тех, которые ранее были обнаружены. Хотя в настоящее время он используется лишь для осуществления атак против гонконгских протестующих, уже в ближайшее время могут найтись хакеры, которые будут применять вредонос в других, гораздо более опасных целях.

Как сообщается в блоге Lacoon, Xsser mRAT связан с аналогичным вредоносом для устройств под управлением Android. Для удаления трояна требуется переустановка операционной системы или полный сброс к заводским настройкам ***(Новый китайский троян крадет персональные данные пользователей iPhone и iPad // InternetUA (http://internetua.com/novii-kitaiskii-troyan-kradet-personalnie-dannie-polzovatelei-iPhone-i-iPad). – 2014. – 2.10).***

***

У четвер, 2 жовтня, сайт ТСН.ua піддався одній з найбільш потужних DDoS-атак за останні кілька місяців. Про це повідомляє прес-служба ТСН.

ТСН.ua з моменту початку Євромайдану восени 2013 р. практично щодня піддавався DDoS-атакам. Однак нинішня – одна з найбільших за останні кілька місяців.

Зловмисники при цьому активно поширюють в антиукраїнських групах у соціальних мережах Twitter і «ВКонтакте» заклики допомогти в організації ще більш масованої DDoS-атаки на ТСН.ua.

За інформацією ТСН, нині хакери атакують ще кілька великих українських новинних сайтів ***(ТСН.ua зазнав потужної DDoS-атаки // Телекритика (http://www.telekritika.ua/rinok/2014-10-03/98796). – 2014. – 3.10).***

***

Команда реагирования на компьютерные чрезвычайные происшествия Украины CERT-UA, которая входит в структуру Государственной службы специальной связи и защиты информации Украины, зафиксировала атаки на сайты Госспецсвязи и Службы безопасности Украины.

Как сообщает Цензор.НЕТ, об этом говорится в сообщении CERT-UA.

«CERT-UA получена информация относительно фиксации, начиная с 20:50, 2 октября, аномальной сетевой активности в сторону веб-сайтов Госспецсвязи и СБ Украины, в результате чего наблюдались временные перебои в их функционировании. Детали выясняются», – отмечается в сообщении ***(Хакеры атакуют сайты Госспецсвязи и СБУ // Цензор.НЕТ (http://censor.net.ua/news/305392/hakery_atakuyut_sayity_gosspetssvyazi_i_sbu). – 2014. – 3.10).***

***

Украинские хакеры взломали сайт русских националистов

При заходе на сайт русских националистов Спутник и Погром открывается зеркало ресурса Информационного сопротивления, который курирует руководитель общественной организации Центр военно-политических исследований Д. Тымчук, пишет korrespondent.net.

Отметим, что Спутник и Погром (он же СиП) – сайт Е. Просвирнина, позиционируется как информационный ресурс русских националистов. На сегодняшний день ресурс активно поддерживает сепаратистов на Донбассе.

Сайт Информационное Сопротивление – неправительственный проект, главной задачей которого является противодействие в информационном поле внешним угрозам, возникающим для Украины в основных сферах: военной, экономической и энергетической, а также в сфере информационной безопасности.

Главным координатором Информационного Сопротивления является Д. Тымчук – офицер запаса, руководитель общественной организации Центр военно-политических исследований.

Кто именно взломал Спутник и Погром – пока неизвестно.

Пока на информационных ресурсах СиП в социальных сетях создатели сайта никак не прокомментировали взлом ***(Украинские хакеры взломали сайт русских националистов // InternetUA (http://internetua.com/ukrainskie-hakeri-vzlomali-sait-russkih-nacionalistov). – 2014. – 3.10).***

***

Хакеры похитили данные о 83 млн счетов, принадлежащих клиентам одного из крупнейших американских банков JPMorgan Chase, а не об 1 млн, как считалось ранее. Об этом пишет The New York Times со ссылкой на сообщение, направленное банком финансовому регулятору.

В результате взлома была похищена информация о 76 млн счетов частных клиентов и 7 млн счетов, принадлежащих малым фирмам. Таким образом, этот взлом стал крупнейшим за всю историю кибератак на банки.

Хакеры, по данным издания, смогли получить доступ к 90 серверам JPMorgan Chase и всем программам, которые работали на компьютерах банка. Из-за этого на ликвидацию последствий взлома уйдет как минимум несколько месяцев.

Как киберпреступникам удалось получить доступ к компьютерной сети банка, до сих пор неясно. При этом следствие оказалось в тупике, так как хакеры не оставили никаких улик, указывающих на то, что со взломанных счетов были похищены деньги. В связи с этим следствие не исключает, что целью взлома был шпионаж, организованный одной из стран Южной Европы или Россией.

О том, что хакеры атаковали американскую финансовую систему, похитив данные из JPMorgan Chase & Co и, по меньшей мере, еще одного банка, стало известно в конце августа. В руках у хакеров оказалась информация не только о клиентах, но и о работниках банка, включая руководителей JPMorgan ***(Хакеры украли информацию о 83 миллионах счетов JPMorgan // InternetUA (http://internetua.com/hakeri-ukrali-informaciua-o-83-millionah-scsetov-JPMorgan). – 2014. – 3.10).***

***

Удобная функция «История файлов» в Windows 8 и 8.1 позволяет существенно сэкономить время, однако если настроить ее без надлежащих мер безопасности, можно подвергнуть угрозе конфиденциальность файлов. Об этом сообщил старший научный сотрудник компании KPMG К. Джонсон на мероприятии (ISC) Security Congress.

Эксперт отметил, что это не уязвимость в самой функции, а ошибка компании Microsoft, которая в своих инструкциях описывает, как обойти эту проблему. Несмотря на предостережения, найти файлы, подобным образом хранящиеся в Интернете, очень легко.

К. Джонсон привел в пример случай, когда он обнаружил в сети резервные копии корпоративных документов, хранившихся на компьютере бывшего главы некой компании, а также записки врача об одном из пациентов.

Функция «История файлов» обычно сохраняет резервные копии документов, папок, файлов и фотографий, поэтому в случае потери, удаления или повреждения оригинала его можно с легкостью восстановить. При настройке функции необходимо указать локацию, куда будут сохраняться резервные копии (например, съемные жесткие диски или сетевые хранилища). Если пользователь указывает подключенные к Интернету сетевые хранилища, позволяющие анонимно использовать FTP-протокол, сохраненные резервные копии можно найти в интернете с помощью поисковых систем.

По словам К. Джонсона, даже если компания, пользующаяся «Историей файлов», будет уверена в безопасности выбранного ею хранилища для резервных копий, они все равно находятся под угрозой. К примеру, если работник копирует файлы на флэш-накопитель и загружает их на некорпоративный компьютер, использующий неверный тип сетевого хранилища, информация будет видна в Интернете ***(Функция «История файлов» в Windows 8 ставит под угрозу конфиденциальность даннях // InternetUA (http://internetua.com/funkciya--istoriya-failov--v-Windows-8-stavit-pod-ugrozu-konfidencialnost-dannih). – 2014. – 4.10).***

***

По результатам исследования, проведенного экспертами из IDG по заказу компании Veracode, предприятия в США и Великобритании используют порядка 4,5 млн приложений, предоставляющих угрозу безопасности.

Эксперты сообщили, что в 2015 г. 70 % разработанных для использования внутри компаний приложений будут уязвимы к таким распространенным видам атак, как SQL-инъекции. Это означает рост числа атак на предприятия, входящие в список Forbes Global 2000.

Недавние масштабные утечки данных клиентов крупных торговых сетей, таких как Home Depot, свидетельствуют о том, что для проникновения

в корпоративные сети киберпреступники используют множество разнообразных техник. Поскольку компании эффективно закрывают свои внутренние сети, для атак хакеры используют уязвимые приложения.

В Veracode считают, что предприятиям необходимо найти новый, более масштабируемый подход к безопасности приложений, позволяющий совершенствовать программы. «Использование автоматизированного облачного сервиса позволит предприятиям идти в ногу с инновационными технологиями без ущерба безопасности», – говорится в уведомлении Veracode.

Поскольку для продвижения своего бизнеса компании продолжают создавать все больше приложений, из-за невозможности масштабирования существующих программ безопасности проверяются только критически важные бизнес-приложения. Из этого следует, что огромное количество используемых предприятиями программ остаются уязвимыми и представляют угрозу безопасности ***(4,5 млн корпоративных приложений представляют угрозу безопасности // InternetUA (http://internetua.com/4-5-mln-korporativnih-prilojenii-predstavlyauat-ugrozu-bezopasnosti). – 2014. – 4.10).***

***

Исследователи компании F-Secure, совместно с аналитиками Британского института и специалистами немецкой компании SySS установили, что рядовые пользователи готовы подключаться к бесплатному Wi-Fi даже если подключение представляет потенциальную опасность.

В ходе эксперимента инженеры SySS установили точку доступа Wi-Fi в деловом центре Лондона. За полчаса к ней подключились 250 устройств. При этом, большинство подключений происходили автоматически, даже без ведома владельцев устройств. В общей сложности, за 30 минут исследователи собрали 32 мегабайта данных о пользователях. При этом, ни один человек даже не озаботился шифровкой своих данных, так что исследователи смогли получить содержимое отправлений, адреса отправителя и получателя, и даже пароли.

Резюмируя исследование, специалисты по безопасности отметили, что пользователи сегодня настолько любят бесплатный Wi-Fi, что стоит любому желающему установить бесплатную точку доступа, и он сможет собирать данные о пользователях в неограниченных количествах. Безусловно, этим могут воспользоваться злоумышленники для копирования чужих паролей и прочих конфиденциальных даннях ***(Пользователи пренебрегают безопасностью ради бесплатного Wi-Fi // InternetUA (http://internetua.com/polzovateli-prenebregauat-bezopasnostua-radi-besplatnogo-Wi-Fi). – 2014. – 5.10).***

***

ИБ-эксперт Л. Пеше создал устройство размером с кухонную доску, которое можно использовать в качестве дешевого инструмента для осуществления атак на беспроводные сети. Предназначением разработки являются атаки, получившие название «военные поставки» (war shipping), в ходе которых вредоносное аппаратное обеспечение доставляется жертве по обычной почте.

Созданное на базе Raspberry Pi устройство, которое отлично помещается в стандартную почтовую коробку, способно проникать в беспроводные сети и сообщать злоумышленникам о своем местонахождении.

«Мы хотели знать, когда устройство прибудет в нужное или близкое к нему место, где есть доступ к определенной сети для того, чтобы убедиться, что мы атакуем нужных людей», – сообщил Л. Пеше на конференции по безопасности Derbycon, состоявшейся в конце прошлого месяца.

Устройство может использоваться для атак на определенные организации, транспортные компании и любые другие жертвы, встречающиеся на протяжении всего пути во время его доставки. Правда, для этого почтовый грузовик должен ехать достаточно медленно и останавливаться.

Для пользователей, желающих создать собственное устройство, Л. Пеше опубликовал на GitHub соответствующее программное обеспечение, которое постоянно совершенствуется и обновляется ***(Эксперт представил небольшое устройство для хакерских атак по обычной почте // InternetUA (http://internetua.com/ekspert-predstavil-nebolshoe-ustroistvo-dlya-hakerskih-atak-po-obicsnoi-pocste). – 2014. – 5.10).***

***

Лаборатория по кибербезопасности компании High-Tech Bridge обнаружила отраженную XSS-уязвимость в CMS TextPattern, позволяющая злоумышленнику выполнить произвольный HTML-код или скрипт в браузере пользователя. Проблема связана с недостаточной санитизацией входящих данных через URI.

Эксперты обнаружили брешь еще в июле 2014 г., но в целях обеспечения безопасности не публиковали детали уязвимости публично. После того, как 20 сентября этого года разработчик TextPattern исправил брешь, детали об уязвимости были разглашены.

Злоумышленники могут заставить пользователя открыть специально сгенерированную ссылку и выполнить произвольный код в браузере в контексте уязвимого веб-сайта. Дальнейшая эксплуатация данной бреши позволит провести фишинговые атаки и, вероятно, получить неавторизованный доступ к ресурсу.

Эксперты опубликовали PoC-код уязвимости. В нем используется функция JavaScript “alert()”, которая отобразит на уязвимом сайте слово Immuniweb:

http://[host]/textpattern/setup/index.php/%22%3E%3Cscript%3Ealert%28immuniweb%29;%3C/script%3E/index.php

Владельцам сайтов на базе TextPattern следует установить обновление 4.5.7, которое исправляет данную уязвимость. На официальном блоге TextPattern опубликованы все исправления ***(В CMS TextPattern обнаружена XSS-уязвимость // InternetUA (http://internetua.com/v-CMS-TextPattern-obnarujena-XSS-uyazvimost). – 2014. – 5.10).***