СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(21.09–4.10)

2015 № 17

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(21.09–4.10)
№ 17

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

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

Упорядник
Т. Касаткіна

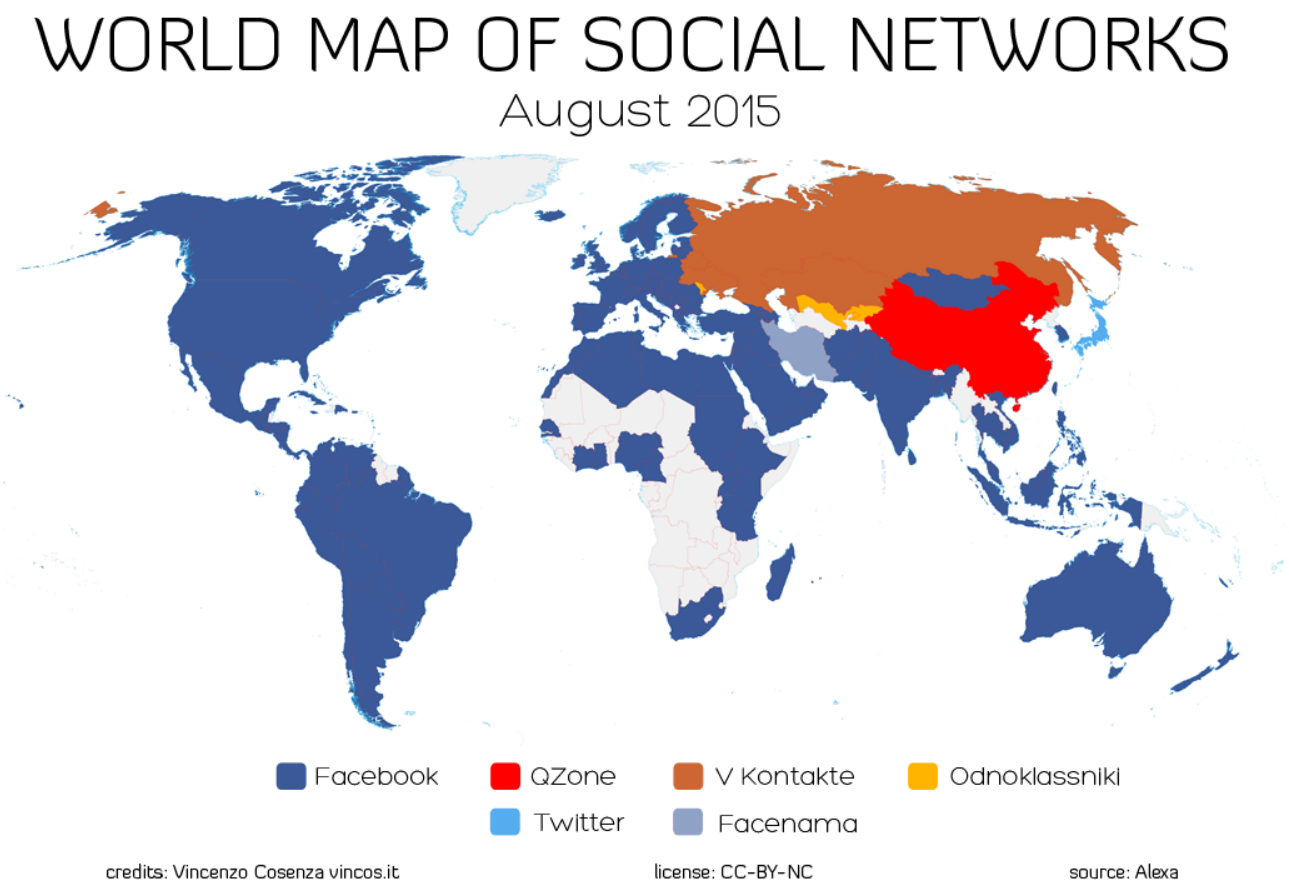
Заснований у 2011 році
Виходить двічі на місяць

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

У 129 зі 137 країн, які двічі на рік потрапляють до так званої «Карти світу соціальних мереж», домінує Facebook. Країни на карті розфарбовано залежно від того, яка соцмережа домінує в них.



З кожним роком кількість країн, де Facebook не є соцмережею № 1, стає дедалі меншою. Як і самих соціальних мереж. Ще два роки тому Україна була серед 10 країн, де Facebook не є соцмережею № 1. На сьогодні таких країн залишилося лише вісім.

Мова йде не про всі країни світу, а лише про ті, статистика щодо яких є достатньою (тобто кількість користувачів достатньо велика), щоб дані можна було зібрати.

«ВКонтакте» та «Одноклассники» продовжують домінувати в багатьох країнах пострадянського простору, QZone – у Китаї.

В Україні найпопулярнішою соцмережею залишається «ВКонтакте».

Чи є шанс у Facebook обійти «ВКонтакте» в Україні? ***(Україна залишилась серед 8 країн, де Facebook досі не став соцмережею №1 // UkrainianWatcher (http://watcher.com.ua/2015/09/21/ukrayina-zalyshylas-sered-8-krayin-de-facebook-dosi-ne-stav-sotsmerezheyu-1/). – 2015. – 21.09).***

***

По данным исследования CMeter компании TNS, список самых популярных сайтов среди украинских интернет-пользователей в августе возглавляют Google.com.ua, Vk.com, Youtube.com. Особого разделения аудитории первой двадцатки сайтов рейтинга по полу нет, большинство ресурсов в равной степени посещают как мужчины, так женщины. Впрочем, по возрасту распределение аудитории тоже относительно равномерное. У Ex.ua и Kinogo.net более молодая аудитория – значимо выше доля аудитории 16–25, чем у остальных сайтов, и в то же время ниже доля аудитории в возрасте 36–45 и 46–55 ***(В августе украинцы предпочли Google, ВКонтакте и YouTube // Marketing Media Review (http://mmr.ua/show/v_avguste_ukraintsy_predpochli_google__vkontakte_i_youtube). – 2015. – 21.09).***

***

Фотосервис Instagram и социальная сеть Facebook блокируют ссылки на «ВКонтакте», передает корреспондент «Газеты.Ru».

При попытке разместить ссылку https://vk.com в личном сообщении или новой записи в Facebook, а также в комментариях под фото в Instagram, сервисы выдают предупреждение об «использовании запрещенной ссылки». Более того, после попытки опубликования ссылки на «ВКонтакте», десктопная версия Facebook предлагает провести онлайн-сканирование компьютера на наличие вредоносного ПО, для чего необходимо скачать программу F-Secure Online Scanner.

При этом ссылки «ВКонтакте» на страницы пользователей, фото и видеоматериалы отправляются без каких-либо проблем.

Ранее «ВКонтакте» перестала поддерживать активные гиперссылки на Instagram. Многие связали это с выходом собственного фотоприложения российской соцсети под названием Snapster ***(Instagram и Facebook блокируют ссылки на «ВКонтакте» // InternetUA (http://internetua.com/Instagram-i-Facebook-blokiruuat-ssilki-na--vkontakte). – 2015. – 21.09).***

***

На прошлой неделе М. Цукерберг пообещал в ближайшее время дать аудитории инструмент «проявления отрицательных эмоций», несмотря на то что в 2014 г. глава Facebook утверждал, что «дизлайков» в соцсети не будет. Невзирая на то, что лента Facebook и так более чем наполовину состоит из негатива, скепсиса и критики – и трудно представить, что случится, дай пользователям возможность жать на кнопку «Мне не нравится».

«Мне не нравится»

Анонс «дизлайков» – обратная сторона проблемы, о которой в своё время шла речь в колонке Д. Уортэм в коллективном блоге Bits от NYT. По её словам, популярные соцсети стали превращаться в этакий цифровой аналог «желтых страниц». Раньше люди пользовались телефонными справочниками; теперь они

пользуются Facebook. Здесь ведут хронику всей жизни – но мало времени беседуют (ну за исключением Facebook Messenger, который недаром превратили в отдельное приложение):

«Став универсальным инструментом, где “все сидят”, где есть большая тусовка и где френдов больше, чем в реальном мире, Facebook потерял былое очарование и новизну для молодежи. А за юными тянутся и те, кто чуть постарше, а там – и вовсе взрослые».

Команда Цукерберга вводит изменения, чтобы вернуть интерес пользователей. Но как в таком случае будет работать маркетинговая составляющая?

Изначально данные об активности всех пользователей соцсети собирались при помощи кнопки Like. Причём – как только стало известно, как применяются «лайки», – почти сразу развернулась дискуссия: а не используется вся эта информация как-то неправильно?

До появления Dislike

21 апреля 2010 г. в ходе своей конференции для разработчиков соцсеть Facebook представляет новую кнопу; при этом М. Цукерберг заявляет, что эта кнопка всё изменит, персонализировав весь опыт потребления контента, товаров и услуг в пределах Интернета.

30 ноября 2010 г. аналитик А. Роозендааль публикует информацию о том, что передача данных после «лайков» происходит даже без нажатия на кнопку. В соцсети эту информацию долгое время не комментируют, а затем говорят о сбое в работе Facebook.

18 мая 2011 г. скандал разгорается с новой силой. The Wall Street Journal сообщает о том, что собирают данные не только кнопки, но и виджеты. Компания снова всё опровергает, но доказательств обратного не приводит.

25 сентября 2011 г. австралиец Н. Кубрилович заявляет, что даже после выхода из социальной сети Facebook продолжает собирать данные и отслеживать действия пользователей. Администрация соцсети признаёт проблему и обещает её устранить.

1 октября 2011 г. IT-журналист и техноблогер М. Аррингтон публикует попавшие к нему сведения о патентованном приложении Facebook, способном отслеживать и мониторить все данные об авторизованном пользователей за пределами Facebook. И лишь 12 июня 2014 г. в Facebook подтверждают, что соцсеть начнет отслеживать действия и предпочтение пользователей в Интернете при помощи кнопок и виджетов Like.

Как теперь поступят в команде Цукерберга из-за идеи ввести «дизлайки»? Привяжут их тоже к маркетинговому инструментарию соцсети? Начнут продавать рекламодателям негативные настроения пользователей? Будут «продавать» ненависть, страх, негатив и апатию психотерапевтам, клиникам, политическим партиям и пиар-технологам? Ответа пока нет.

«Не нравится» как способ вернуть аудиторию

Не первый год подростковая аудитория покидает соцсеть М. Цукерберга. Причинами стала растущая популярность Snapchat, Tumblr, нелюбовь к тому,

что взрослые «суют нос» в дела молодёжи с помощью Facebook; но и растущая травля и негатив в соцсетях:

«Как только соцмедиа перестают быть местом для развлечения и становятся площадкой для агрессии и унижений, подростки из уязвимых подгрупп (девочки, “заучки”, ЛГБТ-подростки, просто молодежь, которая не ладит со сверстниками в школах и колледжах) покидают социальную сеть».

Отказаться от травли можно, лишь дав пользователям возможность выражать негативные эмоции лаконично и быстро. М. Цукерберг (или его аналитический отдел в компании) прекрасно видят, что большую часть материалов люди «лайкают», не дочитывая до конца или вообще не читая. Достаточно прочесть результаты исследования компании Upworthy в области использования Like и Retweet:

«Исследователь из Chartbeat Д. Шварц уточнил, что рост трафика в результате таких публикаций не означает, что люди на самом деле прочли пост или статью, которую сами же опубликовали в социальных сетях… Даже логические обоснования не отменяют один простой, хоть и неприятный для многих редакторов и блогеров факт: люди массово твитят и публикуют в Facebook ссылки на статьи и посты, не читая сами материалы. Любой, кто говорит, что прочел каждую заретвиченную статью от начала до конца, – мягко говоря, врун.

Проект Upworthy измерил взаимосвязь между глубиной просмотров, кликов, отображения и длиной просмотра видео, а также частотой публикаций всех материалов в социальных сетях. Проведенный анализ показывает, что число людей, которые твитят, не читая, достаточно велико, и обычно такие люди читают всего 25 % оригинального материала.

Аналогичные данные выяснили и в команде BuzzFeed: основная масса публикаций в Twitter и Facebook происходит после того, как пользователь провел на странице около трех с половиной минут для настольного устройства или чуть более двух минут – для мобильного».

Если они «лайкают» не читая, то почему бы им не выражать отрицательные эмоции, тоже не вдаваясь в суть? С одной стороны – малое зло: так соцсеть поощряет людей не вникать в суть того, на что они среагировали спонтанно. С другой стороны – предотвращение «войны комментариев».

Со времён Древнего Рима мало что изменилось. Всем нам хотелось бы почувствовать себя «повелителем судеб», только вместо гладиаторов у нас – контент и аватарки. С 2007 г. у нас была возможность жать на «палец вверх» подо всем подряд, не особо заботясь о том, какой будет дальнейшая «судьба» прочитанного нами. Почему теперь не попробовать «палец вниз»? ***(Марк Цукерберг и «палец вниз» // InternetUA (http://internetua.com/mark-cukerberg-i--palec-vniz). – 2015. – 22.09).***

***

В социальной сети Facebook появился новый инструментарий Signal, предназначенный, в частности, для журналистов.

С его помощью пользователь может следить за основными событиями в сфере культуры, спорта, читать самые свежие новости и многое другое, пишет «Зеркало недели».

Signal генерирует контент из Facebook и Instagram, который пользователь затем может использовать для своих статей. Приложение позволяет следить за основными трендами в Facebook и находить связанный с ними внешний контент. Кроме того, с помощью приложения пользователь может проследить и за тем, какие политики, музыканты, спортсмены, актеры и писатели упоминались на Facebook чаще всего.

Сообщение о запуске приложения появилось в официальном блоге Facebook ***(В Facebook появился инструментарий, облегчающий поиск информации // Вечерние Вести (http://www.gazetavv.com/news/ukraine/1442826433-v-facebook-poyavilsya-instrumentariy-oblegchayushchiy-poisk-informatsii.html). – 2015. – 21.09).***

***

Команда Telegram сообщила об очередной новинке, появившейся в мессенджере. На этот раз «создание» П. Дурова научилось отправлять публичные сообщения. Инструмент, с помощью которого это возможно сделать, назвали Channels, пишет therunet.com

С помощью Channels пользователь может создавать на просторах Telegram своеобразные «социальные сети» в миниатюре, поскольку публичные сообщения снабжаются собственными URL и имеют отдельные счётчики просмотров. Почти стена в социальной сети.

Кроме того, команда П. Дурова отмечает: в публичный чат можно добавлять неограниченное количество пользователей. Как только новые участники примкнут к переписке, им станет доступна вся история сообщений в данном «канале».

Сочетая в себе функции социальной «стены», публичного чата и обычного мессенджера, Telegram дал возможность создать даже не социальную сеть, а множество локальных социальных «сеточек», аудиторию которых можно регулировать по желанию пользователя.

Channels уже включены в обновления Telegram и доступны на iOS и Android ***(Павел Дуров превращает мессенджер в «социальную сеть» // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44752/118/lang,ru/). – 2015. – 23.09).***

***

Программист из Киева М. Фрай разработал сервис Zmiya.com.ua, который агрегирует, систематизирует, анализирует и визуализирует все, что происходит в украинских социальных сетях и блогах. Проект призван помочь журналистам и тем, кто стремится следить за повесткой дня в украинском Интернете.

Помимо этого, Zmiya задумывается как блог-платформа, пишет AIN.UA (http://ain.ua/2015/09/22/605069).

Изначально проект создавался совместно с пабликом «Типичный Киев» как плагин для анализа и поиска информации по соцсетям. Когда значительная часть была сделана, появилась идея расширить функциональность и возможности.

«Все делалось для максимально удобного просмотра повестки дня в одном месте. Иногда выходишь на несколько часов с Интернета и не понимаешь, о чем все говорят», – поясняет М. Фрай, создатель проекта, на счету которого уже как минимум два социальных приложения.

Главная страница проекта представляет собой несколько блоков, в которых визуализирована аналитика по тем или иным областям: облако тегов, рейтинги пользователей в соцсетях, рейтинг самых популярных статей в блогах, СМИ, рейтинг твитов. Справа – список самых популярных новостей. Период отображения варьируется. Ранжирование происходит не только по просмотрам, но по отклику на новость в соцсетях.

Главным преимуществом проекта является то, что информация обновляется без задержек: «Сейчас нет систем мониторинга украинского Facebook. Да и в России такого нет. Аналитические компании выпускают рейтинги раз в месяц, и создают их руками, а у нас все онлайн, в режиме реального времени», – рассказывает разработчик. Каким образом программисту удалось изымать информацию из закрытой API Facebook – не признается. Говорит, что нашел возможность обходить постоянно меняющиеся алгоритмы, и именно над этой частью работали дольше всего.

Инвестора в проекте нет. М. Фрай (это псевдоним разработчика, настоящее имя он не раскрывает) ранее работал на позиции senior C++ developer в компании Serena Software и утверждает, что профинансировать такой проект человеку, который работал на подобной позиции, не составляет труда.

Основатель проекта убежден, что лучший способ получать актуальную и объективную информацию в Украине – это агрегировать ее из нескольких источников. Причем не только СМИ, но и личных страниц пользователей Facebook и Twitter. Поэтому в основном сайт собирает user-generated content. Отсюда и название – ЗМІя (ЗМІ – засоби масової інформації).

Рейтинги СМИ, пользователей Facebook и Twitter ранжируются не только по количеству просмотров/подписчиков, но по внутренним алгоритмам сайта, которые учитывают живую активность, комментарии, лайки и шейры в соцсетях.

При переходе на линки можно заметить, что в URL остается домен zmiya.com.ua, а сайт отображается под плашкой ресурса. Основатель уверяет, что это никак не влияет на просмотры или отображение рекламы. Необходимость этой плашки обуславливается лишь возможностью быстро вернуться на главную Zmiya.

Еще одна функция, доступная на сайте, – написание и размещение блогов. Функциональность этого режима отдаленно напоминает Medium. «Мы решили сделать максимально удобный редактор текстов с возможностью вставки любого медийного контента», – говорит М. Фрай. Уже сейчас туда можно вставить персональный Google Analytics, а в ближайшее время также планируется предоставить возможность интеграции своей рекламы.

М. Фрай, создатель сервиса:

«База СМИ в Zmiya отобрана вручную. Принцип отбора: все, что так или иначе касается Украины. Поэтому там часто попадаются те или иные российские медиа. Если пользователь посчитает, что не хватает какого-то источника, на сайте есть контакты разработчиков, которые смогут его добавить».

В настоящее время на проекте М. Фрай не планирует зарабатывать и видит его скорее как социальный. «Ресурс делали как для себя. Есть ряд рекламных моделей, над которыми мы думаем, но к какой именно придем, посмотрим уже после запуска», – признается разработчик ***(Киевский разработчик создал агрегатор и анализатор украинских социальных сетей в реальном времени // AIN.UA (http://ain.ua/2015/09/22/605069). – 2015. – 22.09).***

***

Аудиторія Instagram зросла до 400 млн користувачів, хоча ще в грудні 2014 р. місячна аудиторія сервісу становила 300 млн.

Про це повідомляється на сайті компанії, передає Еспресо.TV.

Як наголошується, співтовариство Instagram стало «ще більш глобальним»: 75 % користувачів сервісу живуть за межами США.

Серед 100 млн користувачів, які приєдналися за останні дев'ять місяців, більш ніж половина – з Європи та Азії, а найбільший приріст становили користувачі з Бразилії, Японії та Індонезії.

У повідомленні фотосервісу наголошується, що за чисельністю аудиторії Instagram продовжує випереджати сервіс мікроблогів Twitter, у якого налічується 316 млн користувачів.

За чотири роки існування Instagram загальна кількість фотографій, розміщених на сервісі, перевищила 30 млрд. Щодня користувачі Instagram обмінюються понад 80 млн фотографій і відеороликів, які залучають по 2,5 млрд лайків на день ***(Instagram випередив Twitter за кількістю користувачів // Espreso.tv (http://espreso.tv/news/2015/09/23/instagram_vyperedyv_twitter_za_kilkistyu_korystuvachiv). – 2015. – 23.09).***

***

Экс-глава «ВКонтакте» П. Дуров на конференции TechCrunch Disrupt 2015 в Сан-Франциско раскритиковал социальную сеть Facebook и чат WhatsApp, сообщает Rbc. Он также заявил, что в его мессенджере Telegram появятся платные сервисы от сторонних разработчиков.

П. Дуров не верит в то, что в России Facebook когда-нибудь обгонит по популярности созданную им социальную сеть «ВКонтакте». По его словам, угроза позициям «ВКонтакте» исходит с другой стороны. Социальная сеть все еще остается лидером с огромным отрывом, но, тем не менее, испытывает трудности с тем, чтобы оставаться постоянно нужным и полезным для пользователей. «Небольшие приложения вроде Instagram, WhatsApp, Viber, Snapchat привлекают все больше и больше людей», – отметил П. Дуров.

При этом он резко раскритиковал некоторые из этих приложений. Так, мессенджер WhatsApp Дуров назвал «отстоем». Он метафорически сравнил его с «садом из стен», имея в виду, что мессенджер не позволяет пользователям хранить свои сообщения на всех устройствах. «Если у вас есть WhatsApp и телефон выходит из строя, у вас нет доступа к вашим сообщениям, вы не можете отправить документы, это плохо с точки зрения приватности. Я не был большим поклонником WhatsApp, не являюсь им и сейчас», – заявил бизнесмен.

П. Дуров рассказал, что в его мессенджере Telegram появится специальное API, которое позволит разработчикам ботов взимать плату с пользователей. В беседе с редактором Techcrunch он рассказал о запущенной летом этого года платформе для разработчиков ботов. Решением, по словам П. Дурова, заинтересовались многие бренды, которые продвигают свои услуги через Telegram.

Кроме того, П. Дуров прокомментировал претензии относительно того, что использование в Telegram сразу нескольких протоколов шифрования привлекает террористов из ИГИЛ, которые пользуются мессенджером для общения между собой. «Наше право на приватность важнее, чем страх перед терроризмом, – заявил П. Дуров. – ИГИЛ всегда найдет другой способ коммуникаций. Я не думаю, что мы принимаем участие в их деятельности, и мы не должны чувствовать за это вину. Если бы они не использовали Telegram, то они бы использовали что-то еще».

В ходе выступления на TechCrunch Disrupt П. Дуров не анонсировал, как ожидали многие пользователи, появление в Telegram голосовых звонков. В WhatsApp и Viber такая функция есть ***(Павел Дуров назвал WhatsApp «отстоем» // InternetUA (http://internetua.com/pavel-durov-nazval-WhatsApp--otstoem). – 2015. – 23.09).***

***

Социальная сеть Facebook начала показывать «сферические» видео с рядом медиа партнеров, включая Star Wars, Discovery, GoPro, LeBron James, NBC’s Saturday Night Live и VICE. Любой, снимающий видео в режиме 360 градусов, сможет загрузить формат, но вначале видео можно будет просмотреть только на ПК или с помощью Android приложения Facebook. Пользователям IOS придется немного подождать, поддержка нового формата появится в последующие месяцы. Как отметил директор по разработке продукта К. Кокс, это уникальный способ взаимодействия с контентом. Над созданием нового

формата компания трудилась с инженерами подразделения Oculus. ***(Facebook запустил 360-градусные видео в ленте // Marketing Media Review (http://mmr.ua/show/facebook_zapustil_360-gradusnye_video_v_lente). – 2015. – 24.09).***

***

Сеть микроблогов Twitter обновила дизайн социальных кнопок Tweet и Follow, который оставался неизменным с 2011 г. Компания сделала новые иконки более «плоскими», лишила их серого ободка и перекрасила в синий цвет.

В рамках обновления Twitter также закроет разработчикам доступ к API, который позволял им создавать собственные кнопки Tweet и Follow со счетчиком твитов. Ширина новых кнопок в пикселях соответствует старым, поэтому веб-дизайнерам не потребуется вносить изменения в дизайн сайтов.

Обновленные кнопки Twitter начнут появляться на месте старых в следующем месяце.

Ранее в сентябре дизайн кнопки Google+ – G+1 – сменила компания Google. Также интернет-поисковик провел самый масштабный за последние 17 лет редизайн своего логотипа. В обновленном фирменном знаке используется шрифт без засечек, что делает его более современным, а цвета стали немного мягче ***(Twitter поменяла дизайн социальных кнопок // InternetUA (http://internetua.com/Twitter-pomenyala-dizain-socialnih-knopok). – 2015. – 24.09).***

***

Крупнейшая в России социальная сеть «ВКонтакте» работает над новым протоколом шифрования данных.

Об этом сообщает «Корреспондент» со ссылкой на газету «Известия».

Операционный директор соцсети А. Рогозов подтвердил информацию: «Мы действительно занимаемся разработкой нового мобильного протокола для ускорения наших приложений и обеспечения высокого уровня безопасности передачи пользовательских данных».

По словам газеты, новый протокол должен увеличить скорость обмена данными между пользователями соцсети. После того как работа завершится, «ВКонтакте» выпустит собственный мессенджер. Будут созданы приложения для iOS и Android, а также версии для установки на компьютеры, работающие на Windows и MacOS.

В настоящее время «ВКонтакте» работает по шифрованному протоколу https, при этом пользователи могут обмениваться информацией через нешифрованный протокол http.

После того как в апреле 2014 г. П. Дурова уволили с поста гендиректора «ВКонтакте», он занялся развитием своего собственного сервиса обмена сообщениями – мессенджера Telegram. Разработчики охарактеризовали новый сервис так: «сверхбыстрый, простой, безопасный и абсолютно бесплатный». В

этом продукте используется протокол передачи данных Mobile Telecommunication Protocol (MTProto), разработанный братом П. Дурова Н. Дуровым, бывшим техническим директором «ВКонтакте».

По словам источника «Известий», «ВКонтакте» работает над урезанной версией протокола MTProto, которая позволит ускорить отправку и прием сообщений ***(«ВКонтакте» зашифрует переписку пользователей // Podrobnosti.mk.ua (http://podrobnosti.mk.ua/2015/09/25/vkontakte-zashifruet-perepisku-pol-zovateley.html). – 2015. – 25.09).***

***

2,7 млн українців користуються Facebook за допомогою смартфона або планшета. Це становить 60 % від загальної кількості українських користувачів соціальної мережі. Їх на сьогодні 4,5 млн. Про це свідчать дані внутрішньої статистики Facebook.

Розподіл всередині мобільної аудиторії такий: 2,2 млн – це користувачі смартфонів і 580 тис. – користувачі планшетів (деякі користувачі мають обидва пристрої). 820 тис. українців заходять у Facebook через пристрої компанії Apple на iOS.

Варто зауважити, що користувачі, які віднесені до мобільної аудиторії, так само можуть користуватись і десктопною версією соцмережі.

Facebook відносить до мобільної або загальної аудиторії користувачів, які хоча б один раз протягом останніх 30 днів зайшли в соціальну мережу, будучи залогіненими ***(60 % українців користуються Facebook за допомогою смартфона або планшета // UkrainianWatcher (http://watcher.com.ua/2015/09/28/60-ukrayintsiv-korystuyutsya-facebook-za-dopomohoyu-smartfona-abo-plansheta/). – 2015. – 28.09).***

***

«ВКонтакте» и дата-центр SDN объявили о подписании договора на размещение части серверного оборудования социальной сети на технологической площадке SDN.

SDN – один из самых крупных ЦОД в Северо-Западном регионе, в настоящее время введены в эксплуатацию четыре очереди проекта, общим объемом 614 серверных стоек. Мощности дата-центра растут и к концу года емкость приблизится к 1000 стоек. Современные технологии охлаждения и электропитания, а также возможности запатентованной технологии «Stack.КУБ», позволяют предоставлять уникальные решения по размещению инфраструктур таких крупных интернет-проектов, как социальная сеть «ВКонтакте». Безопасность и бесперебойность работы ресурсов клиентов – это основная задача всех систем и служб ЦОД.

«С самого начала дата-центр SDN проектировался и строился под большие и сложные IT-инфраструктуры, команда инженеров ЦОД старалась учитывать пожелания и требования будущих клиентов. Размещение крупнейшей российской социальной сети на нашей площадке подтверждает,

что направление развития выбрано правильным, – говорит генеральный директор компании СДН А. Мищенко. В рамках стратегического партнерства «ВКонтакте» получает ИТ-инфраструктуру, на которой сможет легко увеличивать мощности и радовать пользователей надежным и удобным сервисом».

Социальная сеть «ВКонтакте» это высоконагруженный интернет-проект, с трафиком более 80 млн посетителей в день. Постоянная работоспособность ресурса важнейшая цель ИТ-специалистов компании, которые модернизируют и улучшают серверные инфраструктуры и сети передачи данных. С помощью новой площадки «ВКонтакте» обезопасит себя от недоступности сайта и сервисов проекта ***(Социальная сеть «Вконтакте» переезжает // InternetUA (http://internetua.com/socialnaya-set--vkontakte--pereezjaet). – 2015. – 1.10).***

***

Facebook объявила о ряде масштабных изменений в своем приложении на мобильных платформах, сообщается в официальном блоге соцсети.

Главное изменение коснется фотографий профиля пользователей. Вместо них можно будет загрузить короткое зацикленное видео, которое будет демонстрироваться всем посетителям страницы. Кроме того, появится возможность поставить временное фото с подписью, отражающей какое-либо важное событие в жизни.

Сама фотография профиля теперь расположится по центру, а под ней будет возможность сделать подпись длиною до 110 символов с поддержкой эмодзи.

Наконец, пользователи получат возможность выбирать информацию, которую они хотят разместить под фото профиля. Это могут быть как стандартные указания места жительства, работы и учебы, так и последние сделанные фото и видео ***(Facebook позволит загружать зацикленное видео вместо фото профиля // InternetUA (http://internetua.com/Facebook-pozvolit-zaqrujat-zaciklennoe-video-vmesto-foto-profilya). – 2015. – 1.10).***

***

Одно из крупнейших американских изданий Washington Post собирается публиковать все свои материалы напрямую в Facebook через новостную платформу соцсети Instant Articles. «Газета.Ru» выяснила, как этот шаг повлияет на медиа-отрасль и потребление новостей в Интернете.

О том, что социальные сети становятся важнейшим каналом доступа к аудитории для современных медиа, разговоры идут уже не первый год. В марте 2015 г. стало известно, что Facebook ведет переговоры с крупнейшими новостными издательствами о публикации их материалов напрямую в социальной сети, а в мае 2015 г. была запущена платформа Facebook Instant Articles. М. Цукерберг заявил о том, что его компания хочет улучшить пользовательский опыт и скорость загрузки материалов, которая может страдать при переходе на внешний источник. Взамен основатель Facebook

пообещал издательствам разделить доходы от рекламы. Аналогичные новостные платформы запустили YouTube, Twitter и Snapchat, а на сентябрьской презентации свой обновленный новостной сервис представила Apple.

Тем не менее, издательства настороженно отнеслись к предложению М. Цукерберга, поскольку раскрытие данных о читательской аудитории является для них весьма болезненным шагом.

Крупнейшие мировые онлайн-СМИ решились только на ограниченные по объемам тестовые размещения своих материалов в Facebook. Например, по данным WSJ, The New York Times публикует не более 30 материалов в день, а NBC News размещает в Instant Articles 30–40 материалов. Однако BuzzFeed уже собирается публиковать через эту платформу как можно больше своих материалов.

Издательство Washington Post и вовсе хочет быть первым на поприще публикации материалов в соцсетях. «Мы хотим контактировать с нашей нынешней и будущей аудиторией через все возможные платформы», – заявил издатель газеты Ф. Райан. Без накопления соответствующего опыта этот шаг является довольно рискованным. Однако он полностью укладывается в концепцию основателя Amazon миллиардера Д. Безоса относительно современных медиа, которую он ранее озвучил при покупке Washington Post. Д. Безос считает, что Интернет разрушает традиционные медиа, и рекламодатели получили множество новых способов контакта с аудиторией.

«Я ничего не понимаю в газетном бизнесе, – признал Д. Безос после покупки Washington Post. – Однако я кое-что понимаю в Интернете и могу совместить это со своими финансовыми возможностями».

Шаг Washington Post может подтолкнуть медиарынок к настолько же быстрому переходу на новостные платформы социальных сетей, насколько яростно старейшие издательские дома сопротивлялись монополии Google и инициативам молодых интернет-компаний в области новостей.

Одним из доводов против публикации новостного контента через платформы социальных сетей и крупных компаний вроде Apple является опасение, что это убьет мене крупные независимые интернет-СМИ, в результате чего Интернет превратится в некоторое подобие телевидения в плане свободы распространения информации. Пользователи уже неоднократно имели возможность убедиться в том, что М. Цукерберг может вводить своеобразную цензуру в своей социальной сети, исходя из собственного мировоззрения и бизнес-логики компании.

Член правления Всемирной газетной ассоциации В. Гатов считает, что аудитория и доходы Washington Post в результате перехода на платформу Instant Articles, скорее всего, возрастут, хоть ему и неизвестны схемы монетизации, которые планируют использовать издательский дом и Facebook.

«Решение WaPo, наверняка, подтолкнет других издателей к такому же шагу, – рассказал В. Гатов “Газете.Ru”. – Однако и с финансовой, и с

аудиторной точки зрения подобные сервисы набирают значимость не очень быстро».

При этом эксперт уверен, что ни о каком «контроле» за каналами распространения новостного контента не может быть и речи, пока аудитория разлита по множеству методов и форм доставки контента.

«В настоящее время у медиаиндустрии нет ответа на вопрос, как в будущем будет устроено потребление контента, – считает директор по маркетинговым коммуникациям Brand Analytics В. Черный. – Для того чтобы медиа опять стали растущим бизнесом необходимо выработать новые форматы контента, которые придутся по душе пользователям, в том числе молодой аудитории, и адаптировать их под новые каналы распространения. С учетом быстро меняющихся трендов эти задачи выглядят пугающе».

Эксперт полагает, что задача построения нового медиабизнеса в одиночку без сложившейся экосистемы с большой вероятностью обречена на неудачу. Собственно отсюда можно наблюдать и попытки издателей разделить риски, встроиться в новые каналы потребления и оставить за собой только производство контента. «Это понятный и правильный путь», – рассказал В. Черный «Газете.Ru».

С другой стороны, держатели аудитории (соцсети, поисковики, магазины приложений) как новые каналы дистрибуции, заинтересованы «кормить» аудиторию ежедневным контентом. Помимо игр, новости по-прежнему претендуют на заметную долю ежедневного внимания.

Однако пока гиганты упускают время и не могут договориться с партнерами, медийные стартапы достаточно удачно экспериментируют с форматами и каналами распространения, а потому могут предложить более интересные проекты, нежели крупные игроки, которым явно не хватает возможностей для эксперимента – внутренние эксперименты для них слишком дороги.

Таким образом, из нынешних лидеров выживут немногие, и они войдут в альянсы с Apple, Facebook и другими социальными медиа.

«Мы уже полтора года публикуем рейтинги российских СМИ и видим перетекание аудитории новостных медиа в соцсети и сокращение количества цитирования СМИ – это устойчивая тенденция», – говорит В. Черный. По словам эксперта, медийному бренду важно сетевое присутствие в различных каналах потребления, а не статистика продаж собственной площадки. Пищевая цепочка устроена так, что основное потребление контента происходит за пределами первоисточника, а именно в соцсетях. При этом аудитории крупных площадок не показывают заметного роста, поэтому расширение охвата за счет соцсетей и других каналов является общим трендом, а СМИ уступают место социальным медиа.

Что касается перехода контроля над каналами доставки новостей, то эксперт соглашается с тем, что новые новостные платформы в итоге приведут к ограничению свободы в Интернете. Роль поисковиков снижается как за счет роста значимости соцмедиа, так и за счет тренда мобильного потребления и

использования приложений. Да, тема контроля здесь звучит более явственно, однако не она является основным трендом.

«Предыдущие 20 лет драйвером веб-рынка был поиск и бизнес вокруг него, например, контекстная реклама, – говорит В. Черный. – Растущая роль соцмедиа и других каналов потребления требует нового технологического драйвера, который сделает доступными данные социальных сетей и мобильного потребления для бизнеса. Новость об ограничении объема исторического архива сервиса “Яндекс.Блоги” это только подтверждает».

Однако есть и хорошие новости. «Бурно развиваются проекты, целью которых является открытие социальных данных, как минимум, для бизнеса. Среди самых известных – Topsy, Gnip, Datasift. Brand Analytics также работаем над этим», – подытожил эксперт ***(Facebook вместо «бумаги» // InternetUA (http://internetua.com/Facebook-vmesto--bumagi). – 2015. – 29.09).***

***

Через пять лет, к концу 2020 г., каждый житель нашей планеты будет иметь доступ к Интернету. В этом уверен основатель Facebook М. Цукерберг, который объявил на заседании ООН о своих планах. Он намерен создать компанию для внедрения своей мечты в жизнь.

Выступая в Нью-Йорке, М. Цукерберг отметил, что Интернет поможет ООН достичь поставленных целей и покончить с нищетой. Всемирная сеть не только создает новые рабочие места во всем мире, но и дает возможность обмениваться знаниями. А именно знания способны решить возникающие проблемы.

Основатель популярной сети особо подчеркнул, что Интернет является важным средством поощрения прав человека, он помогает достичь «глобальной справедливости».

Как Интернет сможет содействовать экономическому росту? Приступая к новой компании, М. Цукерберг подсчитал, что почти 160 млн людей в развивающихся странах выйдут из нищеты с помощью Интернета. Благодаря расширенному доступ к нему, эти миллионы смогут получить образование. Также этот проект создаст свыше 140 млн рабочих мест.

Информационно-коммуникационные технологии, бесспорно, важны в вопросах обеспечения здравоохранения, образования, для поддержания мира, безопасности и остальных приоритетов.

Миллиардер призвал объединить нации мира, а начать такое объединение предложил с соединение их сетью.

На новую инициативу М. Цукерберга уже откликнулись мировые бизнесмены Р. Брэнсон, Б. Гейтс и актриса Ш. Терон ***(Основатель Facebook победит нищету с помощью интернета // Uinny.ru (http://uinny.ru/index.php?id=1784). – 2015. – 28.09).***

***

«ВКонтакте» встроила плеер YouTube «ВКонтакте» поменяла внешний вид видеороликов с YouTube и Pladform, встроив их в собственный плеер – теперь они стилизованы под стиль самой соцсети.

Нововведение доступно пока лишь в видеокаталоге и новостной ленте, однако в ближайшем будущем планируется применить его ко всем видеозаписям, пишет «Газета.ру». Скин «ВКонтакте» получат и остальные встраиваемые плееры для того, чтобы пользователи видели единый дизайн и работали с привычным интерфейсом.

К оригинальному видеоролику можно будет перейти по ссылке под видео или при помощи клавиши в виде логотипа видеохостинга ***(«ВКонтакте» встроила плеер YouTube // InternetUA (http://internetua.com/vkontakte--vstroila-pleer-YouTube). – 2015. – 3.10).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Президент України П. Порошенко закликав поширювати в соціальних мережах інформацію про агресію Росії проти України із закликом зупинити її під тегом #StopRussianAggression. Про це він написав у своєму Facebook.

«Ми рішуче засуджуємо тероризм у всіх його формах і проявах! Друзі, прошу максимально поширювати: #StopRussianAggression», – закликав П. Порошенко.

Нагадаємо, Президент України П. Порошенко на сесії Генеральної Асамблеї назвав агресію проти України моральним тестом для всього цивілізованого світу, а також закликав ООН засудити пропагандистські гібридні війни.

Президент України П. Порошенко, виступаючи на сесії Генеральної Асамблеї ООН, також закликав ООН і держави-члени організації розпочати безстрокову міжнародну кампанію тиску на російську владу, щоб змусити її негайно звільнити всіх українських громадян, яких вона утримує в заручниках ***(Порошенко просить поширювати повідомлення про агресію Росії під тегом #StopRussianAggression // Телекритика (http://www.telekritika.ua/kontekst/2015-09-30/111729). – 2015. – 30.09).***

***

Фонд Порошенка переказав 73 275 грн благодійному фонду «Таблеточки», який допомагає тяжкохворим дітям.

Ця сума дорівнює кількості привітань Президента в соцмережах із днем народження.

Голова фонду М. Порошенко раніше оголосила відповідний благодійний флешмоб. Нагадаємо, П. Порошенко 26 вересня святкував 50-річчя ***(73 тис. користувачів соцмереж привітали Порошенка з днем народження // LB.ua (http://ukr.lb.ua/news/2015/10/01/317382_73_tis_koristuvachiv_sotsmerezh.html). – 2015. – 1.10).***

***

Прем'єр-міністр України А. Яценюк порадив школярам переходити з російської соціальної мережі «ВКонтакте» в американську Facebook.

Про це повідомив телеканал «112 Україна», який вів трансляцію візиту Прем'єра до київської школи № 148 напередодні Дня вчителя.

Пізніше з офіційної сторінки А. Яценюка у Facebook стало відомо, що він взяв участь в уроці медіаграмотності. Прем'єр запитав, хто з присутніх у класі учнів має акаунти у Facebook.

«Всі решта де? У "ВКонтакте". Пропоную вам переходити у Facebook, ну, це окрема історія, чому. Просто пропоную, я не просто вам кажу, переходьте в Facebook хоча б тому, що М. Цукерберг – засновник Facebook, його сім'я з Одеси, а треба підтримувати своїх», – зазначив А. Яценюк.

Він поцікавився також, чи користають учні YouTube та Twitter, якими темами вони цікавляться. Прем'єр-міністр спитав, чи переписуються діти з вчителями в соціальних мережах. Виявилося, що ні.

Директор школи, колишній журналіст С. Горбачов зазначив, що тільки кілька учнів додалося до нього «у друзі» й додав, що в мережі планується створення робочої групи з медіаосвіти.

На це А. Яценюк запропонував звільняти дітей від уроків, якщо вони «зафрендять» директора. «Ви повинні якось простимулювати. Наприклад, той, хто підписався на акаунт директора, має право на один урок не прийти. Треба стимул якийсь», – жартома зазначив Прем'єр-міністр.

На думку політика, учні та вчителі завдяки новим технологіям зможуть налагодити кращий контакт.

Також Прем'єр-міністр на відкритому уроці з'ясував, що школярів турбують такі теми, як війна і перспектива поліпшення рівня життя в Україні.

Після відвідання школи в соціальній мережі А. Яценюк нагадав, що її директор С. Горбачов став одним із 22 керівників середніх загальноосвітніх навчальних закладів столиці, які були вперше обрані на відкритому незалежному конкурсі. Щодо учнів школи він написав: «Це дуже розумні та глибокі діти!», а також опублікував фото візиту ***(Арсеній Яценюк порадив школярам переходити з «ВКонтакте» у Facebook // Media Sapiens (http://osvita.mediasapiens.ua/web/social/arseniy_yatsenyuk_poradiv_shkolyaram_perekhoditi_z_vkontakte_u_facebook/). – 2015. – 2.10).***

***

Напередодні виступу В. Путіна на Генасамблеї ООН до п’ятірки хештегів в українському Twitter увійшов #PutinKillerMH17. Про це повідомляє espreso.tv.

Український сегмент соцмережі Twitter проводить шторм із нагоди виступу В. Путіна на Генасамблеї ООН. Активісти нагадують, хто винен у падінні малайзійського боїнга MH17, анексував Крим та запроторив за грати українських політув’язнених.

Разом з хештегом #PutinKillerMH17 користувачі соцмережі запускають також хештег #PutinKills, #FreeSavchenko, #FreeSentsov та ін. ***(Twitter штормить хештег про Путіна-убивцю // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44795/118/lang,ru/). – 2015. – 28.09).***

***

На блокпосту при виїзді з Лисичанська Луганської області мешканців перевіряють по кількох базах злочинців та бойовиків. Зокрема, прізвища людей звіряють з базою підозрюваних у сепаратизмі, яку створено і на основі аналізу соцмереж, тобто із сайтом «Миротворець». Про це повідомив полковник МВС С. Альошин.

«Перевірка на КПП проходить по кільком базам. Внутрішню базу учасників незаконних (збройних. – Ред.) формувань складено з оперативної інформації МВС. У неї занесені прізвища підозрюваних у скоєні злочинів, а також осіб, провина яких є доведеною. Такі особи є оголошеними в розшук. Друга база – викрадених авто. У обліку МВС значиться 3950 викрадених автомобілів. Третя база – це база підозрюваних у тероризмі цивільних громадян на сайті “Миротворець”», – повідомив С. Альошин.

За його словами, до внутрішньої бази МВС у Луганській області входить 70,162 тис. осіб, які підозрюються в різних видах злочинів.

«Затримували громадян з підробленими перепустками з окупованих міст Луганщини: Алчевська, Луганська Стаханова та інших. Вони намагались незаконно перетнути лінії розмежування», – повідомив полковник.

Зі слів правоохоронців, сайт «Миротворець» є громадським ресурсом, до якого вносять відомості про сепаратистів із соціальних мереж. Правоохоронці наголосили, що база зазначеного інтернет-ресурсу не є офіційною базою СБУ або інших органів. Причина використання зазначеного інтернет-ресурсу у тому, що він має широку базу.

«Я думаю, що на сайті “Миротворець” є достовірна інформація. Як правило, тут 90 % осіб, які причетні (до незаконних збройних формувань. – Ред.). Соціальні мережі дуже допомагають. Бойовики викладають фотографії у “ВКонтакте”, відео на YouTube про те, як вони убивають та грабують», – повідомив А. Науменко ***(На блокпостах успішно вираховують підозрюваних у сепаратизмі за інформацією з соцмереж // InternetUA (http://internetua.com/na-blokpostah-usp-shno-virahovuuat-p-dozruavanih-u-separatizm--za--nformac--ua-z-socmerej). – 2015. – 29.09).***

***

Учасники найбільшої кіровоградської спільноти в соцмережі «ВКонтакте» – «Кировоград ВКонтакте» проголосували за нову назву для міста.

На вибір було запропоновано сім варіантів назв, серед яких вже у жовтні на загальноміському опитуванні кіровоградці будуть обирати: Благомир, Ексампей, Єлисаветград, Златопіль, Інгульськ, Козацький, Кропивницький.

Найбільше голосів користувачів соцмережі отримав «Єлисаветград» – 73 %. Друге місце посів «Златопіль» – 9,4 %. Третє – Інгульськ, за який проголосувало 7 % учасників групи. Назвати Кіровоград Ексампеєм висловили бажання 3,7 % опитаних. Інші назви не набрали і 3 % голосів. Загалом участь в опитуванні взяли 848 осіб.

Як повідомлялося раніше, Кіровоградська міська рада визначила дату проведення громадського опитування жителів Кіровограда щодо перейменування міста – 25 жовтня, у день проведення в Україні виборів до місцевих рад. Також було затверджено форму опитувального листка ***(У соцмережах обрали назву для Кіровограда // Правдоруб (http://www.pravdorub.kr.ua/news/kirovohrad/u-sotsmerezhah-obrali-nazvu-dlya-kirovograda.html). – 2015. – 30.09).***

***

По благословению архиепископа Запорожского и Мелитопольского Луки были созданы страницы в соцсетях, отражающие новости из жизни Запорожской епархии.

Instagram: https://instagram.com/eparhia_zp

«ВКонтакте»: http://vk.com/zaporozh_eparchia

Facebook: https://www.facebook.com/ZaporozhEparchia

«Одноклассники»: http://ok.ru/group/54614374416391

Twitter: https://twitter.com/EparhiaZP?lang=ru ***(Запорожская епархия УПЦ зарегистрировалась в соцсетях // IPnews (http://www.ipnews.in.ua/index.php/2015/10/02/zaporozhskaya-eparhiya-upts-zaregistrirovalas-v-sotssetyah/). – 2015. – 2.10).***

***

Общественный совет при Федеральной службе безопасности России намерен популяризовать среди населения деятельности ведомства. С этой целью планируется использовать возможности социальных медиа, пишет «Обозреватель» (http://obozrevatel.com/abroad/39871-v-rossii-sobralis-podnyat-imidzh-fsb-pri-pomoschi-sotssetej.htm).

Об этом сообщает Центр общественных связей ФСБ, передает «РИА Новости».

«Контекст социально-политической ситуации в стране требует развития диалога с обществом, создания более ясного представления о деятельности спецслужбы и ориентации на запросы молодого поколения, активно

использующего сеть Интернет. Для выполнения этих задач информационная политика совета при ФСБ России будет шире использовать возможности коммуникации через социальные медиа и сервисы», – отметил председатель совета В. Титов.

На заседании состоялась презентация электронной версии журнала Общественного совета «ФСБ: за и против». Ее запуск в Интернете намечен на IV квартал этого года ***(В России собрались поднять имидж ФСБ при помощи соцсетей // Обозреватель (http://obozrevatel.com/abroad/39871-v-rossii-sobralis-podnyat-imidzh-fsb-pri-pomoschi-sotssetej.htm). – 2015. – 23.09).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

IGate продолжает цикл материалов о том, как получить дополнительный заработок в Интернете, сэкономить или найти добавочную стоимость там, где ее, на первый взгляд, нет.

Миллиарды людей ежедневно посещают социальные сети, из них сотни миллионов составляют русскоязычную аудиторию. Сравнительно новый растущий сегмент интернет-трафика живет по законам, отличным от традиционного Интернета. И возможно именно в этом заключается одно из его главных преимуществ с точки зрения заработка. Тот, кто раньше и эффективнее других научится наращивать базу подписчиков на свои страницы в соцсетях, сможет конвертировать свои преимущества в сотни и тысячи долларов дохода ежемесячно.

Потенциал заработка

По словам А. Зюзикова, SMM менеджера с четырехлетним опытом работы, он знает 11-летних школьников, у которых есть группы «ВКонтакте» с 70 тыс. подписчиков. «Если хотя бы раз в день в таком паблике размещается рекламный пост, то такой школьник, если он планирует поступать в вуз, спокойно может заработать себе на контракт», – говорит А. Зюзиков.

Группа, состоящая из очень денежной и узкой целевой аудитории – жители столицы 25–35 лет – и насчитывающая 50 тыс. подписчиков, может продавать один пост за 20 дол. Размещая не более двух рекламных постов в один рабочий день, группа в месяц может приносить до 800 дол. Однако быстро добиться таких результатов новичку вряд ли удастся, поскольку погружение в «тему» и понимание нюансов бизнеса будет приходить по мере совершения проб и ошибок.

Начало

Начинать SMM бизнес надо с той социальной сети, которая привычнее, где больше пользовательского опыта. Тогда меньше времени уйдет на ее освоение. Кроме того, если человек привык общаться в какой-то одной социальной сети, он знает, как она работает, чувствует стиль общения людей, которые ей пользуются.

Затем надо подписаться на паблики различных тематик и наблюдать за тем, какого рода рекламу они размещают. Тогда придет понимание того, какие товары в данной социальной сети выгодно продвигать, какая ценовая категория этих товаров, где их можно закупить или где найти партнерскую программу, к которой можно подключиться. Особое внимание стоит уделять оформлению рекламного объявления. Оно много расскажет о том, на каком рекламном языке надо доносить информацию, чтобы люди покупали товары и услуги.

Постоянное изучение рынка будет способствовать погружению в SMM бизнес. И со временем станет понятно, какие действия необходимо предпринимать для создания и развития собственного SMM бизнеса.

Упрощенно вся концепция SMM бизнеса заключается в создании в соцсети страниц (Facebook) или групп («ВКонтакте»), набора подписчиков и публикации на своих страницах или в группах:

• постов со ссылками на свои сайты, которые продают товары или услуги;

• постов со ссылками на партнерские программы, которые продают товары или услуги;

• постов за деньги от рекламодателей.

Тематику страниц или групп лучше выбрать из списка самых денежных тематических ниш:

• здоровье;
• мотивация;
• бизнес;
• заработок;
• отношения мужчины и женщины;
• воспитание детей;
• успех;
• самообразование и личностное развитие;
• отдых и туризм;
• роскошь;
• юмор.

В перечисленных темах всегда много рекламодателей, они тратят большие рекламные бюджеты и эти темы интересны широкому кругу людей, у которых есть деньги.

Но еще очень важно, чтобы тема была интересна самому автору страницы или группы. Тогда он будет мыслить также, как подписчик, понимать, какие посты будут полезными и интересными аудитории. Ему будет проще находить полезные публикации, а подписчики будут активнее делиться постами.

Особым преимуществом будет выбор тех тем, в которых автор обладает ценным жизненным опытом и имеет высокую компетенцию, по сравнению с большинством людей. Это будет сильным конкурентным преимуществом, позволит владельцу выделиться на фоне подобных пабликов и будет его «фишкой». Несмотря на огромные массивы бесплатной информации в Интернете, качественных данных очень мало. Поэтому, как говорит

А. Зюзиков, очень много людей сегодня готовы платить за качественную информацию и тратить деньги на самообучение.

Контент

После выбора темы и создания страницы следующий этап – наполнение страницы контентом. С точки зрения ценности и эффективности паблика почти весь контент на нем должен быть уникальным. Но на деле это встречается крайне редко, как, впрочем, и в традиционном сегменте Интернет.

Если нет времени и возможности постоянно создавать собственный контент, профессиональные SMM менеджеры берут контент из других источников. Они лишь по правилам этики в публикации добавляют ссылку на источник. Поэтому основной принцип работы крупных пабликов заключается в агрегировании контента. «В Интернете можно получить доступ к любой информации, вопрос в том, кто первый ее найдет, обработает и разместит у себя», – так объясняет «кухню» А. Зюзиков.

При этом он подчеркивает – неправильно думать, что если я что-то копирую, то значит, что это все читали. «Интернет настолько огромен, что даже если 100 площадок скопируют одно и то же, у них будет своя аудитория читателей, которая впервые узнает о той или иной новости», – говорит SMM менеджер.

Подписчики

После первоначального наполнения контентом в страницу или группу надо приглашать подписчиков. Начать проще всего, пригласив своих друзей. Это может быть массовый запрос или индивидуальный. Затем со своего паблика надо делать перепосты в свой личный профиль, чтобы друзья читали посты, репостили их и их друзья вступали в группу или подписывались на страницу.

Еще можно делать перепосты в сторонние страницы или группы, причем необязательно, чтобы начинающий SMM-щик состоял в них. Например, в Facebook есть огромное количество тематических групп, куда можно делать перепосты. Если в них нет откровенной рекламы, они не частые, носят полезный или веселый характер, без коммерческой составляющей, то многие владельцы групп на это реагируют адекватно.

В некоторых случаях стоит предварительно договориться с владельцами групп о регулярных перепостах полезной информации. Тогда владелец группы регулярно получает контент, а тот, кто делает перепост – получает трафик на свою группу.

Также необходимо использовать рекламу. Она требует денег, но небольших. За счет рекламы можно быстро привлечь подписчиков и намного больше, чем бесплатными способами.

Ориентиры

Количество подписчиков – это ключевой показатель страницы или группы в социальной сети. Он позволяет примерно оценить потенциал дохода от владения такой страницей или группой. А. Зюзиков говорит, если к SMM бизнесу подходить серьезно, то надо ориентироваться на 100 тыс. подписчиков.

Это пороговое значение, достигнув которого, можно зарабатывать на прямом привлечении рекламодателей.

Для заработка без рекламодателей страница, например, в Facebook должна иметь хотя бы 10 тыс. подписчиков. Тогда опубликованный пост с партнерской ссылкой увидит хотя бы тысяча человек, 100 человек перейдет по ссылке, 1 купит. В этом бизнесе стоит ориентироваться на конверсию в 1 %, а соотношение познавательных постов к рекламным – 9 к 1.

Таким образом, 10 тыс. подписчиков позволит заработать первые деньги. А для того, чтобы зарабатывать на жизнь, нужно иметь аудиторию 50–100 тыс. человек ***(Как заработать в социальных сетях // IGate (http://igate.com.ua/news/10258-kak-zarabotat-v-sotsialnyh-setyah). – 2015. – 23.09).***

***

Рекламные расходы на социальные сети растут быстрее, чем ожидалось. По прогнозу eMarketer, они достигнут 25,14 млрд дол. в 2015 г. Рекламные доходы Facebook составят 16,29 млрд дол., увеличившись на 41,8 % за 2014 г. В этом году на Facebook придется 64,8 % всех рекламных расходов на социальные сети. Своему быстрому росту социальная сеть обязана Instagram. На приложение пришлось 5 % всех рекламных доходов Facebook. В 2016 г. рекламные доходы Instagram возрастут на 149 %, достигнув 1,48 млрд дол. На Twitter придется 8,1 % всех расходов на социальные сети в этом году. Его доходы от рекламы возрастут на 61,8 % в 2015 г. «Twitter улучшил рекламный таргетинг и все еще предоставляет коммуникацию в реальном времени, но рекламодатели хотят достичь массовой аудитории, и это труднее сделать на Twitter, чем на Facebook», – отметил аналитик компании ***(На Facebook придется 65 % всех рекламных расходов на соцмедиа в 2015 // Marketing Media Review (http://mmr.ua/show/na_facebook_pridetsya_65_vseh_reklamnyh_rashodov_na_sotsmedia_v_2015) . – 2015. – 24.09).***

***

Как зарабатывать деньги на YouTube

Каждому пользователю Интернета знакомы вирусные видео на YouTube. Они бывают всех форм и размеров, от суперпопулярных музыкальных клипов до роликов с сердитой кошкой. Но у них всех есть кое-что общее. Люди, разместившие эти видео, немало заработали, пишет Business Insider.

Как же начать делать деньги на YouTube?

Первые шаги

Заработать большие деньги на YouTube не так легко, как может показаться на первый взгляд. Существует множество препятствий, которые придется преодолевать в процессе. Так что, определенно, это не быстрый заработок. Но, если у пользователя есть хобби, он в чем-то, по-настоящему, хорош и хотел бы помочь людям, забавный или любит поразвлечься, YouTube

может предоставить шанс заработать несколько долларов, просто делая то, что нравится.

Первый и самый очевидный шаг – завести аккаунт на YouTube. При этом у пользователя заранее должна быть идея того, какие видео он планирует размещать. Затем необходимо активировать монетизацию в сервисе Google AdSense.

Активация монетизации означает, что пользователь обязуется загружать только те видео, на которые имеет права, а также соглашается соблюдать условия сервиса (к примеру, не накручивать просмотры на собственных видеороликах). В Google AdSense нужно указать информации о том, куда будут начисляться платежи, когда деньги начнут «литься рекой».

После этого нужно стать партнером YouTube. В настоящее время сделать это намного проще, чем раньше. Достаточно, чтобы общее время просмотров загруженных видео достигло 15 тыс. часов. Партнерство с YouTube позволяет пользователю загружать видеоролики длиной более 15 мин. Это может быть очень полезно для некоторых видеопроектов. Также партнер получает доступ к аналитике и более продвинутым инструментам редактирования видео.

Теперь, когда у есть канал, соглашение с Google AdSense и партнерство с YouTube, видео-блогер готов к следующему этапу.

Типы рекламы

На YouTube существуют разные типы рекламы: текст, отображающийся в нижней части видео, рекламный клип, который воспроизводится перед самим видео. Можно выбрать, какой из этих типов будет отображаться в видео. Выбор может отличаться в зависимости от аудитории канала и того, какие деньги приносят просмотры.

То, как работает реклама на YouTube, это, вероятно, одна из самых сложных вещей, с которыми придется столкнуться блогерам. Реальная оценка составляет примерно 7,5 дол. за тысячу показов. Сложность состоит в том, как система определяет, что такое «показы». Заработать на YouTube можно только тогда, когда зритель взаимодействует с рекламным объявлением, либо когда состоится «показ» рекламы зрителю.

Это означает, что если кто-то пропускает рекламу, либо пользуется блокировщиком рекламы, блогер не получает деньги за просмотр. Из-за этого оценка количества просмотров и того, сколько эти просмотры приносят пользователю, становится весьма непростой задачей. Она также сильно зависит от того, идет ли речь о рекламном клипе перед роликом, или о баннере, который отображается в нижней части видео. Все это определяет, сколько людей будет взаимодействовать с рекламой, и какую сумму на этом можно заработать.

Кроме этого, существует еще множество факторов, которые могут повлиять на заработок на YouTube. Аудитория канала имеет непосредственное отношение к типу рекламы, который сработает лучше всего. К примеру, если снимать короткие смешные ролики, вероятно, не стоит включать перед ними тридцатисекундные рекламные ролики – зритель просто будет их пропускать. К

счастью, у YouTube есть страница аналитики, где можно посмотреть примерные данные об аудитории видео – от демографии до времени суток и географии просмотров ***(Как зарабатывать деньги на YouTube // InternetUA (http://internetua.com/kak-zarabativat-denqi-na-YouTube). – 2015. – 30.09).***

***

Адміністрація YouTube розіслала лист власникам популярних американських каналів, у якому повідомляє про запуск платної версії сайту без реклами.

У зв'язку з цим до 22 жовтня видавцям відеоконтенту потрібно прийняти нові умови угоди з YouTube. Інакше, їх відео більше не будуть доступні для публічного перегляду або монетизації в США. Імовірно, саме на цю дату і запланований запуск нового сервісу.

Платна версія відеохостингу буде називатися YouTube Red. Плата за використання його становитиме близько 10 дол. на місяць. У ціну підписки також, напевно, увійде доступ до музичного сервісу YouTube Music Key ***(YouTube за місяць запустить платну версію // UkrainianWatcher (http://watcher.com.ua/2015/09/29/youtube-za-misyats-zapustyt-platnu-versiyu/). – 2015. – 29.09).***

***

Google анонсировала появление рекламы в YouTube с возможностью перейти к покупке товара. Об этом компания сообщила в своем блоге.

Принцип функционирования опции компания показала с помощью изображения. Сначала в правой части экрана появляется значок информации («i») и строка с основными данными о товаре. Если пользователь на нее нажимает, открывается изображение продукта с указанием цены и кнопкой «Купить», которая позволяет перейти на сайт рекламодателя.

Продуктовые «карточки» без функции покупки компания представила еще 21 мая. Они делятся на несколько типов: демонстрирующие товар, предлагающие материально поддержать проект (фандрайзинг), рекламирующие видео или плейлист на YouTube, а также переводящие на связанный с каналом сайт.

По сообщению компании, соединение двух этих опций – «карточек» и кнопки «Купить» – сделает объявления более удобными для покупки. Функции будут работать так же, как реклама в поиске Google: по аукционной модели, с таргетингом на основе контекста и аудитории.

По словам представителей YouTube, количество просмотров видео на платформе (таких, как обзоры и уроки) в прошлом году возросло на 40 %. В недавнем исследовании ряд ученых из разных организаций уличили Google в получении средств за просмотр рекламы на YouTube ботами – по итогам эксперимента сервис AdWords выставил счет за 91 показ рекламы при том, что все 150 просмотров были снегерированы ботами ***(YouTube внедрит кнопку «Купить» прямо в рекламные объявления // IGate***

(http://iqate.com.ua/lenta/10410-youtube-vnedrit-knopku-kupit-pryamo-v-reklamnye-obyavleniya). – 2015. – 30.09).

***

Социальная сеть Facebook предоставила новые возможности для закупки рекламы, а также презентовала инструменты для измерения эффективности мобильных кампаний. Об этом пишет adindex.ru (http://www.adindex.ru/news/digital/2015/09/28/128305.phtml).

Facebook запускает новую метрику – TRP (Total rating point, целевой рейтинг), которая позволит рекламодателям планировать размещение, закупать видеорекламу и измерять ее в Facebook наряду с ТВ-кампаниями.

В блоге Facebook говорится, что маркетологи смогут планировать кампании на ТВ и в Facebook параллельно, ставя перед собой общие цели, а также закупать долю TRP напрямую через соцсеть, сообщает издание Campaign.

Нововведения стали доступны благодаря сотрудничеству Facebook с аналитической компанией Nielsen, которая сможет контролировать общий TRP для соцсети и телевидения.

С увеличением числа аудитории, использующей мобильные телефоны, компания Facebook объединилась с Millward Brown Digital, чтобы рекламодатели могли анализировать результаты рекламных кампаний в мобайле. Также клиентам станет доступна возможность проведения мобильных опросов ***(Facebook запустил инструменты таргетинга для ТВ-рекламодателей // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44805/118/lang,ru/). – 2015. – 28.09).***

***

Twitter представил Video App Card – новый формат рекламы установки приложений, который позволяет разработчикам продвигать свои продукты с помощью видеороликов. Об этом пишет searchengines.ru.

Новый формат выведен из беты и запускается по всему миру. Рекламные ролики предлагают пользователям предварительный просмотр приложения и автопроигрываются в новостной ленте. Маркетологи, занимающиеся продвижением мобильных приложений, также смогут использовать все доступные в Twitter виды таргетинга.

Напомним, что бета-версия этого функционала была запущена в июле. На тот момент доступ к ней получило лишь ограниченное число рекламодателей.

В августе Twitter вывел из беты две новые опции для оплаты рекламы установки приложений. Теперь рекламодатели смогут установить приоритет на установки как при оплате на базе CPC, так и при назначении ставок, основанном на цене за установку ***(Twitter запустил новый формат рекламы установки приложений, включающий видео // МедиаБизнес***

(http://www.mediabusiness.com.ua/content/view/44787/118/lang,ru/). – 2015. – 25.09).

***

Трейдеры все чаще обращаются к Twitter, чтобы не отставать от основных рыночных тенденций.

Именно это способствовало появлению компаний, которые трактуют сигналы, полученные из социальной сети.

В прошлом году Twitter выкупила одну из таких компаний, Gnip, за 130 млн дол., которая распространяет полученную из сети информацию хедж-фондам и другим клиентам.

Э. Эллис, директор Gnip по маркетингу, отмечает, что Twitter также продает информацию банкам и хедж-фондам напрямую. «Сообщения в Twitter могут двигать рынки, так как являются отражением положения вещей в реальном времени. В будущем для финансовой индустрии наши услуги станут уже не полезным дополнением, а маст-хевом», – утверждает она.

Рассмотрим ряд стартапов, которые занимаются конвертированием твиттов в торговые сигналы:

Selerity сотрудничает с Symphony

Selerity привлекла к себе всеобщее внимание еще в начале года, опубликовав финансовые результаты Twitter, еще до их официального выхода.

Ежедневно компания анализирует около 8 млн документов, в числе которых и публикации в СМИ, генерируя сигналы для пользователей.

Недавно она начала сотрудничать с системой передачи сообщений Symphony.

iSentium популярна в Goldman Sachs

Компания рассчитывает Индикатор силы настроений, SSI, на основе Индекса относительной силы (RSI), с использованием запатентированных значений вместо цены.

Эта компаний появилась на рынке уже давно и уже стала рентабельной. Ее услугами пользовались Д. Хеллер, работавший в Goldman и М. Спайкер, бывший президент Apollo Global.

TickerTags обрабатывает 350 тыс. сигналов из соцсетей

Компания из Далласа анализирует сигналы из соцсетей и выводит определенные тенденции, впоследствии оценивая их влияние на рынок.

Так называемые «тэги», или сигнальные слова фильтруются из более чем 50 млн твиттов, однако услуги TickerTags обходятся трейдерам недешево, а именно 10 тыс. дол. в месяц.

PsychSignal намерена стать новым инструментом оценки волатильности

Основатель компании Д. Крейн-Бейкер отмечает, что «через 5 лет сигналы из соцсетей будут на экранах каждого трейдера».

TheySay ориентируется на Китай

Лондонская компания продает пакеты данных за 5 тыс. дол., и среди ее клиентов уже есть ряд хедж-фондов.

Принимая во внимание волатильность фондового рынка Китая, TheySay намерена сконцентрироваться на более глубоком анализе экономических настроений в стране.

MarketPsych – еще один из аналитических сервисов, сотрудничающих с крупными компаниями

С 2012 г. MarketPsych сотрудничает с Thomson Reuters, делая оценку психологической обстановки на рынке, посредством анализа 7 тыс. соцстраниц и 40 тыс. других ресурсов.

Contix планирует внести социальный контекст на сырьевые рынки

Множество алгоритмов ежедневно обрабатывают торговые сигналы Twitter, однако Contix намерена применять эту методику и на сырьевых рынках, на пользу институциональным клиентам.

Dataminr лидирует по финансовой поддержке

Dataminr – один из крупнейших и наиболее хорошо финансируемых сервисов, работающих в сфере соцсетей. В своем распоряжении она имеет финансовую базу в размере 180 млн дол.

Компанию поддерживают бывший глава Citigroup, В. Пандит, Thomson Reuters – Т. Глосер и Morgan Stanley – Д. Мек ***(Twitter создал новую экосистему на Уолл-Стрит // Take-profit.org (http://take-profit.org/newsreview.php?mid=64914). – 2015. – 30.09).***

***

Спустя два года тестирования Twitter официально запускает кнопку «Купить». Она доступна для всех торговцев на территории США, которые используют одну из трех главных платформы электронной коммерции. Магазины, клиенты Demandware, Bigcommerce или Shopify могут вставить ссылку на продукт в твит, в котором затем появится кнопка для покупки.

Пользователи социальной сети смогут покупать товары в два клика: первый – на кнопке, второй – для подтверждения покупки. Хотя в первый раз им придется ввести платежные данные и адрес доставки.

«Мы перешли от тестирования функции с сотнями до работы с миллионами торговцев. Новая возможность встроена в программное обеспечение, которым они пользуются для управления бизнесом каждый день», – сообщил директор по коммерции Twitter Н. Хаббард в официальном блоге компании ***(Twitter в США запустил кнопку «Купить» // Marketing Media Review (http://mmr.ua/show/twitter_v_ssha_zapustil_knopku_). – 2015. – 30.09).***

***

Instagram начал 30 сентября показ рекламы для российских пользователей, говорится в сообщении компании, поступившем в редакцию lenta.ru. Объявления будут сопровождаться пометкой «Реклама».

Фотохостинг намерен предоставлять свою площадку как крупным рекламодателям, так и малому бизнесу в более чем 30 странах. Партнером на российском рынке стал реселлер AiTarget, который также отвечает за рекламу в Facebook в России. Кроме того, Instagram планирует расширить количество локальных партнеров. К ним, например, добавится IMHO Vi (сотрудничает с Facebook, «Яндексом», Rambler&Co).

Рекламодателям будут доступны три формата: видео длительностью до 30 секунд, картинка со ссылкой и картинка с кнопкой установки приложения. Также компании могут использовать таргетинг: пол, возраст, интересы пользователей и т. д.

В свою очередь пользователь может скрыть не интересные ему рекламные посты, и со временем алгоритмы сайта будут подстраиваться под его вкусы. Первыми рекламодателями стали «Яндекс.Такси», Beeline, Samsung, L'Oreal, Nestle, Unilever и Lamoda.

О запуске рекламы в Instagram на российском рынке стало известно в начале сентября. Глобальная аудитория сервиса на сегодняшний день превысила 400 млн человек. Россия входит в пятерку стран по числу пользователей сервиса ***(Instagram запустил рекламу в России // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44839/118/lang,ru/). – 2015. – 1.10).***

***

Instagram обладает самой молодой аудиторией, отмечает исследование globalwebindex.net. Около 70 % моложе 35 лет, а более 60 % заходят на платформу ежедневно, показывая самый высокий уровень вовлеченности среди других соцмедиа, кроме Facebook. Именно активное взаимодействие пользователей с брендами привлекает внимание маркетологов. Более половины из них отметили, что следуют за своими любимыми брендами. Кроме того, они заходят на площадку, чтобы больше узнать о продукте и бренде. 30 сентября рекламный кабинет сервиса стал доступен и для украинских компаний ***(Половина пользователей следуют за брендами // Marketing Media Review (http://mmr.ua/show/polovina_polyzovateley_instagram_sleduyut_za_brendami). – 2015. – 1.10).***

***

Как избежать распространенных ошибок в рекламной кампании в Facebook

Р. Брар – владелец издательства Fetopolis, журналы которого имеют миллионы подписчиков в Facebook.

Чтобы увеличить эффективность канала, он запустил масштабную рекламную кампанию в соцсети – по предварительным исследованиям, она должна была окупиться в двух- или трехкратном размере. Предприниматель потратил более 600 тыс. дол. за четыре дня, но не получил вообще никакой прибыли.

В рубрике Digital – перевод заметки журналиста Э. Тэйта о том, как избежать распространенных ошибок при работе с рекламой Facebook.

Вам не нужны поклонники

«Чтобы у нас появились преданные поклонники, мы потратили более 600 тыс. дол.», – признался Р. Брар в публикации на Business Insider. Но вдумайтесь – поклонники? Они и есть у Т. Свифт, The Giants, пылесосов Dyson. У компании же есть только клиенты. И если вас интересуют «метрики тщеславия» (лайки или фанаты), в конечном счете вы не получите ничего кроме пустых кликов.

Перед тем как запускать рекламу в Facebook, необходимо в первую очередь определить наиболее приоритетную цель – от этого зависит выбор способа оплаты. В Facebook они представлены тремя типами: CPM, CPC, и oCPM.

CPM (Cost per mille) – плата за показ

Если вам требуется только повысить узнаваемость бренда, это самый оптимальный вариант. Вы платите только за показы объявлений, а не за переходы по ссылке или просмотры целевых страниц. Оплата происходит за каждую 1000 показов.

Этот способ не гарантирует наплыва новых пользователей на ваш сайт или запредельное количество кликов, поэтому, если вам нужны конкретные результаты, лучше воздержаться от использования этой опции.

CPC (Cost per click) – плата за клик

На мой взгляд, неумелое обращение с этой опцией и разорило Р. Брара. При ее использовании вы платите за каждый клик в области объявления: это могут быть клики по картинке, кнопке «мне нравится», «комментировать», имени – необязательно по сопряженной ссылке. Это и приводит новичков в замешательство: вроде бы клики есть, рекламный бюджет исправно тает, а конверсия всё равно стремится к нулю.

В настоящее время Facebook хочет оптимизировать расчет за клики и привязать его непосредственно к целям конкретной рекламной кампании. Учитываться будут переходы по ссылке с последующим просмотром целевой страницы, переходы по призывам («Подписывайтесь на канал», «Участвуйте в рассылке» и т. д.), переходы с последующей установкой ПО или клики с просмотром видео на стороннем сайте.

oCPM (оптимизированный CPM)

Если у вас слишком мало (или, наоборот, слишком много опыта) в закупках рекламы в Facebook, эта опция подойдет как нельзя лучше. При планировании рекламной кампании она стоит по умолчанию. Всё, что вам требуется, – это указать лимит максимально допустимой платы за желаемое действие пользователя, а алгоритмы Facebook выберут наиболее эффективную стратегию расходов.

Также радует возможность настройки практически под любые цели кампании, будь то переход пользователей на целевую страницу, увеличение охвата и вовлеченности аудитории, учет установок программного обеспечения

или сбор «лайков». Если вы хотите увидеть на своем сайте большое количество новых посетителей, лучше воспользоваться именно этим инструментом.

Никогда не пускайте на самотек свои собственные рекламные кампании. В Fetopolis вместо того, чтобы тщательно всё спланировать, решили ограничиться раздутым рекламным бюджетом. Вам же нужно точно знать, сколько вы готовы потратить и строго придерживаться принятого бюджета.

Всегда главная цель любой рекламы – получение прибыли. До тех пор, пока доходы от продаж превышают затраты на рекламу, она работает, причем независимо от того, сколько лайков и поклонников вы привлекли.

Если вы используете oCPM, значит, вы уже сообщили Facebook о своем бюджетном максимуме, так что в этом случае можно не переживать о выходе за пределы установленного лимита. Сколько бы средств вы не закладывали, размещая рекламу на Facebook, начните с небольшой суммы, а затем постепенно (не за пару дней) увеличивайте ее до установленного значения.

Точно определите целевую аудиторию

На мой взгляд, основная причина провала большинства рекламных кампаний на Facebook – это отсутствие четкого понимания, кому должно быть адресовано то или иное рекламное сообщение. Из-за размытой целевой аудитории реклама проходит мимо тех, кого она могла бы заинтересовать.

На сегодняшний день лучшей опцией таргетинга однозначно является Custom Audiences. Если вам доступна необходимая информация – списки почтовых ящиков, номера телефонов, ID пользователей, то в этом случае вы сможете получить доступ именно к той аудитории, которую хотите привлечь.

Воспользовавшись опциями Lookalike Audiences (поиск похожей аудитории) и Audience Insights (данные о демографических показателях аудитории), вы сможете существенно расширить базу таргетинга.

Те специалисты, чья реклама не приносит желаемого эффекта, наверняка не уделяют таргетингу должного внимания. В лучшем случае они выделяют сегменты аудитории на основе ее интересов. Раньше этот способ был эффективен, но сейчас он приносит в основном пустые лайки от фейковых аккаунтов, обладатели которых стараются сделать страницы более реалистичными, копируя интересы других пользователей.

Другая опция таргетинга – это сегментирование по стране проживания. Вполне очевидно, что, если вы продаете продукт только в США, его реклама среди жителей Катманду станет досадной ошибкой. Более того, некоторые страны славятся организацией целых синдикатов по генерации лайков (чаще всего это юго-восточная Азия).

Людей отталкивают непривлекательные объявления

Разрабатывайте дизайн рекламы с оглядкой на целевую аудиторию. Объявления Facebook должны соответствовать задачам кампании и привлекать внимание ЦА с первого взгляда. Всегда срабатывают яркие, заметные публикации, ориентированные на конкретных покупателей.

Кроме этого, они должны обладать отличным графическим и информационным содержанием. Эта реклама предназначена для стартапов и играет на их потребности в расширении пользовательской базы.

Также рекламе необходимо обладать социальным влиянием и явным призывом к действию.

Форматы

Не менее важным атрибутом объявления является место появления объявления. Наибольшим количеством просмотров и кликов обладает нативная реклама, которые демонстрируются непосредственно в ленте пользователя. С ее помощью можно неплохо увеличить количество продаж и лидов.

Более скромным успехом пользуются нативная реклама в мобильном приложении и объявления, отображаемые в правой колонке. При этом для ретаргетинга они подходят лучше всего и стоят на порядок меньше.

В новостной ленте мобильной версии Facebook лучше рекламировать другие приложения, предлагая пользователям их немедленную установку. Реклама веб-ресурсов едва ли окажет существенное влияние на их конверсию.

Ни дня без тестов

Р. Брар наивно полагал, что всё, что от него требуется, – это зарегистрироваться, составить объявление и тихо ждать, пока волна народной любви не накроет его потоком лайков.

Беда именно в том, что большинство пользователей Facebook Ads не является профессиональными рекламщиками. Они просто вводят номер кредитной карты и надеятся на чудо.

К сожалению, действовать нужно прямо противоположным образом. Чтобы реклама заработала, требуется постоянный контроль.

Так выглядит алгоритм работы с Google Ad: вы составляете объявление, проводите тесты, вносите требуемые изменения, отмечаете результат и забываете про него: система работает без вашего участия. Всё потому что Google – это инструмент для удовлетворения потребностей: ваше объявление показывается только тем, кто ищет нечто близкое к его содержанию.

А вот так выстраивается алгоритм работы с Facebook: вы составляете объявление, проводите тесты, вносите изменения, снова проводите тесты, снова вносите изменения, надеясь попасть на волну пользовательского интереса, и т. д. до бесконечности.

Но самое главное – необходимо регулярно тестировать и обновлять дизайн рекламного объявления: изображения, текст, заголовки в зависимости от предпочтений целевой аудитории. Иными словами, Facebook – это инструмент для создания потребностей, ведь объявления демонстрируются определенной группе пользователей.

Поэтому да, для того чтобы получить видимые результаты, требуется много работы, но она стоит потраченных усилий, особенно, когда вы видите прирост аудитории. Это сложный процесс, но он открывает массу возможностей.

Тестирование также включает в себя проверку пригодности Facebook как инструмента в целом. Может оказаться, что он является далеко не лучшим каналом для вашего продукта. Следует помнить, что реклама в соцсетях работает отнюдь не как AdWords, и если вы ожидаете аналогичных результатов, вас ждет разочарование.

Как не прогореть на Facebook Ads

Как только вы решили начать рекламную кампанию в соцсети, вам необходимо четко решить, каких целей вы хотите достичь, кто ваша целевая аудитория и сколько вы готовы потратить. Ну а затем вам нужно снова и снова тестировать и оптимизировать объявление – до тех пор, пока конверсия не достигнет желаемого уровня.

Возможно, у вас от потраченных 60 дол. толка выйдет больше, чем у Р. Брара от 600 тыс. дол. Понимая, как работают механизмы Facebook Ads и как выжать из них все по максимуму, вы можете провести рекламную кампанию, которая зацепит именно ту аудиторию, которая вам нужна, и приведет этих людей к вам на лендинг ***(Как избежать распространенных ошибок в рекламной кампании в Facebook // Состав.ру (http://sostav.ua/publication/nachalo-reklamnoj-kampanii-v-facebook-kak-izbezhat-rasprostranennykh-oshibok-68578.html). – 2015. – 1.10).***

***

Останнім часом кількість користувачів соцмереж безперервно зростає. Багато з них зареєстровані на кількох ресурсах одночасно. При цьому небагато хто задумується про те, що профіль у соцмережі може вплинути на процес працевлаштування. За даними дослідження HeadHunter, 76 % роботодавців переглядають сторінки кандидатів перед тим, як запросити їх на співбесіду або взяти на роботу. Експерти запропонувати п’ять кроків, як поводитися в соціальних мережах, щоб не зашкодити майбутній кар’єрі, передає кореспондент Львівського порталу.

На перший погляд, найпростіший спосіб убезпечити себе – видалити або блокувати акаунт. Такий підхід докорінно неправильний. На думку роботодавців, сторінки в соцмережах можуть стати ще одним аргументом, щоб запропонувати вам роботу. Прихований профіль, навпаки, насторожить рекрутера і примусить будувати здогадки щодо питань, які його цікавлять. Тому найкращим рішенням буде відредагувати зміст сторінки і використовувати її як додатковий інструмент при пошуку роботи.

Крок 1. Погляньте на контент очима роботодавця

Відвідуючи профіль пошукача, роботодавець має перед собою цілком конкретну мету. Для нього важливо дізнатися, які у вас інтереси й цінності, а також зрозуміти, чи впишетесь ви в корпоративну культуру компанії. Репости на стіні, статуси і коментарі повинні працювати на професійний імідж пошукача. Особливо насторожі слід бути тим, чия професійна діяльність напряму пов’язана з брендом компанії (маркетинг, PR, SMM).

Крок 2. Видаліть фотографії, що вас компрометують

Опинившись на сторінці пошукача, рекрутер може і не читати статуси або коментарі, але фотографії подивиться обов'язково. Не варто викладати фото з вечірок або застільних посиденьок, а також знімки на пляжі. Фото в соцмережах відображають діяльність пошукача, його інтереси й захоплення. Наприклад, фотографії з мандрівок розкажуть про активність пошукача, його прагнення дізнаватися щось нове, а фото з дітьми – про сімейні цінності. Якщо у вас є цікаве хобі (берете участь у велопробігах, займаєтесь верховою їздою або танцюєте), можна розповісти про це з допомогою фотографій. Також не забудьте розмістити фото із семінарів і професійних конференцій. Нехай фотоальбоми будуть свідченням ваших досягнень.

Крок 3. Встановлюйте контакти і розширюйте френдліст

Приказка «скажи мені, хто твій друг, і я скажу, хто ти» найкраще ілюструє взаємодію в соцмережах. Професійний світ дуже тісний. І потенційний роботодавець може побачити спільних знайомих, які готові надати вам хороші рекомендації. Пам'ятайте про правило шести рукостискань і не закривайте свій френдліст. Активно користуйтеся інструментами нетворкінгу, розширюйте своє коло спілкування. Користувач, у якого список друзів обмежений найближчим оточенням, може здатися закритим і не готовим іти на контакт. Водночас у професійних соцмережах вважається моветоном надсилати запит на дружбу тим, з ким не знайомі особисто.

Крок 4. Спілкуйтесь у професійних співтовариствах

Спільноти, до яких належить користувач, завжди відображають його інтереси. Це можуть бути співтовариства за захопленнями (спорт, історія, рукоділля) або професійні спільноти. Об'єднання за назвою «клуб любителів поспати» або «найлінивіші люди в світі» не з найкращого боку характеризують пошукача. Зосередьте увагу на профільних спільнотах: спілкуйтеся з колегами, діліться новинами ринку, обговорюйте питання про вашу сферу діяльності. Репости таких спільнот покажуть рекрутеру, що ви залучені до «професійної тусовки» і хочете розвиватися як спеціаліст.

Крок 5. Оперативно поновлюйте інформацію про себе

Будьте активними і не забувайте оновлювати актуальну інформацію про себе. Акаунт у соцмережі є чудовим майданчиком для самопрезентації в неформальній обстановці. У відповідних розділах зазначте освіту, попереднє місце роботи, контакти. Ці дані не повинні суперечити тому, що написано в резюме. Чим більше потрібної інформації буде доступно рекрутеру, тим більше шансів для подальшої освіти. Не перестарайтеся. Компаніям не потрібен співробітник, який днями «висить» у соцмережах.

Досвідчений рекрутер не буде ухвалювати рішення, спираючись лише на інформацію із соцмереж. Проте якщо він матиме доступ до акаунту, то зможе ще раз переконатися, що компанія і співробітник на сто відсотків підходять один одному ***(Більшість роботодавців, перш ніж запропонувати роботу, переглядають профіль працівника в соцмережах // Львівський портал (http://portal.lviv.ua/news/2015/10/01/bilshist-robotodavtsiv-persh-nizh-***

***zaproponuvati-robotu-pereglyadayut-profil-pratsivnika-v-sotsmerezhah*). – 2015. – 1.10).**

***

В соцсетях распространяется призыв к иностранцам покупать украинское

На этот раз пользователей всемирной паутины просят делиться информацией об украинских товарах, которые можно приобрести за рубежом, популяризируя отечественную продукцию среди иностранцев. Как говорят волонтеры страницы In Ukraine, инициаторы кампании, несмотря на то что экономическая часть соглашения об ассоциации с ЕС была подписана еще в прошлом году, резкого роста украинского экспорта не произошло. А дипломатические представительства, которые призваны способствовать нахождению иностранных партнеров и рынков сбыта, также не всегда идут навстречу украинским производителям. Однако люди в сети сразу откликнулись на призыв.

«Присылают фото из разных мест: наши товары есть и в США, и в Европе, и даже в Иордании… Чаще всего – это конфеты и украинское пиво», – комментируют активисты и добавляют: «Мы хотим, чтобы украинские товары стали узнаваемыми среди покупателей на Западе. И Facebook здесь помогает гораздо больше, чем государственные институты».

Призыв распространять украинские продукты за рубежом подхватили не только пользователи, но и чиновники. Министр аграрной политики и продовольствия А. Павленко дал старт флешмоба #FoodUA в Twitter, и за сутки сеть заполонили фото украинских продуктов из Америки, Китая, Азии и Европы. По наблюдению волонтеров, иностранцы ценят украинские продукты за вкус и натуральные составляющие и поддержали бы украинских экспортеров с радостью, но пока найти эти товары не так легко ***(В соцсетях распространяется призыв к иностранцам покупать украинское // Marketing Media Review (http://mmr.ua/show/v_sotssetyah_rasprostranyaetsya_prizyv_k_inostrantsam_pokupaty_ukrainskoe). – 2015. – 1.10).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Учёные психометрического центра Кембриджского университета разработали алгоритм, который определяет черты характера человека по его лайкам в Facebook. По словам многих пользователей, проверивших работу алгоритма, он работает чересчур точно.

Мы всё ближе подбираемся к тому моменту, когда наши предпочтения в сети будут лёгким способом определить, каковы мы на самом деле. И не последнюю роль в этом сыграет технология, представленная психометрическим центром Кембриджского университета.

Технология называется Apply Magic Sauce и позволяет составить психологический, политический и сексуальный портрет пользователя на основании лайков, поставленных в Facebook.

Помимо логичных следствий вроде возраста, пола, образования, любимых фильмов и музыки, алгоритм умеет «додумывать» более глубокие характеристики. К примеру, предположить, насколько пользователь открыт, самокритичен, уверен в себе. Любит ли он соревноваться или предпочитает работать в команде. Импульсивен или организован. Консервативен и традиционен или либерален и креативен.

Для работы алгоритму нужно внушительное количество лайков. Если лайков недостаточно, появляется надпись: «Мы не можем сгенерировать предположение. Количество лайков недостаточно, а мы не верим в работу наугад» ***(Что лайки в Facebook могут рассказать о вашем характере // InternetUA (http://internetua.com/cto-laiki-v-Facebook-mogut-rasskazat-o-vashem-haraktere). – 2015. – 21.09).***

***

Группа политологов и специалистов по медиа из Делаварского университета обнаружила, что позитивные комментарии в постах Facebook о политиках улучшают мнение избирателей о них. В то же время негативные комментарии имеют прямо противоположный эффект. Работа опубликована в The Journal of Experimental Political Science.

Исследователи создали на Facebook страницу фиктивного политика – кандидата на выборах регионального уровня. В описании жизни, деятельности и достижений вымышленного политического деятеля использовалась исключительно общая информация, без каких-либо эмоционально окрашенных или оценочных суждений.

Далее ученые отобрали группу респондентов в количестве 183 человек. Половине из них демонстрировалась страничка кандидата с двумя критическими комментариями, а другой половине – с двумя хвалебными. После чего испытуемые должны были высказать свои впечатления о политике и дать общую его оценку.

Подавляющее большинство респондентов, посмотревших страничку с положительными комментариями, оценило политика в позитивном ключе и выразило готовность поддержать его на выборах. Те же, кто видел отрицательные комментарии, наоборот, в большинстве своем оценивали кандидата негативно и отказывали в поддержке. «Ответы» фиктивного политика на комментарии не оказывали какого-либо значимого эффекта на восприятие его избирателями.

На основании данных эксперимента ученые пришли к двум выводам. Во-первых, потенциальные избиратели в социальных сетях больше доверяют комментариям «простых людей», нежели репликам самих кандидатов или стоящих за ними специалистов по PR. А, во-вторых, интерактивное взаимодействие между электоратом и политиками в социальных медиа привносит совершенно новое измерение в предвыборную борьбу. Старые каналы коммуникации и методы создания положительного имиджа больше не работают, и ключевую роль в принятии решения избирателями начинает играть коллективное мнение в соцсетях.

Ведущий автор исследования отметил, что, несмотря на простоту эксперимента – это первая подобная работа такого рода. Важно отметить также, что это вообще редкий случай применения экспериментального метода в политических науках ***(Влияние комментариев в Facebook на мнение избирателей впервые доказали экспериментально // InternetUA (http://internetua.com/vliyanie-kommentariev-v-Facebook-na-mnenie-izbiratelei-vpervie-dokazali-eksperimentalno). – 2015. – 29.09).***

***

По результатам нового исследования Кардиффского университета в Уэльсе, каждую неделю одна треть тинейджеров просыпается посреди ночи, чтобы проверить социальные медиа. Исследователи опросили 848 подростков в возрасте от 12 до 15 лет и обнаружили, что 22 % из группы 12–13 лет и 23 % из группы 14–15 лет «почти всегда» просыпаются, чтобы проверить социальные медиа и ответить на сообщения от друзей. 14 % младшей группы и 15 % старшей группы отметили, что с ними случается такое хотя бы раз в неделю. Проверка социальных сетей посреди ночи связывается с более низким уровнем чувством благополучия и счастья.

Другое исследование канадцев, в рамках которого были опрошены 753 студента в Онтарио, обнаружило, что интенсивное потребление социальных медиа связано с депрессией у подростков. Особенно у тех тинейджеров, которые проводят в социальных сетях более двух часов в день – четверть опрошенных говорили о плохом психическом здоровье и расстройстве, которое

включало и мысли о самоубийстве ***(Исследование: соцсети лишают подростков сна // Marketing Media Review (http://mmr.ua/show/issledovanie:_sotsseti_lishayut_podrostkov_sna). – 2015. – 29.09).***

***

В исследовательском подразделении Ericsson (NASDAQ:ERIC) ConsumerLab изучили влияние современных технологий на процесс общения между родителями и детьми.

Возможность быть все время на связи положительно сказывается на уровень счастья в семье.

Для родителей сообщения и голосовые вызовы все еще остаются основными способами коммуникации с детьми в рабочее время. Активное использование новых коммуникационных сервисов детьми, стимулирует родителей осваивать новые приложения. Родители, которые используют новые сервисы, в пять раз чаще связываются между собой и в восемь раз чаще связываются с детьми.

Дети из поколения Z, рожденные после 1994 г., активные пользователи смартфонов и планшетов. Городские дети проводят больше времени в телефоне, чем перед телевизором. По данным Ericsson, поведение поколения Z изменилось – дети отказываются от телевизора в пользу Интернета, доступного на мобильном телефоне. Меняется и поведение родителей. Это подтверждается тем фактом, что 72 % родителей ограничивают ребенку доступ к мобильному телефону в качестве наказания.

Примечательно, что у детей сформировалось четкое разделение приложений на те, которые используются для общения с друзьями и те, которые предпочтительны для связи с родителями. Более того, 68 % опрошенных детей не хотели бы, чтобы их родители стали пользоваться сервисами, которые они используют для общения с друзьями.

«Приложения разрабатываются нами, в том числе, как коммуникационный инструмент для детей и родителей. Работа с приложением – это новый формат взаимодействия между ребенком и взрослым. Поскольку многие дети играют вместе с родителями, важно, чтобы приложения были интересными для любого возраста. Это относится к темам, музыке, дизайну, открытым игровым механикам. Хорошие детские приложения прекрасно чувствуют себя в музейном пространстве и в семейной гостиной», – говорит О. Ставицкий, генеральный директор BUBL, компании-разработчика цифровых развивающих арт-приложений для детей.

Тем не менее, новые коммуникационные сервисы несут новые угрозы, от которых современные родители стараются защитить своих детей с помощью введения ограничений и определенных правил поведения в информационной среде.

«Когда родители принимают решение приобрести ребенку мобильный телефон, в первую очередь их волнуют проблемы безопасности. Единого

решения, обеспечивающего защиту ребенка при использовании подключенных устройств, нет. Мобильные операторы, производители телефонов и разработчики приложений предлагают различные опции, которые позволяли бы оградить ребенка от нежелательного контента, покупок, и даже такие функции, как ограничение использования по времени, а также предоставляли бы возможность обнаружения местонахождения ребенка. Инструментов очень много, но все же основная ответственность за безопасность детей в цифровом пространстве лежит именно на родителях. Детская сфера интересов меняется, и одновременно с этим родителям приходится подстраиваться, чтобы своевременно отслеживать информацию, к которой дети получают доступ с мобильных телефонов», – отмечает Т. Ледовская, руководитель службы аналитики и ConsumerLab Ericsson в регионе Северная Европа и Центральная Азия.

Хотя информационные технологии существенно упростили процесс общения внутри семьи и сделали его постоянным, это не сможет заменить живого общения и результаты исследования подтверждают это. Более 50 % детей, принявших участие в опросе, утверждают, что хотели бы больше общаться с родителями в будние дни.

В исследовании приняло участие больше 1000 семей из США, среди которых 570 детей в возрасте от 12 до 15 лет ***(Ericsson ConsumerLab: Технологии улучшают общение внутри семьи // ITnews (http://itnews.com.ua/news/78454-ericsson-consumerlab-tekhnologii-uluchshayut-obshhenie-vnutri-semi). – 2015. – 29.09).***

***

Фахівці Microsoft Research і лінгвісти з Пенсільванського університету виявили взаємозв'язок між тим, як людина поводиться у Twitter і його рівнем доходу, пише Eurekalert. Детальні результати дослідження опубліковані в журналі PLOS One, пише «Корреспондент» (http://ua.korrespondent.net/lifestyle/3570019-eksperty-Microsoft-poiasnyly-zalezhnist-povedinky-v-merezhi-vid-rivnia-dokhodiv).

З'ясувалося, що найбільш «бідні» в соціальній мережі – це оптимісти. Подібні результати зроблені під час аналізу 10 млн «твіттів» і понад 5000 акаунтів. Основою для дослідження стали використовувані користувачами слова і вирази, згруповані за класами.

Примітно, що користувачі з більш високим рівнем доходу не тільки менш оптимістичні, але і частіше виражають через Twitter такі емоції, як страх і гнів.

Також з'ясувалося, що в лексиці менш заможних людей у мікроблозі частіше присутні непристойні слова й вирази.

«Люди з невеликим заробітком використовують Twitter для спілкування один з одним, у той час як більш забезпечені люди постять у стрічку новини і використовують мікроблоги частіше в професійних, ніж в особистих цілях», – пояснив один з ініціаторів дослідження Н. Алітрас.

На думку вчених, зміст тексту в мікроблозі може розповісти експертам практично все – починаючи від належності до гендерних і вікових категорій і закінчуючи соціальним статусом ***(Експерти Microsoft пояснили залежність поведінки в Мережі від рівня доходів // Корреспондент.net (http://ua.korrespondent.net/lifestyle/3570019-eksperty-Microsoft-poiasnyly-zalezhnist-povedinky-v-merezhi-vid-rivnia-dokhodiv). – 2015. – 30.09).***

***

В зависимости от того, каким устройством вы пользуетесь при отправке сообщений в соцсети, можно сказать, какую эмоциональную окраску они будут иметь.

Например, любители отправлять твиты с мобильника пишут в эгоцентричном стиле с преобладанием негативных оттенков. Отправленные со смартфонов твиты на 25 % чаще несут негативный контекст, установили ученые из Университета Лондона.

По данным ученых, большая часть сообщений в Twitter начинается со слов «я», «у меня», «мой», «моя» и др. Они объясняют это тем, что социальные сети являются прекрасным местом для нарциссов, которые часто меняют аватарки, выкладывают снимки с отдыха и любуются результатами труда. А смартфоны еще и усиливают эти возможности.

Ученые также выяснили, что твиты были наиболее негативными и эгоцентричным в определенные дни недели и определенное время дня. Наибольшее количество негатива появляется рано утром и поздно вечером. А в воскресное утро плохие сообщения почти никто не пишет ***(Любители сидеть в соцсетях с телефона – эгоисты // InternetUA (http://internetua.com/luabiteli-sidet-v-socsetyah-s-telefona---egoisti). – 2015. – 4.10).***

***

Вихваляючись у соціальних мережах, ви можете справити враження на ваших знайомих, однак це може переписати ваші спогади, замінивши «красивою картинкою» те, що було насправді.

Про це свідчать результати дослідження, проведеного одним із засновників Товариства нейропсихоаналізу Р. Шеррі.

За словами Р. Шеррі, зрозуміло, що люди хочуть справити хороше враження, отримати підтримку колег та знайомих. Однак таке устремління має негативну сторону – той, хто вихваляється, може забути свій реальний життєвий досвід, або те, що він переживав, говорить психолог.

У цьому випадку, «ми губимо себе справжніх або заперечуємо те, що було», говорить Р. Шеррі. За словами психолога, таким чином соціальні мережі можуть розірвати узгодженість між реальним життям людини та її спогадами.

Дослідження Р. Шеррі показало, що 10 % опитаних спотворили свої спогади після того, як написали про певні події. 16 % із тих, хто таким чином «переписав собі пам’ять» – молоді люди у віці 18–24 років. Спотворювали,

переважно, описи того, як вони відпочивали, а також речі, пов'язані з кар'єрою та стосунками. На це їх підштовхувало бажання виглядати цікавішими.

Зміни пам'яті стосувалися записів у соціальних мережах, де люди мають акаунти для спілкування з друзями, зокрема Facebook та Twitter. У той же час дослідження показало, що втрачені спогади за бажання можна повернути ***(Соцмережі переписують людську пам'ять // Велика Епоха (http://www.epochtimes.com.ua/novyny-nauky/socmerezhi-perepysuyut-lyudsku-pamyat-119006). – 2015. – 3.10).***

***

Общение с друзьями из других городов и стран с помощью социальных сетей нередко помогает подросткам избавиться от чувства одиночества и собственной ненужности, так свойственного этому возрасту. Об опасности злоупотребления школьниками общением в социальных сетях предупреждают родителей и педагогов шотландские ученые из университета города Глазго, пишет «Сегодня» (http://www.segodnya.ua/life/health/zloupotreblenie-obshcheniem-v-socialnyh-setyah-vredno-dlya-podrostkov-648742.html).

Возникающая потребность как можно дольше находиться в режиме онлайн, постоянно читать комментарии на свои сообщения и отвечать на них, заниматься пересылкой «твитов» и тому подобное может оказаться слишком большой нагрузкой для нервной системы подростка.

Ученые опросили почти 470 подростков, учащихся старших классов, о том, сколько времени те проводят за общением в социальных сетях каждый день.

Исследователей также интересовало время суток, когда продолжительность такого общения была максимальной.

Юные участники исследования также отвечали на вопросы специальной анкеты, что позволяло выявить у них наличие проблем со сном, и подвергались специальному тестированию для выявления психологических проблем.

Ученые из Глазго обнаружили, что в подавляющем большинстве случаев участники исследования посвящали наиболее интенсивному общению в социальных сетях вечернее время и начало ночи.

У тех из них, кто просиживал за компьютером допоздна и посвящал социальным сетям более двух часов в день, очень часто имелись проблемы с качеством сна и наблюдались признаки повышенной тревожности, а иногда и депрессии ***(Злоупотребление общением в социальных сетях вредно для подростков // Сегодня.ua (http://www.segodnya.ua/life/health/zloupotreblenie-obshcheniem-v-socialnyh-setyah-vredno-dlya-podrostkov-648742.html). – 2015. – 2.10).***

***

Американські експерти з'ясували, що близько 92 % закоханих підлітків використовують для спілкування зі своїми другими половинками соцмережі.

Фахівці провели опитування серед кількох тисяч американських підлітків у віці від 13 до 17 років.

На основі результатів проведеного опитування вдалося дізнатися, що 35 % респондентів вирішили повідомити, що в цей час перебувають у деяких романтичних стосунках.

При цьому приблизно половина з опитаних підлітків погодилася з тим, що додавання людини в список своїх друзів на основі соціальних мереж можна вважати одним з видів флірту.

До того ж різні «лайки» або ж коментарі у 47 % опитаних міцно асоціюються з виразом знака уваги в складному процесі залицяння ***(Вчені: 92 % закоханих підлітків спілкуються між собою в соціальних мережах // NEWS.COM.UA (http://news.com.ua/zdorovja/zakohani_pidlitku_spilkyjytsja_cherez_socmerezi_03602.html). – 2015. – 4.10).***

Маніпулятивні технології

Негативна інформація, яка містить ознаки «чорного піару», поширюється через соціальну мережу Facebook про потенційних кандидатів на посаду міського голови Ужгорода. Таку тенденцію спостерігачі ОПОРИ фіксують у перші тижні початку виборчої кампанії.

Зокрема, 21 вересня на Facebook-сторінці ужгородського нічного клубу Eila White Club з'явився запис, у якому потенційний кандидат у міські голови Ужгорода М. Качур звинувачується в неефективній роботі керованого ним підприємства ВАТ «Ужгородський Турбогаз».

Зокрема, на сторінці клубу без доказів озвучується така інформація: «Согласившись подписать убийственный для завода кредит в 25 млн дол., которые в последствии выкачали з бугор, М. Качур с рабочего пилорамы "Турбогаза" сел в кресло директора!! В интересах олигархов, которые за бесценок, благодаря разным махинациям, практически отсудили "Турбогаз" от Держмайна, М. Качур продолжает гробить предприятие!». Дане повідомлення станом на 22 вересня отримало у Facebook 23 поширення.

Варто зазначити, що всі інші записи на сторінці стосуються тематики дозвілля на нічних дискотеках, подано анонси проведення таких дискотек.

Спостерігач ОПОРИ зателефонував до нічного клубу за вказаним на сторінці номером – 066 033 00 32. Там відповіли, що наповненням Facebook-сторінки клубу займається арт-директор і пообіцяли передати йому контакти спостерігача ОПОРИ. Утім, протягом доби на зв'язок ніхто не вийшов, а наступного дня телефон закладу взагалі перестав відповідати.

Запис на сторінці нічного клубу містить і «прикріплену» статтю місцевого сайту. У матеріалі авторства «оглядача Т. Т. Макарова» інформація про потенційного кандидата в міські голови також подається з негативним

вмістом, зокрема озвучується посил, що нібито М. Качур неефективно керує ужгородським підприємством. «А что сделано для возрождения завода? Хоть какой-либо план действий в этом направлении имеется? Об этом М. Качур и его команда умалчивают. Как же тогда они собираются возрождать экономику Ужгорода в целом? Об этом тоже – молчок. Мол, “я иду” – а там видно будет…».

Спостерігач ОПОРИ звернувся до редактора сайту В. Кривошапка з питанням, чи буде надано потенційному кандидату М. Качуру право на відповідь, якщо він звернеться з такою пропозицією. На це редактор прямо не відповів. З його слів, подані в матеріалі факти відповідають дійсності: «А що там коментувати? Білборди – реально стоять. Біографія М. Качура (в т.ч. по списках якої партії він обирався) – на офіційній сторінці обласної ради (розділ Депутати). “Турбогаз” у минулому – Вікіпедія. “Турбогаз” сьогодні – розсилка прес-служби ОДА за фактом відвідання цього підприємства тодішнім головою ОДА В. Губалем (від 10 липня ц.р.)».

12 вересня на Facebook-спільноті «Місто Ужгород», де подається суто позитивна, іміджева інформація про потенційного кандидата в міські голови Ужгорода В. Щадея, була поширена негативна інформація про іншого потенційного кандидата в міські голови – голови Закарпатської облради В. Чубірка. Тут наведена цитата В. Щадея, де він обвинувачує В. Чубірка у спробі забрати від мешканців їх гуртожиток: «Вже 4 роки допомагаємо мешканцям захищати їхнє житло від зазіхань голови обласної ради В. Чубірка. Людям важко протистояти в судах грошовим мішкам, які хотіли привласнити кімнати мешканців. Рейдери навіть встигли відібрати в людей частину приміщень. Зрештою, в цій боротьбі нарешті поставлено крапку – жителі гуртожитку таки приватизують своє житло».

13 вересня В. Чубірко на своїй сторінці у Facebook написав відгук на публікацію, де про В. Щадея зазначив – «людина, в якої за спиною лише досвід відкатів, хабарів та проплачених голосувань за регіоналів у міській раді, вирішила по другому колу використати мешканців гуртожитку, очорнити мене і заробити собі якихось балів напередодні виборів».

ОПОРА закликає усіх учасників виборчого процесу, а також працівників ЗМІ дотримуватися вимог ч. 5 ст. 60 Закону України «Про місцеві вибори», згідно з якою забороняється розповсюдження завідомо недостовірних відомостей про кандидата, політичну партію або її місцеву організацію – суб’єкта виборчого процесу, а також поширення завідомо недостовірної інформації про підтримку певного кандидата або місцевої організації партії іншими кандидатами, політичними партіями або їх місцевими організаціями.

Згідно з вимогами ч. 2 ст. 52 цього ж Закону, інформаційні агентства та засоби масової інформації поширюють повідомлення про перебіг виборчого процесу, події, пов’язані з виборами, базуючись на засадах достовірності, повноти й точності, об’єктивності інформації та її неупередженого подання. ***(В Ужгороді через соцмережу нічний клуб розповсюджує негативну інформацію про кандидата, інші потенційні з’ясовують стосунки //***

Закарпаття онлайн (http://zakarpattya.net.ua/News/145467-V-Uzhhorodi-cherez-sotsmerezhu-nichnyi-klub-rozpovsiudzhuie-nehatyvnu-informatsiiu-pro-kandydata-inshi-potentsiini-ziasovuiut-stosunky). – 2015. – 23.09).

***

В пику так называемым «кремлевским троллям», которые активно проявляют себя в Интернете, в Литве появились «эльфы» – активные, образованные люди, которые жертвуют своим досугом ради борьбы с «фабрикой троллей», нанятых путинским режимом для распространения в киберпространстве лжи и клеветы.

Литовцы решили назвать борцов с интернет-троллями «эльфами». Наверное, в первый раз на официальном международном мероприятии это название прозвучало в конце августа в столице Латвии на конференции, организованной Центром компетенции стратегической коммуникации НАТО «Рижский диалог стратегической коммуникации: важность понимания». Участница конференции американка доктор Р. Гулсби, отвечая на вопрос, что делать с кремлевскими троллями, которые уже активно проявляют себя не только в интернет-пространстве стран Балтии, но и в интернет-пространстве других западных стран, посоветовала бороться с ними, как это делают литовские эльфы.

Аналитик Литовской армии, наблюдающий за интернет-пространством, сказал, что первая массовая организованная, активная и агрессивная атака московских троллей против Литвы в интернет-пространстве была зафиксирована еще в 2010 г. – в комментариях к статье «Особо секретную аппаратуру КГБ для шифровки ЦРУ получила от литовцев» на портале DELFI.

Хотя статья была опубликована в полночь, тролли напали сразу же, не дожидаясь утра – посыпались комментарии, очерняющие Литву и Запад, прославляющие СССР и Россию и т. д.

А активную, но не такую организованную деятельность троллей военные Литвы, следящие за интернет-пространством, заметили еще в 2007 г. Во-первых, по словам аналитиков, они стали проявлять себя на самом популярном литовском информационном портале DELFI, через некоторое время тролли стали появляться и на других литовских порталах.

Позже в СМИ стала попадать информация о так называемых «фабриках троллей» и «интернет-бригадах» в России (такие бригады организуют и в соседних странах, где проживает много русскоязычных жителей, например, такую бригаду разоблачили в Украине).

Тролли за деньги целыми днями пишут комментарии на информационных порталах, в социальных сетях и т. д. Их называли по-разному (например, «30-рублевая армия»), но в конце концов их стали называть «кремлевскими троллями».

В Литве деятельность троллей давно заметили не только аналитики, но и общество, СМИ, политики. А Запад проснулся совсем недавно, после

оккупации Крыма, хотя московские тролли давно пишут комментарии на английском, немецком, французском языках.

«Значение Интернета в последние несколько лет значительно увеличилось. Значимее стал и троллинг», – сказал аналитик.

Кстати, тролли не ограничиваются одними комментариями, стараясь оказать влияние на общество, они используют и другие способы.

Один из самых популярных – визуализация. Например, сравнивают Японию с Литвой: число чиновников – в Японии намного больше жителей, а чиновников намного меньше. Сначала такая визуализация применялась в отношении Украины, затем – стран Балтии.

Правда, в этих визуализациях – только численность населения, численность чиновников не имеет ничего общего с реальностью, но много не думающий человек, увидев такую картинку в Интернете, запоминает ее и начинает возмущаться.

«В демократическом государстве фабрики троллей, как в России, невозможны. Эльфы – общественная инициатива, родившаяся из желания защищать свое мировоззрение», – сказал аналитик армии. Некоторых работающих в Литве эльфов военные знают, но далеко не всех: в последнее время это движение очень распространилось не только в Литве, но и в Латвии, Эстонии, Украине, к армии эльфов присоединяются поляки, финны.

«Путь эльфов – высказывание правды. Ее столько, что не нужно никаких искажений и лжи, – сказал военный, наблюдающий за информационным пространством. – Они берут информацию, которую распространяют тролли и представляют правду на подвергшуюся троллингу тему в комментариях, делают визуализации, которые распространяют в социальных сетях и т. д.». Борющиеся с троллями литовцы в социальных сетях создают отдельные темы («По следам красного медвежонка», «Распознай недружественную пропаганду» и др.).

Эльфы в Интернете отслеживают некоторых троллей, находят их страницы в соцсетях. Чаще всего эти страницы полны ностальгией по советскому времени, «украшены» советской символикой или символикой украинских сепаратистов. На такие страницы эльфы помещают информацию, визуализации (например, тролль на своей странице пишет, что в советское время жизнь была прекрасна, а эльфы «развешивают» фотографии пустых прилавков в советских магазинах и т. п.).

Аналитик сказал, что эльфов стало больше, поскольку «когда видишь поток лжи, идущий с Востока, появляется естественное желание дать отпор» ***(«Эльфы» восстали против кремлевских «троллей» // Newsland (http://newsland.com/news/detail/id/1611386/). – 2015. – 23.09).***

***

Радикальные идеи социальных сетей

Социальные сети сыграли едва ли не ключевую роль в распространении «Арабской весны». Интернет, как политический и даже геополитический

инструмент, доказал свою состоятельность, привлекая молодых и активных граждан – самую значимую аудиторию интернет-пространства. Эффективным каналом распространения нужной информации пользуются все, кто имеет выход в сеть, в том числе и радикально настроенные группировки исламского мира.

Сцены казней и насилия с эффектом массового вируса разлетающиеся по сети; радикальные идеи, являющие собой некий симбиоз политической идеологии и догматов ислама, интерпретированные на разных языках мира; собственное медиа-агентство и тонны качественной полиграфии, несущей разрушительный заряд всемирного халифата – вот что представляет сегодня «рекламная» кампания радикального исламизма в лице одной из главных мировых угроз современности – Исламского Государства. В настоящее время социальные интернет-платформы продолжают помогать пополнять ряды ИГ среди европейцев и не только. Подросток способен принимать на веру многое, что прочитает в социальных сетях, причем степень эффективности зачастую – в разы выше, чем сила убеждения на тех же телевизионных каналах. В той же зоне риска находится и более взрослый сегмент не определившейся во взглядах молодежи. В этом случае интерес подпитывается сценами расстрелов и казней и пронизан новыми, в том числе, и радикальными идеями.

Причем для начала достаточно не только, чтобы человек проникся идеями халифата, а просто начал получать удовольствие от контента: будь то насилие, жажда наживы, ироничные демотиваторы или экстремистские призывы в «модной обертке» мемов. Тем самым террористические организации уже давно не ориентируются лишь на заповеди Корана, активно пользуясь плодами научно-технической революции. «Радикальные котики» в Twitter, аккаунты в Instagram и группы и аккаунты в Facebook. Только если котиков после общественного резонанса закрыли, то другие площадки продолжают функционировать.

ИГ в социальных сетях (https://www.facebook.com/diduknow4)

Эта площадка, на которой ИГИЛ позиционируется как полноправное государство, идейная линия направлена в сторону радикального исламизма. Количество подписчиков – 5173.

Здесь есть призывы к объединению мусульман, в названии профиля есть словосочетание «Исламское Государство» (الدّولة الإسلاميّة). Несмотря на ироничную подачу контента, также прослеживается идейная линия радикального ислама.

Теперь к Twitter. Перейдя по этой ссылке (https://twitter.com/ahmadkhaled101), например, вы наткнетесь на твиты, призывающие бороться за идеи провозглашенного халифата.

В российском интернет-сегменте активную пропаганду ИГ также нельзя не заметить. Но вернемся к зарубежным сайтам. Вот (http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq) целая книга, которая содержит лекции на религиозные темы и новости о деятельности ИГ. И ее запросто можно скачать в сети.

Итак, это лишь малая часть примеров радикальной пропаганды в сети, и список можно продолжать долго.

Финансирование и привлечение специалистов в ИГИЛ

Если раньше пропаганда радикального ислама ограничивалась призывами на улице, личными дневниками террористов или книжками, то теперь ИГИЛ стал использовать современные методы. Законы маркетинга, рекламы и PR, а не законы Корана. Четкая, непрерывная и последовательная схема коммуникации в Интернете, прессе и СМИ. Силами радикалов, которые после боев садятся за компьютер и начинают спамить в Интернете, вопрос эффективной пропаганды не решить. Это вопрос больших денег и целой бригады специалистов. Которая у Исламского государства… имеется. Начнем с финансов. Такие масштабы пропаганды возможны лишь при наличии немалого бюджета. С этим у ИГИЛ проблем нет. Грабежи и вымогательства, большие куши от продажи краденых реликвий на черных рынках, спонсорские вливания, нелегальная продажа нефти, деньги за выкуп заложников – все это в комплексе сформировало бюджет исламистов, который на сегодняшний день оценивается примерно в два миллиарда долларов.

«Радикальный медиахолдинг»

Еще в 2006 г. ИГ совместно с «Аль Каидой» создают целое медиа-агентство «Аль-Фуркан». За основу деятельности организации взяты передовые мировые технологии. Единственное отличие – это бренд, бренд радикального исламизма, идеи исключительно экстремистского характера. Фильмы с жестокими убийствами, идеологические брошюры, активная работа в социальных сетях.

С каждым годом данное медиа-агентство набирает такие обороты, что позавидовать может любой холдинг. В 2013 г. у ИГИЛ даже появляется своя звукозаписывающая студия! Интересно, сколько видеоклипов и фотоотчетов у них выходит в день? Так вот, это три клипа на разных языках и четыре фотоотчета, разлетающиеся ежедневно посредством сетей Интернет и СМИ по всему миру!

Радикальные идеи с молниеносной скоростью способны добраться до любой точки планеты благодаря мировой сети. Тем самым, они быстрыми темпами интегрируются в современный мир, получив возможность ворваться в каждый дом. Эта машина пропаганды обладает немалой мощью, игнорируя ее, мировое сообщество рискует ежедневно терять законопослушных граждан, приобретая все больше врагов, готовых разрушить все существующие устои ***(Радикальные идеи социальных сетей // Newsland (http://newsland.com/news/detail/id/1611300/). – 2015. – 23.09).***

***

Флешмоб «Остров 90-х», запущенный российским изданием Colta.ru, вышел за рамки РФ и захлестнул Украину, в том числе представителей IT-индустрии. Ленты пользователей наводнили ностальгические фото из 1990-х годов. Но если копнуть глубже, оказывается, что на самом деле «флешмоб из

90-х» – пиар-акция, поддерживаемая российским провластным фондом «Ельцин Центр», пишет AIN.UA (http://ain.ua/2015/09/21/604795).

Первыми публиковать фотографии из 90-х принялись российские журналисты и блогеры, в частности О. Кашин. Идею быстро подхватили представители российского медиа-сообщества и ностальгические фото захлестнули российский сегмент Facebook.

Позже флешмоб вышел за рамки специализированных сообществ и распространился на всех. Многие представители украинского IT-сообщества тоже продемонстрировали свои фото из 90-х годов прошлого столетия.

Не все поддержали идею. Д. Довгополый опубликовал пост в Facebook с критикой флешмоба. По его словам, 90-е – это время, в которое лучше не возвращаться. «В эти годы было слишком много мерзкого – нищета, попытки совка кровавыми руками зацепиться за страну, формирование олигархов, бандитизм, убийства на каждом шагу», – пояснил Д. Довгополый.

Изначально, флешмоб был запущен в поддержку фестиваля «Остров 90-х», который прошел в Москве 20 сентября. Информационными партнерами фестиваля выступили Colta.ru, образовательный проект «Твоя история» и Фонд «Ельцин Центр».

Основной целью флешмоба сами организаторы, помимо рекламы фестиваля, называют переосмысление 90-х, подталкивание к осознанию того, что эти времена были не так плохи, как запечатлелись в памяти у населения. «Приглашаем вместе с нами исследовать этот мир, потому что уверены: это не прошлое. Оно не исчерпано. Там, на острове, не только корни проклятых вопросов, встающих перед нами сегодня, но и ключи ко многим ответам. А еще – источники вдохновения и азарта, которых сейчас так не хватает», – говорится на сайте «Ельцин Центр».

«Ельцин Центр» – некоммерческая организация имени первого президента России, которая ставит себе за цель «сохранение, изучение и осмысление исторического наследия Б. Ельцина в контексте политических и социальных событий 90-х». В попечительский совет центра входят первые лица российского политикума, в частности руководитель Администрации президента РФ С. Иванов, министр обороны РФ С. Шойгу, глава «Роснано» А. Чубайс.

Проект «Остров 90-х» – не первый, целью которого является освежение памяти об этом периоде. Ранее «Ельцин Центр» делал проект «Девяностые. От первого лица» совместно с еще одним либеральным российским СМИ – телеканалом «Дождь».

Пользователи Facebook, не поддержавшие флешмоб, отмечают, что возрождение ностальгии по 90-м годам является одной из линий кремлевской информационной политики. «Соседняя страна туда [в лихие 90-е] идет бодрым шагом, и этот флешмоб направлен на то, чтобы этот возврат прошел через ностальгию не так тяжело, как может», – говорит на своей странице Д. Довгополый.

Российский журналист К. Баранов также считает, что флешмоб направлен на обеление российской власти за счет ностальгических чувств пользователей. «Нам хотят рассказать, что в 90-х было светло и красочно, что не надо мазать черной краской, что это было время свободы и возможностей и те, кто не смог адаптироваться, сами виноваты», – комментирует К. Баранов ***(Бондаренко А. Новый флешмоб в уанете: ностальгия по 90-м оказалась кампанией российского провластного фонда // AIN.UA (http://ain.ua/2015/09/21/604795). – 2015. – 21.09).***

Зарубіжні спецслужби і технології «соціального контролю»

Генеральный директор британской контрразведки Э. Паркер считает, что усовершенствование технологий позволяет террористам взаимодействовать «вне пределов досягаемости властей». Об этом он заявил в интервью журналистам BBC.

Как отметил Э. Паркер, правоохранителям становится все сложнее получать информацию из сети, подчеркнув, что интернет-провайдеры должны проявлять «этическую ответственность» и информировать соответствующие спецслужбы о потенциальных угрозах. Однако MI5 не намерена «подглядывать» в частную жизнь пользователей, добавил глава ведомства.

В настоящее время британское правительство готовит ряд законов, касающихся электронного наблюдения, но окончательное решение о том, какие пункты будут в них включены, останется за парламентом.

По словам Э. Паркера, шифрование данных в Интернете привело к возникновению ситуации, когда ни полиция, ни разведслужбы «больше не могут получить доступ к коммуникациям людей, подозреваемых в терроризме, на основании соответствующего законного ордера».

Шеф контрразведки также добавил, что в настоящее время с точки зрения безопасности терроризм является наиболее серьезной угрозой для Великобритании ***(Гендиректор MI5: Шифрование online-данных усложняет борьбу с тероризмом // InternetUA (http://internetua.com/qendirektor-MI5--shifrovanie-online-dannih-uslojnyaet-borbu-s-terrorizmom). – 2015. – 20.09).***

***

Роскомнадзор вніс у реєстр заборонених сайтів п’ять спільнот «ВКонтакте». Причиною такого рішення стала пропаганда нетрадиційних сексуальних стосунків серед підлітків.

У прес-службі відомства заявили, що назви груп і контент орієнтовані на цільову групу «діти/підлітки».

Наголошується, що в групах публікували оголошення про знайомства з підлітками з метою нетрадиційних сексуальних стосунків, відверті зображення

нетрадиційних сексуальних стосунків між підлітками і дорослими. Інформація повинна бути видалена із соціальної мережі протягом трьох днів.

Прес-секретар Роскомнагляду В. Ампелонський розповів, що йдеться в тому числі про групу «Діти-404» ***(В Росії заборонили п'ять спільнот «ВКонтакте» через гей-пропаганду // InternetUA (http://internetua.com/v-ros---zaboronili-p-yat-sp-lnot--vkontakte--cserez-gei-propagandu). – 2015. – 21.09).***

***

В Бельгии начался судебный процесс по делу Facebook – соцсеть обвиняется в нарушении ряда европейских законов о защите частной жизни, обрабатывании и использовании данных пользователей без их согласия. Бельгийская Комиссия по защите данных призывает судью «не бояться» Facebook, так как американская компания должна изменить политику конфиденциальности для того, чтобы соответствовать местному законодательству. Об этом сообщает издание Bloomberg.

Бельгийская Комиссия по защите данных является одним из нескольких европейских регуляторов, у которых возникли вопросы по поводу обработки пользовательских данных компанией Facebook. Двадцать восемь организаций, занимающихся вопросами конфиденциальности в ЕС, взаимодействуют между собой для выявления факта нарушения соцсетью европейского законодательства в области неприкосновенности частной жизни. Нидерландский регулятор был первым, кого насторожила новость о том, что Facebook с января 2015 г. меняет политику пользовательского соглашения.

«Не будьте запуганными Facebook», – призвал общественность представитель интересов Комиссии Ф. Дебюссер в бельгийском суде на слушаниях в Брюсселе 21 сентября. «Руководство Facebook будет утверждать, что наши требования не могут быть выполнены только в Бельгии. Требование прекрасно могут исполнятся в нашей стране», – заявил Ф. Дебюссер.

«Вторжение в личную жизнь пользователей без их ведома является крайним неуважением со стороны Facebook, которое нужно прекратить», – отметил президент Комиссии В. Дебекеларе. Бельгийские власти грозят американской компании ежедневным штрафом в 250 тыс. евро до тех пор, пока выявленные нарушения не будут устранены.

По словам представителей Facebook, компания должна следовать европейскому законодательству в области неприкосновенности частной жизни только в Ирландии, где расположена штаб-квартира Facebook. «Как соцсеть может следовать бельгийским законам, если 900 сотрудников компании занимаются сбором данных в Ирландии», – возмутился адвокат, защищающий права американской компании, П. Лефевр.

«Когда общественность узнала, что АНБ США шпионит за гражданами, все были крайне возмущены. Так вот Facebook занимается чем-то подобным», – заявляет Ф. Дебюссер.

Ранее бельгийские регуляторы обвинили Facebook в шпионаже, который может осуществляться посредством использования социальных плагинов,

главным образом, за счет кнопок «нравится», «поделиться» и комментариев на других интернет-сайтах. В свою очередь, П. Лефевр отметил, что Facebook использует cookie-файлы для того, чтобы определять вредоносную активность в сети. «Без этого Бельгия давно превратилась бы в площадку для кибертерроризма, чего так пытается избежать Комиссия», – заявил П. Лефевр ***(Бельгийские регуляторы призывают суд «не бояться» Facebook // InternetUA (http://internetua.com/belgiiskie-regulyatori-prizivauat-sud--ne-boyatsya--Facebook). – 2015. – 22.09).***

***

Сотрудники Службы безопасности Украины задержали по подозрению в антиукраинской пропаганде и поддержке сепаратистов в социальной сети «ВКонтакте» жительницу Запорожья.

Как передает Цензор.НЕТ, об этом «Українським Новинам» сообщил представитель пресс-службы УСБУ в области.

По данным ведомства, в апреле женщина познакомилась в социальной сети с гражданином России по имени Игорь, который предложил ей за деньги «вести» группу в соцсети, размещать антиукраинские материалы, материалы в поддержку ДНР и ЛНР, а также инструкции по уклонению от мобилизации. Материалы для размещения он присылал женщине личными сообщениями. Также она занималась модерированием группы и удаляла все проукраинские комментарии и публикации с последующим блокированием пользователя.

Подозреваемая задержана, планируется начать уголовного производства по ст. 109 (действия, направленные на насильственное изменение конституционного строя), ст. 110 (посягательство на территориальную целостность Украины) Уголовного кодекса ***(СБУ задержала подозреваемую в антиукраинской пропаганде и поддержке сепаратистов жительницу Запорожья // InternetUA (http://internetua.com/sbu-zaderjala-podozrevaemuua-v-antiukrainskoi-propagande-i-podderjke-separatistov-jitelnicu-zaporojya). – 2015. – 22.09).***

***

Безопасность данных граждан ЕС на американских серверах может находиться под угрозой, утверждает европейский суд. Более 4 тыс. американских компаний, включая Facebook, Apple и Amazon, хранят данные европейских пользователей на территории США, чем облегчают их попадание в руки американских спецслужб.

Европейский суд серьезно озаботился вопросом безопасности находящейся в руках американских компаний информации о гражданах Евросоюза.

По словам генерального адвоката И. Бота, личные данные европейцев передаются на серверы в США, но их безопасность и неприкосновенность при этом совершенно не гарантируются. Таким образом, американские компании нарушают законы ЕС.

В ближайшее время соответствующее дело будет рассмотрено группой из 15 судей, которые вынесут окончательное решение до конца года. Если они признают, что данные европейских граждан, имеющиеся в распоряжении компаний из США, действительно находятся под угрозой попадания в руки третьих лиц, то компаниям придется серьезно изменить политику конфиденциальности вплоть до создания дата-центров на территории ЕС.

Судебное разбирательство против целого ряда американских компаний еще несколько лет назад инициировал австрийский бизнесмен М. Шрамс, который забеспокоился о сохранности личных данных европейцев после разоблачений бывшего контрактника АНБ Э. Сноудена о массовой слежке американских спецслужб. М. Шрамс предположил, что собирающие данные о европейских пользователях американские компании хранят их на серверах в США, а значит, могут беспрепятственно предоставлять информацию спецслужбам.

На американские дата-центры опираются и многие популярные в Европе облачные сервисы, так что потенциально доступный властям США массив данных просто огромен.

Теперь же потенциальное решение европейского суда может обязать фирмы из США «начать инвестировать в создание дата-центров уже в пределах ЕС», заявил М. Шрамс.

Изначально под подозрение австрийца попала социальная сеть Facebook, в распоряжении которой находится информация о более чем 1 млрд пользователей по всему миру. М. Шрамс поспешил обратиться в штаб-квартиру Facebook в Ирландии, однако его первый запрос был отклонен.

Впоследствии представители Facebook заявили, что соцсеть действительно предоставляет данные по запросу властей, однако эти случаи связаны лишь с криминалом. Более того, социальная сеть делает это избирательно, то есть не все запросы властей в адрес Facebook остаются удовлетворены.

В ирландском офисе соцсети также напомнили, что благодаря закону, носящему название Safe Harbor, американские компании могут хранить всю информацию о европейских гражданах за пределами ЕС.

Safe Harbor позволяет зарубежным компаниям хранить информацию о европейских гражданах в пределах другой страны при наличии гарантии адекватной защиты персональных данных.

Однако, по мнению М. Шрамса, по факту Safe Harbor, наоборот, способствует беспрепятственному мониторингу данных со стороны американских властей, поскольку закон гарантирует лишь защиту информации от несанкционированного доступа со стороны злоумышленников. В то же время компании зачастую предоставляют спецслужбам доступ к данным на добровольной основе.

Оказавший поддержку инициативе австрийца И. Бот также признал, что схема, по которой работает Safe Harbor, не предоставляет должных гарантий отсутствия массового доступа к данным граждан ЕС.

Если суд установит необходимость пересмотра Safe Harbor, то меры по ограничению передачи данных коснутся не только интернет-гигантов вроде Facebook, Apple или Google, но также и более мелких фирм. А в случае законодательного постановления о хранении информации о гражданах Евросоюза в европейских дата-центрах многие американские компании понесут значительные убытки или будут вынуждены покинуть важный для них сегмент рынка.

Тем не менее ведущий аналитик Российской ассоциации электронных коммуникаций К. Казарян считает, что никаких радикальных последствий грядущее судебное разбирательство не принесет.

«Несмотря на все заявления генерального адвоката Европейского суда, утвержденные на уровне Евросоюза правила обработки персональных данных пока что не позволяют регуляторам отдельных стран оперативно принимать собственные решения. Мы уже видели это на примере принятия нового регламента ЕС по защите персональных данных в июне 2015 г. Тогда далеко не все страны выступали за возможность уничтожения компаниями личной информации по запросу пользователей. Тем не менее новый регламент был утвержден на общеевропейском уровне», – рассказал эксперт «Газете.Ru».

По словам К. Казаряна, среди требований адвоката Европейского суда пока не прозвучала идея о необходимости полностью отменить действие Safe Harbor, так что в обозримом будущем мы вряд ли увидим какие-либо ограничительные меры в отношении передачи и размещения данных американскими компаниями.

«К тому же принцип Safe Harbor действует в обе стороны, так что любые попытки ограничить американским компаниям передачу персональных данных на серверы в США обернутся симметричным запретом по отношению к европейским компаниям, которые от этого потеряют в разы больше», – напоминает эксперт ***(Google и Facebook угрожают европейцам // InternetUA (http://internetua.com/Google-i-Facebook-ugrojauat-evropeicam). – 2015. – 25.09).***

***

Роскомнадзор по требованию Генпрокуратуры России заблокировал страницу украинского детского патриотического лагеря «Азовец» в социальной сети «ВКонтакте». Прокуроры усмотрели в деятельности сообщества «пропаганду запрещенных экстремистских организаций».

«Материалы сообщества побуждали несовершеннолетних становиться их последователями, а также стимулировали насилие, обосновывали и оправдывали его допустимость», – отмечают в Роскомнадзоре.

В настоящее время страница группы аффилированного с добровольческим полком «Азов» Нацгвардии Украины детского лагеря уже заблокирована на территории России.

Ранее российский детский омбудсмен П. Астахов направил обращение в Следственный комитет России и Комитет по правам ребенка ООН с просьбой проверить деятельность сообщества на экстремизм.

«Азов» был сформирован в Мариуполе в мае 2014 г. Он входит в состав Национальной гвардии Украины. Первоначально он представлял собой батальон, однако в сентябре прошлого года его состав расширили до полка.

Российские СМИ регулярно обвиняют бойцов «Азова» в приверженности крайне правым взглядам ***(В России заблокировали страницу украинского детского лагеря // InternetUA (http://internetua.com/v-rossii-zablokirovali-stranicu-ukrainskogo-detskogo-lagerya). – 2015. – 29.09).***

***

В России суд в Челябинске приговорил блогера и общественного активиста К. Жаринова за репост обращения украинского «Правого сектора» в социальной сети «ВКонтакте» к двум годам лишения свободы условно и сразу же амнистировал. Об этом сообщает krymr.com.

Уголовное дело против К. Жаринова возбуждено по инициативе управления ФСБ России по статье «публичные призывы к осуществлению экстремистской деятельности».

Сам К. Жаринов ранее объяснял, что, как политолог, следит за событиями в мире, в том числе в Украине, рассматривая их с разных позиций. Именно поэтому он сделал репост обращения украинской организации «Правый сектор» в социальной сети.

В нем призывали оказывать сопротивление режиму В. Путина, выходить на улицы, создавать партизанские отряды и не верить пропаганде.

К. Жаринов – член российской партии «Демократический выбор». Он написал несколько книг об истории терроризма ***(В России блогера осудили за репост обращения «Правого сектора» // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44815/118/lang,ru/). – 2015. – 29.09).***

***

Головний прокурор Закарпаття розповів журналістам, що загрозу сепаратизму відомство моніторить і в соцмережах та у ЗМІ.

Під пильною увагою і Facebook, сказав В. Янко.

Висловлювання і заклики в публікаціях і профілях продивляються прокурори і на ті, де міститься потенційна загроза сепаратизму, буде відповідна реакція – обіцяє прокурор Закарпаття.

Щоправда, наразі такого не було, хоч доповідають і кожен день: «На сьогодні не маємо нових кримінальних проваджень з цього приводу. Сподіваюся, що краяни люблять Закарпаття і не будуть породжувати суперечності». Відзначивши це, В. Янко наголосив також: «Кримінальних проваджень щодо сепаратизму в області немає. Були матеріали, але для порушення проваджень їх недостатньо. Профілактичними заходами ці моменти присікаються. На сьогодні загрози немає».

Що ж, схоже, громадським діячам і журналістам варто допомогти прокуратурі з таким спостереженням, адже в мережі досі діють сторінки й

профілі, які провадять активну пропаганду закарпатського сепаратизму й чиї модератори таки заслуговують на увагу СБУ та згаданого відомства ***(Закарпатським користувачам facebook варто бути обережнішими! Якщо вони – сепаратисти // Закарпатський інформаційно-діловий портал (http://uzhgorod.in/ua/novini/2015/sentyabr/zakarpats_kim_koristuvacham_facebook_varto_buti_oberezhnishimi_yakscho_voni_separatisti). – 2015. – 29.09).***

***

На Дніпропетровщині в Жовтих Водах Служба безпеки України затримала місцевого жителя, який вів антиукраїнську пропаганду в соціальних мережах. Про це УНН повідомили в прес-службі СБУ.

Зловмисник активно поширював матеріали, спрямовані на дискредитацію органів державної влади та Збройних сил України, зрив мобілізації, дестабілізацію ситуації в країні та популяризацію терористичних організацій «ДНР/ЛНР».

Також на початку 2015 р. спільник терористів встановив контакт зі спецслужбами Російської Федерації, за вказівкою яких намагався збирати інформацію про кількість військової техніки, що розташована на ремонтних базах у місті, волонтерські центри та добровольців, які беруть участь у військових діях.

Під час обшуку правоохоронці вилучили у зловмисника комп'ютерну техніку з доказами вказаної діяльності.

За вказаним фактом відкрито кримінальне провадження за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України ***(Плавська С. Адміністратора антиукраїнських груп у соцмережах затримали в Жовтих Водах // Українські Національні Новини (http://www.unn.com.ua/uk/news/1505720-administratora-antiukrayinskikh-grup-u-sotsmerezhakh-zatrimali-v-zhovtikh-vodakh). – 2015. – 30.09).***

***

В Казахстане заблокировали видеохостинги Vimeo, Dailymotion и сервис хранения фото Flickr. Часть пользователей жалуется на полную недоступность сайтов, однако некоторые провайдеры не выполняют требования местного аналога Роскомнадзора. Об этом пишет tjournal.ru.

Решение о блокировке Vimeo в Казахстане было принято ещё 7 сентября судом Астаны, однако о его причинах пресс-служба суда сообщила только 25 сентября. По словам её представителей, на видеохостинге и на ряде других сайтов шла «пропаганда идей экстремизма и терроризма».

О каких ещё ресурсах шла речь и какой контент был признан запрещённым, в суде не уточнили. Однако в Комитете связи, информации и информатизации Министерства по инвестициям и развитию Казахстана (местный интернет-регулятор, выполняющий часть схожих с Роскомнадзором функций) пояснили, что речь шла о видеоматериалах Исламского государства.

Если нарушающие местное законодательство видео будут удалены, Vimeo будет разблокирован, пояснили в Комитете связи.

Помимо Vimeo недоступными из Казахстана также оказались фотохостинг Flickr и видеохостинг Dailymotion. Этих сайтов не было в списке ресурсов, указанных в решении суда Астаны, но пользователи также сообщали, что они перестали работать.

Против блокировки Vimeo выступили участники сообщества Wedstory.kz казахстанских свадебных фотографов: они заявили, что используют видеохостинг профессионально и платят около 90–100 дол. в год за аккаунт с продвинутыми функциями. «В отличие от того же YouTube, Vimeo считается более удобным и чистым хостингом для профессионалов. Надеюсь, что сайт будет разблокирован в Казахстане», – заявил организатор сообщества Т. Юлдашев.

Несмотря на распоряжение казахстанского регулятора, сайты оказались недоступными не у всех провайдеров. Как рассказал видеограф Д. Макеев, ему подтвердили наличие блокировки в техподдержке государственного интернет-провайдера «Казахтелеком», однако абоненты «Билайн» и Tele2 по-прежнему имели доступ к сайтам с мобильных устройств.

Весной 2015 г. в Казахстане блокировали музыкальный хостинг Soundcloud за размещённые на нём материалы экстремистской организации «Хизб-ут-Тахрир». Сайт был недоступен около месяца: после получения жалобы от Комитета связи администрация Soundcloud удалила запрещённые записи.

В октябре 2014 г. в Казахстане заблокировали доступ к «Медузе» после репортажа из Усть-Каменогорска – спустя сутки после запуска издания. В ноябре на несколько часов оказались недоступными «ВКонтакте», Twitter, Instagram и Facebook, при этом представители местного провайдера утверждали, что никакой блокировки не производилось ***(В Казахстане заблокировали Vimeo и Flickr // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/44807/118/lang,ru/). – 2015. – 28.09).***

***

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) передала руководству соцсети Facebook требование об исполнении Закона о персональных данных, сообщает информагентство «ТАСС» со ссылкой на главу ведомства А. Жарова. По словам руководителя службы, до конца 2015 г. в Роскомнадзоре надеются получить ответ.

А. Жаров отметил, что компания Facebook «получила презентацию ведомства о том, как оно намерено действовать, как оно может проверять компании, которые имеют юридическое представительство в Российской Федерации, и которые его не имеют. Роскомнадзор способен делать проверку и

тех, и других». Закон не предполагает запрета на трансграничную передачу данных при условии согласия гражданина на такой перенос.

«Проверки будут осуществляться в основном документально – если у нас нет подозрений о том, что компания нарушает закон, компании достаточно будет предоставить документы, подтверждающие, что сервера ее находятся на территории Российской Федерации», – подчеркнул глава Роскомнадзора.

Напомним, согласно Закону о персональных данных, который вступил в силу 1 сентября текущего года, операторы веб-сайтов обязаны «обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ». Нарушители будут внесены в спецреестр, который будет вести Роскомнадзор. Кроме того, за несоблюдение требований законодательства предусмотрен штраф в размере 10 тыс. р. или ограничение доступа к ресурсу-нарушителю. После устранения нарушений доступ предполагается восстановить ***(Роскомнадзор будет следить за тем, как Facebook исполняет Закон о персональных данных // SecurityLab.ru (http://www.securitylab.ru/news/474830.php). – 2015. – 26.09).***

Проблема захисту даних. DDOS та вірусні атаки

По крайней мере 10 библиотек в США намерены последовать примеру Нью-Гэмпширской публичной библиотеки в городе Лебанон и запустить выходные узлы TOR, несмотря на предупреждение Министерства внутренней безопасности страны.

Об этом журналистам издания Motherboard рассказала Э. Макрина, основатель проекта Library Freedom Project, главной задачей которого является запустить как можно больше выходных узлов в уже существующих библиотеках. Предполагается, что это поможет пользователям осуществлять поиск в интернете, не беспокоясь о правительственной слежке.

Небольшая публичная библиотека Kilton Public Library в Лебаноне стала первой в стране, где появился безопасный выходной узел TOR. Вскоре после запуска состоялась встреча руководства библиотеки с местными правоохранителями и представителями власти, в ходе которой обсуждалась возможность использования TOR для криминальной активности. В результате узел был временно отключен, однако ранее на этой неделе совет попечителей принял решение вновь его активировать.

По словам Э. Макрина, действия Министерства внутренней безопасности привлекли внимание к проекту, участие в котором намерено принять все большее количество библиотек и членов общины ***(Более десятка публичных библиотек в США намерены запустить выходные узлы TOR // InternetUA***

(http://internetua.com/bolee-desyatka-publicsnih-bibliotek-v-ssha-namereni-zapustit-vihodnie-uzli-TOR). – 2015. – 21.09).

***

Компания Apple сообщила о первой крупнейшей кибератаке на свой магазин приложений App Store. Ее результатом стало заражение сервиса вредоносной программой, которая встраивалась в официальные приложения производителя.

Хакеры внедрили вредоносный код XcodeGhost в инструмент для создания программного обеспечения для платформ Apple. Таким образом, разработчики приложений могли пользоваться зараженной версией программы, не зная о встроенном вирусе.

Пресс-секретарь Apple К. Монеган сообщил, что компания уже убрала приложения из магазина, которые были созданы с помощью вредоносной программы. Также она добавила, что сейчас они проверяют разработчиков для будущего правильного использования версии Xcode. Примеров хищения данных в Купертино не обнаружили.

«Мы удалили приложения из App Store, которые, как мы знаем, были созданы с помощью этой вирусной программы», – сообщила пресс-секретарь Apple К. Монахан. Компания подчеркивает, что контролирует своих разработчиков, чтобы они использовали правильную версию Xcode, а не вредоносный XcodeGhost.

О количестве зараженных приложений представитель Apple ничего не сказала, также она не уточнила, как пользователи iPhone и iPad могут узнать, не заражены ли их устройства.

Такая крупная кибератака для приложения iOS была зафиксирована впервые. По данным китайской компании KQihoo360 Technology Co., заражены могли быть 344 приложения.

Ранее, по данным компании по кибербезопасности Palo Alto Networks Inc., в магазине приложений за все время были обнаружены не более пяти вредоносных программ ***(Apple сообщила о крупнейшей хакерской атаке на App Store // InternetUA (http://internetua.com/Apple-soobsxila-o-krupneishei-hakerskoi-atake-na-App-Store). – 2015. – 21.09).***

***

Компания «Доктор Веб» обнаружила троян семейства Android.SmsBot, способный незаметно для владельцев смартфонов и планшетов отправлять SMS на дорогостоящие премиум-номера, опустошая счета пользователей Android. Зловред получил обозначение Android.SmsBot.459.origin.

Троян распространяется посредством SMS-спама. Потенциальной жертве приходит сообщение якобы от имени заинтересованного покупателя, откликнувшегося на размещённое ранее объявление о продаже чего-либо. В послании предлагается посетить некий веб-сайт для получения более подробной информации. В некоторых случаях для большей убедительности

киберпреступники обращаются к пользователю по имени, что говорит о хорошо спланированной таргетированной атаке, в которой применяется специально сформированная база реально существующих объявлений. Если пользователь перейдёт по указанной в сообщении ссылке, на его устройство будет загружен apk-файл трояна.

Зловред маскируется под клиентское приложение популярного сервиса по размещению объявлений и имеет соответствующий значок. Сразу после запуска троян пытается получить доступ к функциям администратора мобильного устройства, чтобы в дальнейшем осложнить попытки своего удаления. Вредоносная программа фактически вынуждает пользователя предоставить ей нужные права: она препятствует нормальной работе с Android-смартфоном или планшетом, блокируя его экран постоянно демонстрируемым запросом.

Далее троян передаёт на управляющий сервер сведения о зараженном устройстве, включая его IMEI-идентификатор и информацию об операторе. Затем программа осуществляет проверку наличия подключенной к телефонному номеру жертвы услуги мобильного банка нескольких кредитных организаций и выполняет запрос текущего баланса абонентского счёта, а также баланса учётной записи одной из популярных платёжных систем.

Троян может отсылать SMS-сообщения с заданным текстом на указанный номер, выполнять USSD-запросы, перехватывать SMS и пр. При наличии денег на каком-либо из имеющихся счетов пользователя киберпреступники незаметно похищают их, отдав соответствующее указание вредоносному приложению ***(Новый троян крадет деньги у Android-пользователей // InternetUA (http://internetua.com/novii-troyan-kradet-dengi-u-Android-polzovatelei). – 2015. – 21.09).***

***

21 сентября сайт Херсонрыбохраны подвергся нападению хакеров. Атака сайта началась с самого утра.

На сайте разместили видео и текстовые сообщения, посвященные геноциду армян в 1015–1923 гг.

Ответственность за странное вторжение взял на себя некий М. Мелконян. Взломщик позиционирует себя как член киберармии, пишет «Набережная».

Управление охраны, использования и воспроизведения водных ресурсов быстро отреагировало на ситуацию и очистило сайт ***(Кибер-армия взломала сайт Херсонрыбохраны // Kherson (http://kherson.net.ua/news/kiber_armija_vzlomala_sajt_hersonrybohrany). – 2015. – 21.09).***

***

Яндекс разработал технологию активной защиты пользователей Браузера – Protect.

Это комплекс механизмов, которые защищают от наиболее распространённых в Интернете опасностей: фишинга, вредоносных сайтов, перехвата личных данных. Ключевая особенность Protect – в том, что она действует на опережение. Технология срабатывает до, а не после того, как пользователю нанесён вред.

«Protect построена таким образом, чтобы пользователь всегда оставался в безопасности. Во-первых, для того чтобы она заработала, ничего делать не надо – технология уже встроена в браузер, основную программу для работы в интернете. Во-вторых, Protect нацелена на то, чтобы предотвратить угрозу, а не устранять последствия, – говорит Р. Иванов, руководитель Яндекс.Браузера. – В современном Интернете защита необходима и опытным пользователям, и новичкам, и обеспечить её – одна из задач браузера».

Protect защищает личные данные человека при работе в открытой сети Wi-Fi – например, в кафе или аэропорту. Такие сети широко распространены и удобны, но позволяют злоумышленникам легко перехватывать информацию. Protect направляет трафик через защищённые сервера, так что перехват становится невозможен. Технология умеет противостоять фишинговым сайтам – ресурсам, которые маскируются под соцсети или интернет-банки, чтобы выманить у человека личные данные. Если пользователь ввёл на сайте-подделке важные логин и пароль, Protect заблокирует отправку данных и предупредит об опасности. Также Protect предостерегает от перехода на ресурсы с вредоносным кодом и автоматически проверяет загружаемые из интернета файлы на вирусы. Если файл окажется опасным, Protect не даст ему запуститься и нанести вред устройству. Более подробно о технологии читайте в блоге Яндекса.

Технология активной защиты Protect встроена в Яндекс.Браузер для Windows, OS X и Android. Загрузить браузер для компьютера можно на сайте https://browser.yandex.ua/protect, а для смартфона или планшета – в Google Play. Если браузер уже установлен, он обновится автоматически ***(Технология Protect защитит пользователей Яндекс.Браузера // ITnews (http://itnews.com.ua/news/78344-tekhnologiya-protect-zashhitit-polzovatelej-yandeksbrauzera). – 2015. – 21.09).***

***

Так называемая «Центральная избирательная комиссия» «ДНР» зафиксировала множественные хакерские атаки на свой сайт. Об этом сообщает «Коммерсант» со ссылкой на «РИА Новости» и так называемого «главу» «ЦИК» Р. Лягина.

«Мы не можем восстановить работу сайта, потому что он “ложится” бесконечно. Мы его реанимировали уже семь раз. Бесконечные атаки, и мы из этого положения выйти пока не можем. Это наш официальный ресурс», – заявил сепаратист Р. Лягин ***(Хакеры «положили» сайт так называемого «ЦИК» «ДНР» // InternetUA (http://internetua.com/hakeri--polojili--sait-tak-nazivaemogo--cik---dnr). – 2015. – 22.09).***

***

Экспертам удалось обнаружить опасную уязвимость в новейшей версии операционной системы для iPhone и iPad. Умельцам удалось обойти экран блокировки, защищенный паролем и сканером отпечатка пальцев в iOS 9, пишет издание idownloadblog.

Как выяснилось, при помощи несложных махинаций злоумышленники могут получить доступ к личным фотографиям и владельцам смартфона. Для этого нужно четыре раза неправильно ввести пин-код на заблокированном устройстве. После этого пользователь должен в пятый раз начать вводить пароль, но вместо ввода четвертой цифры надо вызвать Siri и спросить у нее, который час.

Тогда неавторизированный пользователь сможет перейти в приложение с часами, зайти в меню регионов и написать в пустой графе любой текст. Выделив его, злоумышленнику достаточно будет нажать кнопку «Поделиться», чтобы попасть в «Сообщения», а уже оттуда можно просмотреть все контакты владельца смартфона. Если же пользователь захочет получить доступ к фотографиям, ему нужно будет создать новый контакт и добавить к нему аватар: при этом он увидит все фотографии на устройстве.

Как сообщает издание, каждый пользователь новейшей iOS может обезопасить свой смартфон еще до того, как Apple выпустит исправление уязвимости. Для этого нужно зайти в «Настройки», выбрать там меню «Touch ID и пароль» и отключить доступ к Siri для заблокированного экрана ***(В iOS 9 нашли опасную уязвимость // InternetUA (http://internetua.com/v-iOS-9-nashli-opasnuua-uyazvimost). – 2015. – 22.09).***

***

WordPress – далеко не самая безопасная CMS в мире, но одна из наиболее простых и популярных. Именно из-за совокупности двух этих факторов, WordPress регулярно становится мишенью хакеров. Новая вредоносная кампания, нацеленная на сайты, работающие под управлением популярного движка, длится всего две недели, но число пострадавших ресурсов уже достигло почти 6 тыс. и стремительно растет.

Эпидемию, набирающую обороты в геометрической прогрессии, заметили специалисты компании Sucuri Labs. По данным экспертов, 95 % зараженных в ходе атаки сайтов работают под управлением WordPress и только 17 % из них уже попали в черные списки Google.

Кампания получила имя VisitorTracker, так как злоумышленники используют функцию visitorTracker_isMob(), внедряя во все javascript-файлы на сайтах жертв код:

```
function visitorTracker_isMob( ){
var ua = window.navigator.userAgent.toLowerCase();
if(/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od)|iris|kindle|lge
|maemo|mi..|v400|v750|veri|vi(rg|te)|vk(40|5[0-3]|\-v)|vm40|voda|vulc ..
```

|vx(52|53|60|61|70|80|81|83|85|98)|w3c(\-|)|webc|whit|wi(g |nc|nw)|wmlb|wonu|x700|yas\-|your|zeto|zte\-/i.test(ua.substr(0,4))) {
return true;
return false;
} /* .. visitorTracker .. */ /*

Цель данной масштабной атаки – заставить максимальное количество пользователей перейти на страницу, зараженную популярным на черном рынке эксплоит китом Nuclear. Внедренный на сайты код заставляет ресурс запустить вредоносный iframe, открыть инфицированную страницу и отправить туда ничего не подозревающего юзера. Исследователи пишут, что сейчас малварь отсылает пользователей на vovagandon.tk (193.169.244.159), но домены и содержание вредоносной страницы постоянно меняются. Только использование Nuclear неизменно.

Конкретную «точку входа», которую хакеры используют для столь массового заражения сайтов, специалисты Sucuri Labs обнаружить не смогли. Судя по всему, атакующие подошли к делу креативно и заражают сайты, эксплуатируя самые разные уязвимые плагины для WordPress, которых насчитывается огромное количество.

Эксперты рекомендуют администраторам сайтов, конечно же, обновить WordPress и все плагины до самых последних, актуальных версий. Также Sucuri Labs советует воспользоваться поиском и при помощи простой команды grep -r “visitorTracker_isMob” /var/www/ проверить, не является ли сайт уже состоявшейся жертвой атаки ***(Тысячи сайтов на базе WordPress пострадали в ходе новой вредоносной кампании // InternetUA (http://internetua.com/tisyacsi-saitov-na-baze-WordPress-postradali-v-hode-novoi-vredonosnoi-kampanii). – 2015. – 22.09).***

***

Каждый раз после выхода нового гаджета Apple сообщество хакеров готовит инструменты для его джейлбрейка. С их помощью пользователи могут обойти защиту операционной системы, чтобы устанавливать неофициальные приложения и твики, не допущенные до официального каталога приложений.

19 сентября Apple выпустила новую версию операционной системы watchOS для смарт-часов Apple Watch, в которой наряду с добавлением нового функционала исправила в общей сложности 37 уязвимостей. По мнению экспертов, выход этого обновления уменьшает шансы на скорый выход инструментов для джейлбрейка носимого компьютера Apple.

Как рассказали специалисты The Register, среди прочих уязвимостей в watchOS 2.0 были устранены «дыры» безопасности, эксплуатация которых открывала возможность для удаленного выполнения кода посредством использования вредоносной веб-страницы, текстовых и аудиофайлов. Также исправлены ошибка в системе Apple Pay, позволявшая терминалу просмотреть недавно осуществленные транзакции, даже если покупка не была совершена, и

брешь в CoreCrypto, которая позволяла атакующему расшифровать частный ключ пользователя.

Другие исправленные уязвимости позволяли злоумышленнику, обладающему физическим доступом к Apple Watch, просмотреть данные приложения и информацию памяти ядра. Кроме того, устранены бреши, позволявшие вредоносному приложению повышать привилегии.

Первоначально релиз watchOS 2 был запланирован на 16 сентября – тот же день, что и выход iOS 9. Однако в связи с обнаружением уязвимости в новой версии прошивки для Apple Watch, релиз был отложен.

Для чего необходим джейлбрейк Apple Watch и что получит пользователь после освобождения от накладываемых ограничений? В действительности причин освободиться от «рабства» множество. В их числе новые темы оформления, улучшение автономности, гибкая настройка Taptic Engine, воспроизведение музыки с помощью встроенного динамика, веб-серфинг и другие функции ***(С обновлением watchOS Apple устранила 37 уязвимостей // IGate (http://iqate.com.ua/lenta/10259-s-obnovleniem-watchos-apple-ustranila-37-uyazvimostej). – 2015. – 23.09).***

***

На перший погляд, символи «%%30%30» – формена абракадабра. Але якщо ви спробуєте набрати їх (без лапок) наприкінці адресного рядка Google Chrome, або ж ввести в адресний рядок посилання http://a/%%30%30, браузер зависне і потім його робота припиниться. До речі, незалежно від того, чи ви перейдете за посиланням, чи просто наведете на нього курсор.

Такий баг Google Chrome днями виявив дослідник безпеки з Латвії А. Аттека. 18 вересня він повідомив про це Google.

Помилка впливає на поточну версію Chrome для Windows і OS X, але при цьому не зачіпає версію для пристроїв з Android.

Розробники браузера обіцяють усунути проблему ***(Новий баг у Google Chrome «вішає» браузер за допомогою 16 символів // World Life Press (http://wlpress.net/ua/suspilstvo/8451-novyi-bah-u-google-chrome-vishaie-brauzer-za-dopomohoiu-16-symvoliv). – 2015. – 23.09).***

***

За последние пять лет Южная Корея пострадала от более чем 110 тыс. кибератак. Об этом сообщил член Общественной администрации Национальной ассамблеи и комитета безопасности Южной Кореи И. Су-гён 18 сентября. Основываясь на данных Национального комп’ютерного информационного агентства (NCIA), было установлено, что с 2011 г. по июнь нынешнего года против правительственных организаций Южной Кореи было успешно осуществлено 114,035 кибератак.

Несмотря на то что в большинстве случаев правительство Южной Кореи обвиняет в осуществлении кибератак своего северного соседа, подтвердить эти

обвинения не удалось. В целом лишь пять нападений осуществлялись с северокорейских IP-адресов – два в 2012 и три в 2013 г.

Чаще всего правительственные организации атаковали сами южные корейцы – 66 805 нападений были зарегистрированы с местных IP-адресов. 18 943 атаки были осуществлены с территории Китая, еще 8092 – из США.

Больше всего от взломов пострадало Министерство иностранных дел Южной Кореи, которое злоумышленники атаковали 8663 раза. Министерство торговли, промышленности и энергетики подверглось 5735 атакам, в то время как Министерство администрации правительства и внутренних дел пострадало от 5224 нападений. Министерство здравоохранения и Национальное полицейское агентство атаковали по 3 тыс. раз каждое.

Чаще всего злоумышленники пытались получить неавторизованный доступ к тем или иным данным – правительство зарегистрировало 33 544 такие атаки. Помимо этого, киберпреступники пытались раскрыть важные данные (18 607 случаев), похитить учетные данные (16 243 атаки) или внедрить вредоносное ПО для негласного сбора информации (14 077 нападений).

«Если засекреченная правительственная информация окажется в публичном доступе, последствия могут быть катастрофическими, – заключил И. Су-гён. – Мы должны предпринять все усилия, чтобы остановить все увеличивающееся количество кибератак». ***(За последние 5 лет Южная Корея стала жертвой сотен тысяч кибератак // InternetUA (http://internetua.com/za-poslednie-5-let-uajnaya-koreya-stala-jertvoi-soten-tisyacs-kiberatak). – 2015. – 22.09).***

***

Adobe Systems выпустила целый набор обновлений для Flash Player, исправляющих ряд критических уязвимостей в программном обеспечении.

Эти уязвимости позволяли злоумышленникам устанавливать на компьютеры пользователей вредоносное ПО. Обновление устраняет 23 уязвимости, 18 из которых могли позволить запустить на компьютере вредоносный код. Некоторые ошибки могли привести к утечке информации. Посредством двух патчей была добавлена или улучшена защита против повреждений модулей вектора, а также против вредоносного содержимого в уязвимых API, используемых работающими в браузерах программами на базе javascript.

Пользователям Windows и Mac следует незамедлительно обновить Flash Player до версии 19.0.0.185, пользователям Linux – до версии 11.2.202.521. Если вы используете версию программы с расширенной поддержкой, то вам нужно убедиться, что версия Flash Player у вас – 18.0.0.241.

Плагины, встроенные в Google Chrome, Microsoft Edge и Internet Explorer 10 и 11, обновятся автоматически вместе с браузерами. Adobe Systems также выпустила обновление для своего проекта AIR под номером 19.0.0.190. ***(В Flash Player исправили ряд критических ошибок // Ultramir.net***

(http://ultramir.net/techno/25119-v-flash-player-ispravili-ryad-kriticheskih-oshibok.html). – 2015. – 24.09).

***

В результате хакерской атаки на компьютерные системы госучреждений США были похищены данные об отпечатках пальцев приблизительно 5,6 млн американцев, сообщает News24.

Уточняется, что в настоящее время возможность махинаций с чужими отпечатками пальцев довольно ограниченна, однако ситуация может измениться с развитием новых технологий.

Всем пострадавшим от утечки данных будут предложены бесплатные услуги по защите от мошенничества ***(В США хакеры похитили отпечатки пальцев более 5 млн американцев // InternetUA (http://internetua.com/v-ssha-hakeri-pohitili-otpecsatki-palcev-bolee-5-mln-amerikancev). – 2015. – 23.09).***

***

Після успішного встановлення троян отримує адміністративні привілеї користувача, тому видалити додаток непросто, пише «Кореспондент» (http://ua.korrespondent.net/lifestyle/videoigry/3566846-populiarni-dodatky-z-Google-Play-vrazyv-virus).

Частина популярних ігор для операційної системи Android виявилися заражені небезпечним вірусом, у результаті чого хакерам вдалося отримати повний контроль над телефоном жертви. Інформацією про це поділилися експерти з компанії ESET, передає The Daily Dot.

Трояну під назвою Mapin вдалося подолати «гуглівський» захист і пробратися в офіційний магазин додатків Google Play. У результаті шкідливий код потрапив у найпопулярніші безкоштовні ігри для Android.

Так, згідно з дослідженням ESET, з кінця 2013 до кінця 2014 р. Mapin встиг заразити хітові додатки Candy Crash, Temple Run, Subway Surfers і Plants Vs. Zombies 2, останній з яких було викачано з магазину десятки тисяч разів протягом року, до того як його не видалили з магазину.

Крім того, вірус вразив сторонні магазини додатків для Android: шкідливий код заразив десятки популярних додатків, деякі з яких досі перебувають у вільному доступі в Інтернеті.

Наразі Mapin вже видалений з Google Play. За інформацією дослідників, найбільше від нього постраждали індійські користувачі: близько 75 % із загальної кількості заражених пристроїв припало на Індію.

Щоб користувачі не помітили небезпечний троян, Mapin вичікує 24 години після встановлення шкідливої програми на смартфон, а потім отримує контроль над пристроєм, пропонуючи встановити оновлення для Google Play.

«Середньостатистичний користувач буде впевнений, що це якесь важливе оновлення, тому в якийсь момент він напевно його встановить, тільки щоб позбутися повідомлення», – розповідають експерти.

Після успішного встановлення троян отримує адміністративні привілеї користувача, тому додаток буде дуже складно видалити. Щоб убезпечити свій смартфон від подібних вірусів, фахівці рекомендують завантажувати додатки тільки з надійних джерел і уважно читати дозволи, які будуть запитувати нові програми при встановленні ***(Популярні додатки з Google Play вразив вірус // Корреспондент.net (http://ua.korrespondent.net/lifestyle/videoigry/3566846-populiarni-dodatky-z-Google-Play-vrazyv-virus). – 2015. – 23.09).***

***

Глобальный сбой Skype 21 сентября был восстановлен лишь ближе к ночи. Компания Microsoft объяснила, что Skype не работал из-за ошибки в авторизации пользователей.

Однако 22 сентября поступила информация, мол, на самом деле Skype был взломан хакерами, которые похитили все пароли пользователей, которых несколько миллионов.

Несмотря на то что работа Skype восстановлена, хоть и не во всем мире, функция смены пароля работает, и разработчики мессенджера настоятельно рекомендуют сменить их, как можно быстрее.

Отдел разработки Skype опасается, что со взломанных аккаунтов стоит ждать массовой вирусной рассылки. Поэтому не рекомендуется переходить по подозрительным ссылкам в Skype ***(Skype взломали хакеры и украли пароли // podrobnosti.ua (http://podrobnosti.ua/2060481-skype-vzlomali-hakery-i-ukrali-paroli.html). – 2015. – 22.09).***

***

Специалисты компании ERPScan обнаружили уязвимость в популярной системе удаленного управления смартфонами Afaria, позволяющую злоумышленникам стирать все содержимое целевых устройств. Проэксплуатировав брешь, киберпреступники могут обойти процедуру аутентификации и удалить все данные со смартфона жертвы.

Системные администраторы могут управлять телефоном с установленной Afaria, отправив на него SMS со специальной цифровой подписью. В ней используется хэш SHA256, выведенный из трех параметров: IMEI-кода смартфона, идентификатора передатчика и значение переменной LastAdminSession. Злоумышленник может получить идентификатор передатчика, отправив на сервер Afaria запрос соединения, а также использовать произвольное значение переменной LastAdminSession. Код IMEI можно получить при перехвате мобильного трафика. Поскольку корпорации обычно закупают смартфоны для сотрудников партиями, злоумышленники могут узнать IMEI-коды остальных сотрудников путем подбора.

Уязвимости подвержены все смартфоны с установленным ПО Afaria. По подсчетам ERPScan, их число достигает 130 млн. Отметим, что разработчик выпустил исправление, устраняющее брешь ***(Брешь в ПО Afaria позволяла удалять данные на любых смартфонах // InternetUA***

(http://internetua.com/bresh-v-po-Afaria-pozvolyala-udalyat-dannie-na-luabih-smartfonah). – 2015. – 24.09).

***

Власти Южной Кореи в апреле приняли нормативный акт, обязывающий продавцов электроники устанавливать на продаваемые детские смартфоны специальное программное обеспечение, призванное заблокировать всё то, что юное поколение не должно видеть. На словах идея была отличная, по факту получилось совсем наоборот. По сведениям, полученным от специалистов подразделения Университета Торонто под названием Citizen Lab, самое популярное приложение для защиты детей Smart Sheriff имеет как минимум 26 уязвимостей в защите.

Данные уязвимости позволяют злоумышленникам обходить защиту для получения доступа к смартфонам и персональным данным детей, причём делать это одновременно в отношении сотен и тысяч телефонов. Специалисты из Citizen Lab поспешили уведомить о бреши в системе безопасности разработчиков данного программного обеспечения, которые незамедлительно заявили, что все ошибки были устранены ***(Южнокорейская система защиты детей от запрещённого контента даёт сбои // InternetUA (http://internetua.com/uajnokoreiskaya-sistema-zasxiti-detei-ot-zapresx-nnogo-kontenta-da-t-sboi). – 2015. – 24.09).***

***

Троянцы для операционных систем семейства Linux распространены не столь широко, как вредоносные программы, ориентированные на заражение других операционных систем, однако вирусным аналитикам компании «Доктор Веб» время от времени все же приходится знакомиться с новыми представителями данной категории опасных приложений. Одним из них стал троянец Linux.Ellipsis.1, отличающийся весьма параноидальным поведением на зараженном компьютере.

Linux.Ellipsis.1 был разработан злоумышленниками для создания на атакованной машине прокси-сервера, однако этот образец отличается от других вредоносных программ для ОС Linux весьма своеобразным поведением, которое специалисты компании «Доктор Веб» назвали «параноидальным». На сегодняшний день достоверно известно, что киберпреступники используют прокси-сервер в целях обеспечения собственной анонимности для доступа к устройствам, взломанным при помощи другой вредоносной программы, – Linux.Ellipsis.2. В целом применяемая киберпреступниками схема атаки выглядит так: при помощи троянца Linux.Ellipsis.2 они получают несанкционированный доступ по протоколу SSH к какому-либо сетевому устройству или компьютеру, а затем используют этот доступ в различных противоправных целях, сохраняя анонимность посредством Linux.Ellipsis.1.

После запуска на инфицированном ПК Linux.Ellipsis.1 удаляет свой рабочий каталог и очищает список правил для iptables, а затем пытается

завершить ряд работающих приложений, в первую очередь – программы для ведения и просмотра логов, а также анализа трафика. После этого троянец удаляет существующие директории и файлы системных журналов и создает на их месте папки с соответствующими именами. Тем самым блокируется возможность создания логов с такими именами в будущем.

На следующем этапе троянец Linux.Ellipsis.1 модифицирует конфигурационный файл «/etc/coyote/coyote.conf» таким образом, чтобы он содержал строку: alias passwd=cat\n. Затем он удаляет ряд системных утилит из каталогов /bin/, /sbin/, /usr/bin/, добавляет атрибут «неизменяемый» (immutable) к некоторым необходимым для его дальнейшей работы файлам и блокирует IP-адреса подсетей, указанные в переданной троянцу команде или перечисленные в его конфигурационном файле. При этом под «блокировкой» понимается предотвращение приема или передачи пакетов информации с/на определенный IP-адрес по заданному порту или протоколу с помощью создания соответствующих правил iptables.

Как уже упоминалось ранее, основное предназначение Linux.Ellipsis.1 заключается в организации на инфицированном компьютере прокси-сервера. Для этой цели троянец контролирует соединения по заданному локальному адресу и порту, проксируя весь транслируемый через этот адрес и порт трафик.

Для вредоносной программы Linux.Ellipsis.1 характерно весьма необычное поведение: троянец имеет довольно обширный список характерных строк, обнаруживая которые в сетевом трафике он блокирует обмен данными с соответствующим удаленным сервером по IP-адресу. Список запрещенных слов также имеет вариативную часть, которая зависит от содержимого входного пакета. Например, если поступающий на зараженную машину пакет данных содержит строку «User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)», то в список добавляются значения eapmygev. и ascuviej. Кроме того, в своей работе Linux.Ellipsis.1 использует список подозрительных и игнорируемых слов.

«Параноидальность» поведения Linux.Ellipsis.1 заключается еще и в том, что помимо блокировки удаленных узлов по адресам из заложенного в него списка троянец проверяет все сетевые подключения компьютера и отсылает на управляющий сервер IP-адрес узла, с которым установлено соединение. Если сервер отвечает командой kill, троянец прекращает работу приложения, которое установило соединение, а заодно блокирует этот IP-адрес с помощью iptables. В своем домашнем каталоге Linux.Ellipsis.1 создает файл с именем ip.filtered, где вместо ip подставляется строчное представление заблокированного IP-адреса. Аналогичная проверка производится для процессов, имеющих в имени строку sshd. IP-адреса из списков блокируются навсегда, в то время как все остальные – на 2 часа: отдельный процесс троянца раз в полчаса проверяет содержимое собственного домашнего каталога и ищет там файлы, созданные более двух часов назад, имя которых начинается с IP-адреса, после чего удаляет их и соответствующее правило в таблице iptables.

Вскоре после обнаружения описанной выше вредоносной программы специалисты компании «Доктор Веб» выявили троянца Linux.Ellipsis.2, являющегося, судя по ряду характерных признаков, творением того же самого автора и предназначенного для подбора паролей методом грубой силы (брутфорс). Аналогично Linux.Ellipsis.1, этот троянец в процессе своей работы очищает список правил для iptables и удаляет «мешающие» ему приложения, создает папки, предотвращающие возможность ведения операционной системой файлов журналов, и обращается за получением задания к управляющему серверу, адрес которого он принимает в качестве входного аргумента при запуске. Количество потоков сканирования и ssh-подключений Linux.Ellipsis.2 автоматически вычисляет на основе данных о частоте процессора зараженной машины.

Получаемое троянцем с управляющего сервера задание содержит IP-адрес подсети, которую вредоносная программа сканирует на наличие устройств с открытым SSH-подключением на порту 22. При обнаружении таких устройств троянец пытается получить к ним доступ, перебирая пары логин-пароль по имеющемуся у него словарю, а в случае успеха отправляет сообщение об этом на сервер злоумышленников ***(Троянец-параноик организует прокси-сервер в ОС Linux // ITnews (http://itnews.com.ua/news/78411-troyanets-paranoik-organizuet-proksi-server-v-os-linux). – 2015. – 25.09).***

***

Членов Конгресса США и работников, задействованных в аппарате, призвали не полагаться на ненадёжные сотовые сети и общаться вместо этого через приложения вроде WhatsApp и Signal, уровень шифрования в которых значительно выше. По заявлениям группы по гражданским правам, сотовые сети используют слабые и попросту устаревшие системы шифрования, в то время как во многих приложениях шифрование достаточно мощное для того, чтобы можно было без опасений отправлять важные сообщения другим членам государственного аппарата.

В Конгрессе США от такого нововведения не разорятся: большинство членов законодательного органа уже давно имеют современные смартфоны, а приложения для коммуникации можно бесплатно скачивать из магазинов. Более того, в iOS встроены FaceTime и iMessage, так что при наличии iPhone даже скачивать ничего не нужно. В то же время алгоритм шифрования A5/1, использующийся в США в сотовых сетях, был создан в 80-х годах, а взломан в 90-х.

«Убедившись в безопасности коммуникации в Конгрессе касательно всех преград, будь то иностранные правительства, преступники или даже другие ветви американского правительства или враждебные работники Конгресса, мы сможем защитить как базовые интересы свободы, так и национальную безопасность», – заявила группа по гражданским правам ***(Членов Конгресса США призвали общаться только с помощью приложений // InternetUA***

(http://internetua.com/clenov-kongressa-ssha-prizvali-obsxatsya-tolko-s-pomosxua-prilojenii). – 2015. – 24.09).

***

Исследователи Heimdal Security сообщили о вредоносной спам-кампании, направленной на пользователей ОС Windows в Скандинавии. В ходе атаки злоумышленники распространяют электронные письма, которые замаскированы под уведомления от местных почтовых отделений, но на самом деле содержат новый вариант вымогательского ПО CryptoLocker, получивший название CryptoLocker2 (или crypt0l0cker).

Спам-сообщения написаны на местных языках и содержат информацию о якобы недоставленных посылках. Для того чтобы ознакомиться с подробностями, пользователям предлагается перейти по указанной ссылке. Таким образом, отмечают специалисты, злоумышленники пытаются заманить потенциальных жертв на сомнительный веб-сайт, который не имеет ничего общего с почтовыми отделениями. При помощи данного ресурса атакующие пытаются заставить пользователей загрузить и открыть файл, содержащий вредонос.

После инфицирования CryptoLocker2 шифрует данные, хранящиеся локально, а также информацию, доступную на устройствах, подключенных к Интернету.

Эксперты Heimdal Security отмечают наличие новых тактик, позволяющих CryptoLocker2 избежать обнаружения антивирусными решениями. Один из таких методов заключается во внедрении вредоносного кода для того, чтобы получить доступ к легитимным процессам Windows.

Владельцы ПК на базе Windows в Норвегии, Швеции и Дании оказались под прицелом серии продолжающихся спам-кампаний, предупреждает Heimdal Security. Ранее похожая тактика была использована в атаках, направленных на пользователей в США, Великобритании, Австралии и других странах. Тогда спам-сообщения рассылались от имени крупных почтовых компаний и содержали трояны Zeus GameOver и Shylock ***(Пользователей в Скандинавии атакует новый вариант CryptoLocker // InternetUA (http://internetua.com/polzovatelei-v-skandinavii-atakuet-novii-variant-CryptoLocker). – 2015. – 25.09).***

***

Злоумышленники использовали серьезную брешь в online-сервисе для загрузки, хранения и обмена фотографиями Imgur для внедрения вредоносного кода в изображения, похищения истории браузеров посетителей, а также манипуляции с имиджбордами 4Chan и 8Chan.

По словам администрации Imgur, которая уже устранила уязвимость, скомпрометированные страницы использовались преступниками в целевых атаках, но не были опубликованы в главной галерее сайта.

В ходе атак злоумышленники внедряли в локальную память жертвы вредоносный код JavaScript, который отправлял ping-запросы на C&C-сервер каждый раз, когда пользователь посещал 8Chan. В настоящее время неизвестно, с какой целью атакующие совершали кибернападения, также нет данных о том, что C&C-сервер отправлял какие-либо команды на инфицированные устройства.

Администрация Imgur ввела ограничения для своих серверов, которые теперь будут размещать только «достоверные» файлы изображений.

По словам директора по работе с сообществами С. Шааф, команда Imgur провела анализ, который показал, что эксплоит был нацелен конкретно на пользователей 4chan и 8chan. Хотя брешь уже исправлена, и сервис более не распространяет вредоносные изображения, С. Шааф рекомендует пользователям удалить историю браузера, cookie-файлы и очистить локальную память ***(Хакеры использовали брешь в Imgur для распространения вредоносных изображений // InternetUA (http://internetua.com/hakeri-ispolzovali-bresh-v-Imgur-dlya-rasprostraneniya-vredonosnih-izobrajenii). – 2015. – 25.09).***

***

Исследователь компании PhishMe П. Бербедж успешно взломал троян удаленного доступа Dendroid, проэксплуатировав обнаруженные в нем уязвимости. Об этом сообщает издание The Register. Специалист представил результаты своей деятельности на конференции DerbyCon.

Dendroid является разработкой американского студента М. Калбертсона. Стажируясь в компании FireEye на должности эксперта по мобильной безопасности, М. Калбертсон предположительно модифицировал свой RAT таким образом, чтобы сделать его необнаружимым. В то же время киберпреступник якобы принял меры по ликвидации нескольких конкурирующих продуктов и начал продавать свой троян. За 300 дол. любой желающий мог приобрести лицензионную копию Dendroid, в то время как исходный код можно было купить за 65 тыс. дол. В августе нынешнего года М. Калбертсон полностью сознался в совершении преступления.

П. Бербедж обнаружил в функционирующем после ареста создателя трояне несколько уязвимостей, позволяющих удаленному пользователь выполнить произвольный код, осуществить XSS-атаку и SQL-инъекцию. Во время своего выступления в пятницу, 25 сентября, на конференции DerbyCon эксперт рассказал о своем открытии, а также представил PoC-коды, позволяющие скомпрометировать вредоносное ПО.

По словам специалиста, Dendroid является одним из наиболее функциональных мобильных RAT, ориентированных на неопытных киберпреступников. Он входит в тройку наиболее используемых семейств вредоносов, и даже после ареста создателя пользуется огромной популярностью во всем мире. Тем не менее, М. Калбертсон допустил несколько ошибок в коде трояна, позволяющих полностью скомпрометировать его работу.

Одна из уязвимостей существует в файле applysettings.php, который записывает настройки в config.php. Удаленный пользователь может с помощью специально сформированного POST-запроса скомпрометировать систему ***(Специалист обнаружил множественные уязвимости в трояне Dendroid // InternetUA (http://internetua.com/specialist-obnarujil-mnojestvennie-uyazvimosti-v-troyane-Dendroid). – 2015. – 29.09).***

***

В начале текущего года издание Forbes отметило, что число осуществляемых DDoS-атак по всему миру растет с каждым днем. Многие компании, которые столкнулись с инцидентами, отмечают, что злоумышленники начали использовать более сложные и разнообразные методы атаки. ИБ-эксперта заявляют, что для осуществления кибернападения хакеры чаще всего эксплуатируют веб-приложения и веб-сайты, отмечает CSO Online.

Согласно последнему отчету компании Verizon, в I квартале 2015 г. число DDoS-атак увеличилось на 34 % по сравнению с аналогичным периодом 2014 г. Эксперты также сообщают, что их мощность увеличилась на 52 %. Главными целями злоумышленников являются банки и другие финансовые учреждения, которые имеют доступ к важной финансовой информации пользователя.

Исследователи из «Лаборатории Касперского» отметили, что в некоторых случаях хакеры осуществляют DDoS-атаку для того, чтобы отвлечь ИБ-экспертов компании от более масштабной целенаправленной устойчивой угрозы. «В настоящее время DDoS- и DoS-атаки часто являются прелюдией к более крупному нападению, поэтому мгновенное обнаружение и устранение данных атак имеют решающее значение для компаний», – рассказывает ИБ-эксперт из PwC Р. Меткалф.

Специалисты из IBM и PwC отмечают, что в случае, если злоумышленники действительно хотят навредить организациям, они используют хакерскую технику под названием RansomWeb. Подобно классическим DDoS-атакам, RansomWeb направлена на то, чтобы сделать ресурсы жертвы недоступными. Однако в отличие от DDoS-нападения RansomWeb может продолжаться очень длительный период, при этом не требуя дополнительных затрат, и нанести более серьезный финансовый ущерб.

Verizon заявляет, что в 2014 г. было раскрыто 99,9 % эксплуатированных уязвимостей. Большое количество существующих брешей позволяет злоумышленникам скомпрометировать уязвимую систему, а затем использовать RansomWeb. ИБ-эксперты сообщают, что эксплуатация уязвимостей позволяет хакерам осуществлять сложные атаки, которым предшествовало более «легкое нападение». На устранение «атак-прелюдий» ИБ-исследователи тратят много времени и ресурсов, в то время как злоумышленники начинают осуществлять действительно масштабное нападение ***(DDoS-атаки – отличное прикрытие для APT-атак и незаметных взломов систем // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/09/29/ddos-for-apt.html). – 2015. – 29.09).***

***

Специалисты компании «Доктор Веб» столкнулись с очередным трояном, предустановленным на Android-устройствах в качестве предустановленного приложения. Вредоносное ПО Android.Backdoor.114.origin было обнаружено в официальной прошивке планшета Oysters T104 HVi 3G.

Android.Backdoor.114.origin собирает и передает на C&C-сервер информацию о зараженном устройстве. В зависимости от модификации злоумышленникам передается уникальный идентификатор девайса, MAC-адрес Bluetooth-передатчика, тип устройства, параметры конфигурации, его MAC-адрес и IMSI-идентификатор, данные о версии вредоносного ПО, ОС Android и ее API, тип сетевого подключения, название APK-файла, данные о стране жертвы, разрешение экрана и модель устройства, информация о занятом и свободном месте на SD-карте и внутренней памяти, а также список установленных приложений.

Основной целью Android.Backdoor.114.origin является скрытая загрузка и установка приложений по команде с C&C-сервера. Вредоносное ПО способно самостоятельно включать опцию установки ПО из непроверенных источников, даже если настройка была отключена пользователем. Как результат, даже при соблюдении пользователем всех мер безопасности устройство останется незащищенным. Android.Backdoor.114.origin преимущественно устанавливает рекламные и шпионские приложения.

Троян скрывается в файловой системе устройства в качестве предустановленного приложения GoogleQuickSearchBox.apk. Производитель планшета был уведомлен о проблеме, но в настоящее время не предпринял никаких мер по удалению вредоносного ПО из прошивки устройства ***(В официальной Android-прошивке обнаружено вредоносное ПО // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/09/29/android-malware.html). – 2015. – 29.09).***

***

CERT (Cyber Emergency Response Team, группа экстренного реагирования на кибератаки), поддерживаемая DHS (Department of Homeland Security, министерство внутренней безопасности) и функционирующая на базе института разработки программного обеспечения Университета Карнеги – Меллон, выпустила оповещение, в котором предупреждает пользователей о продолжающемся господстве целого класса уязвимостей cookie-файлов, которые подвергают риску персональные и даже финансовые данные пользователей.

Оповещение было вдохновлено отчетом об исследовании Cookies Lack Integrity: Real-World Implications, представленным в прошлом месяце на конференции USENIX и написанным С. Чжэном, Ц. Цзяном, Ц. Ляном, Х. Дуанем, Ш. Чэнем, Т. Ванем и Н. Вивером из китайского Университета

Цинхуа, Международного института информатики, Microsoft, Huawei Canada и Университета Беркли.

Авторы документа углубились в атаку внедрением cookie-файла, которая может быть проведена даже в защищенных HTTPS-соединениях. Они описывают уязвимости и слабые места реализации спецификации cookie-файлов RFC 6265.

Атака, описанная на USENIX, требует нахождения в сети на позиции «человека посередине», что дает возможность внедрять в HTTP-сеанс cookie-файлы, которые также будут передаваться по HTTPS-соединениям. Исследователи заявили, что эти уязвимости присутствуют в ряде высоконагруженных сайтов (по именам они назвали Google и Bank of America), и добавили, что последствия могут включать утечку персональных данных, угоны учетных записей, а также финансовые потери.

«Допустим, вы находитесь в сети, которую злоумышленник может контролировать (такой как Starbucks или открытый Wi-Fi). Злоумышленник временно перехватывает управление вашим браузером, чтобы вставить cookie-файл для целевого сайта, – рассказал Н. Вивер сайту Threatpost. – Далее, немного позже, когда вы посещаете сайт (в другой сети, в других обстоятельствах), ваш браузер передает сайту поддельный cookie, и сайт обрабатывает этот cookie. Например, он может просто следить за пользователем, или это может быть полная XSS-атака, заданная в самом cookie-файле».

В документе исследователи отмечают, что доменная изоляция cookie недостаточна и что разные, но связанные домены могут иметь общий набор cookie. Выдержка из отчета:

«Cookie может иметь флаг secure, обозначающий, что cookie должен передаваться только по HTTPS, что усиливает его конфиденциальность во время атаки “человек посередине”. Тем не менее нет подобной защиты целостности от того же противника: HTTP-запросу позволено устанавливать защищенное cookie для своего домена. Злоумышленник на связанном домене может разрушить целостность cookie, используя общий cookie».

Даже политика одного источника, которая должна разграничивать содержимое разных доменов, не является эффективной защитой от таких атак, так как злоумышленник может вынудить браузер жертвы посетить вредоносный сайт.

«Так как RFC 6265 не определяет механизм для обеспечения изоляции и гарантирования целостности, не все веб-браузеры аутентифицируют домен, устанавливающий cookie-файл, – говорится в оповещении CERT. – Злоумышленник может использовать это для установки cookie-файла, который впоследствии будет использован через HTTPS-соединение вместо cookie, установленного на настоящем сайте».

Исследователи предложили ряд возможных защитных мер, главные из которых – внедрение HSTS (HTTP Strict Transport Security) и изменения, которые должны произвести производители браузера. Документ также

описывает пример браузерного расширения, которое лучше изолирует cookie-файлы между HTTP- и HTTPS-доменами.

«HSTS не позволяет вашему браузеру принимать cookie злоумышленника для всех сайтов, поддерживающих HSTS, которые вы уже посетили, так как они идут не по HTTPS, а по HTTP, – сказал Н. Вивер. – Таким образом, любой сайт, установивший HSTS для своего базового домена и всех поддоменов, является иммунным».

«[Браузеры] должны поменять способ обработки cookie-файлов, так как это всегда область вероятных рисков из-за возможности того, что более жесткая политика защиты cookie может сломать имеющиеся веб-сайты», – добавил Н. Вивер ***(Новые атаки используют старые проблемы с браузерными cookie-файлами // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2015/09/29/new-attacks-recall-old-problems-with-browser-cookies.html). – 2015. – 29.09).***

***

Аналитики сообщили о достижении мощности зомби-сети из Linux-устройств 150 Гбит/с, что позволяет злоумышленникам вывести из строя ИТ-инфраструктуру практически любой компании в мире.

Мощность и активность ботнета

Зомби-сеть (ботнет) на основе Linux-трояна XOR DDoS достигла мощности свыше 150 Гбит/с, что во много раз превышает пропускную способность большинства корпоративных инфраструктур, сообщает исследовательская компания Akamai Technologies.

Ботнет активно используется. Ежедневно с его помощью злоумышленники атакуют до 20 целей, 90 % которых расположены в Азии. В основном это компании из игровой индустрии, на втором месте – образовательные учреждения.

Заражение и состав зомби-сети

Ботнет состоит из Wi-Fi-роутеров, серверов и сетевых систем хранения данных с поселившимся в них трояном XOR DDoS. По словам аналитиков, все эти устройства были взломаны по протоколу SSH при помощи атаки типа «грубой силы» (brute force) – то есть путем перебора паролей для доступа к настройкам устройства.

Согласно FireEye, перебор паролей осуществляется со скоростью свыше 20 тыс. попыток в сутки в расчете на одно устройство. В отношении одного из наблюдаемых серверов аналитики зафиксировали свыше 1 млн попыток за период с ноября 2014 г. по конец января 2015 г.

После того как пароль угадан, хакеры отправляют на устройство SSH-сообщение, длина которого в некоторых случаях достигает 6 тыс. символов, представляющих собой команды, разделенные точкой с запятой.

Происхождение трояна

Впервые троян XOR DDoS был обнаружен в сентябре 2014 г. исследовательской группой Malware Must Die. Аналитики считают, что он был

разработан в Азии. По данным FireEye, в ряде случаев взлом сетевых устройств происходил с IP-адресов, принадлежащих гонконгской организации Hee Thai.

Фокусировка на Linux

По словам аналитиков Akamai, ботнет на базе XOR DDoS – пример мощной вредоносной инфраструктуры, построенной на открытом программном обеспечении.

«Десять лет назад Linux представлял собой более защищенную альтернативу Windows, на которую тогда приходилась львиная доля атак. Поэтому компании активно переходили на Linux, для того чтобы укрепить свою инфраструктуру. Но по мере распространения Linux-систем, привлекательность их взлома для злоумышленников тоже возросла», – содержится в отчете Akamai.

Аналитики полагают, что тенденция продолжится. И злоумышленники продолжат активно использовать и развивать троян XOR DDoS.

40 тыс. зараженных роутеров

В мае 2015 г. исследовательская организация Incapsula сообщила об обнаружении свыше 40 тыс. домашних и офисных роутеров, зараженных троянами MrBlack, Dofloo и Mayday. Все три трояна предназначены для устройств под управлением операционных систем с ядром Linux и разработаны злоумышленниками для проведения DDoS-атак ***(Зомби-сеть из Linux-устройств способна «положить» почти любую компанию в мире // InternetUA (http://internetua.com/zombi-set-iz-Linux-ustroistv-sposobna--polojit--pocsti-luabuua-kompaniua-v-mire). – 2015. – 30.09).***

***

Компания CloudFlare подверглась совершенно новому типу DDoS-атаки, никогда ранее не наблюдавшемуся в Интернете. Как сообщается в блоге CloudFlare, в качестве вектора атаки злоумышленники использовали рекламные объявления, отправляющие на сайты примерно 275 тыс. HTTP-запросов в секунду.

Представители CDN-провайдера не назвали, против какого именно сайта велась атака. Они сказали, что флуд-атаки через 7 уровень модели OSI представляют собой отличный пример того, как киберпреступники прибегают к новым векторам атаки, о которых ранее говорилось лишь в теории.

Инженер компании М. Майковски сказал, что, хотя подобные атаки ранее обсуждались среди экспертов, практической их реализации мешало распространение вредоносного сценария JavaScript в рекламном объявлении. Эксперт сказал, что еще ни разу не наблюдал достаточно крупных атак, использующих подобный вектор.

В ходе атаки на серверы CloudFlare ежедневно перенаправлялось 4,5 млрд запросов с 650 тыс. уникальных IP-адресов. Весь вредоносный трафик исходил из мобильных устройств, находящихся на территории Китая.

По словам М. Майковски, в браузере жертвы отображался iframe, содержащий вредоносную рекламу. Как только на странице появлялся такой

элемент, веб-обозреватель начинал отправлять XHR-запросы на серверы CloudFlare ***(CloudFlare подверглась совершенно новому типу DDoS-атаки // InternetUA (http://internetua.com/CloudFlare-podverglas-sovershenno-novomu-tipu-DDoS-atak). – 2015. – 30.09).***

***

ИБ-исследователи из «Лаборатории Касперского» сообщили, что группа политически мотивированных хакеров из Ближнего Востока сосредоточила свое внимание на ИБ-компаниях и командах по реагированию на инциденты. Впервые о существовании кибергруппировки Gaza стало известно еще в 2012 г., однако вредоносная деятельность хакеров активизировалась во втором квартале текущего года.

Обычно злоумышленники орудуют на территории Ближнего Востока и Северной Африки, в частности в Египте, Объединенных Арабских Эмиратах и Йемене. По словам специалистов из «Лаборатории Касперского», хакеры отправляют сотрудникам ИБ-компаний и командам по реагированию на инциденты связанные с ИБ-тематикой вредоносные файлы для того, чтобы получить привилегированный доступ к целевым сетям.

Эксперты отмечают, что ИБ-специалисты имеют более широкий доступ и права внутри организаций, в отличие от других сотрудников компаний. Команды реагирования на инциденты получают доступ к конфиденциальным данным, связанным с текущими киберисследованиями, а также с методами пресечения и борьбы с кибератаками. Именно поэтому эксплуатация компьютерных устройств таких работников несет для злоумышленников особую ценность.

Для осуществления целевых фишинговых атак хакеры используют специально созданные имена файлов, контент и доменные имена. После того как сотрудник перешел по вредоносной ссылке, его устройство инфицируется такими троянами для удаленного доступа, как XtremeRAT и PoisonIvy. По словам специалистов из «Лаборатории Касперского», основными целями хакеров являются компьютеры ИБ-сотрудников из государственных учреждений, в частности посольств ***(Хакеры из Gaza заинтересованы в целевых атаках на устройства ИБ-специалистов // InternetUA (http://internetua.com/hakeri-iz-Gaza-zainteresovani-v-celevih-atakah-na-ustroistva-ib-specialistov). – 2015. – 30.09).***

***

В популярном архиваторе WinRAR, которым пользуются свыше 500 млн людей во всем мире, обнаружена критическая уязвимость, позволяющая злоумышленникам дистанционно выполнить в системе произвольный код.

Критическая уязвимость

Специалисты обнаружили в последней стабильной версии утилиты WinRAR (5.21) критическую уязвимость, позволяющую злоумышленнику дистанционно выполнить на компьютере жертвы произвольный код.

Информация об этом появилась на сайте Vulnerability Laboratory, представляющим собой агрегатор уязвимостей.

Суть уязвимости

Уязвимость содержится в функции Text and Icon. Она позволяет злоумышленникам интегрировать в самораспаковывающийся RAR-архив вредоносный HTML-код. Этот код достаточно поместить в поле Text to display in SFX window при создании архива. Когда пользователь запустит файл архива, код автоматически исполнится. Он может активировать загрузку на компьютер жертвы троянов или шпионского софта, утверждают исследователи.

Комментарий команды WinRAR

В настоящее время на официальном сайте WinRAR – rarlab.com – опубликована бета-версия WinRAR 5.30, однако не упоминается, была ли в ней описанная уязвимость устранена.

Разработчики WinRAR разместили на сайте сообщение по поводу находки, опубликованной в Vulnerability Laboratory. Они указали на тот факт, что самораспаковывающийся RAR-архив представляет собой исполняемый файл (с расширением EXE). Поэтому бить тревогу о том, что он может содержать вредоносный код, бессмысленно. Так как под EXE-файлом может быть замаскирован вообще любой вирус. И пользователь не будет знать об этом, пока не запустит его. Таким образом, все сводится к надежности источника, из которого RAR-архив был получен.

WinRAR – самый популярный архиватор файлов для Windows, которым пользуются свыше 500 млн людей во всем мире ***(Критическая «дыра» в самом популярном архиваторе затронула миллионы пользователей по всему миру // InternetUA (http://internetua.com/kriticseskaya--dira--v-samom-populyarnom-arhivatore-zatronula-millioni-polzovatelei-po-vsemu-miru). – 2015. – 1.10).***

***

Исследователь безопасности Т. Орманди, который на прошлой неделе обнаружил множественные уязвимости в «Антивирусе Касперского», нашел брешь в антивирусе Avast. Неизвестная ошибка в парсере SSL-трафика позволяет злоумышленнику выполнить произвольный код на целевой системе.

Об открытии исследователь сообщил на своей странице в Twitter. Вскоре на запись отреагировал директор отдела киберугроз Avast Д. Кубеч. Он отметил, что в использовании уровневой защиты нет ничего плохого, на что Т. Орманди возразил, что в данном случае уровневая защита оказывается вектором атаки. Исследователь порекомендовал немедленно сменить спорный метод защиты, используемый специалистами Avast.

Запись об обнаруженной уязвимости была опубликована 25 сентября, но представители Avast до сих пор не предприняли никаких мер по ее устранению. На момент написания статьи брешь осталась неисправленной ***(В антивирусе Avast обнаружена уязвимость, позволяющая скомпрометировать систему // InternetUA (http://internetua.com/v-antiviruse-Avast-obnarujena-uyazvimost--pozvolyauasxaya-skomprometirovat-sistemu). – 2015. – 1.10).***

***

Насколько опасна уязвимость, позволяющая атаковать Android через mp3-файлы?

На этой неделе компания Zimperium, занимающаяся вопросами безопасности, опубликовала отчет об очередной уязвимости в Android, которая получила название StageFright 2.0. Она теоретически позволяет злоумышленнику запускать удаленный код на устройстве, на которое был загружен файл формата mp3 или mp4.

Что за StageFright 2.0?

Злоумышленник может спрятать вредоносный код в метаданные к mp3- или mp4-файлу. Такие файлы могут распространяться на пиратских сайтах, и если пользователь включит «зараженную» песню или запустит видео, вирус, содержащийся в метаданных, будет запущен, а хакер через открывшуюся уязвимость, сможет без ведома пользователя удаленно исполнять на его устройстве любые команды. Google присвоила обнаруженной Zimperium уязвимости номера CVE-2015-3876 и CVE-2015-6602.

Какие устройства подвержены уязвимости?

Смартфоны, планшеты и прочие устройства, работающие на Android от версии 1.0 до версии 5.1.1. Теоретически хакеры могут взломать 100 % Android-устройств.

А что на практике?

В действительности ни одно Android-устройство не подверглось атаке с использованием StageFright 2.0. Компания Zimperium не станет выкладывать подробную инструкцию с демонстрацией работы этой уязвимости, хотя предоставила ее Google.

И что сделала Google?

В этом месяце устройства Nexus получат патчи, устраняющие некоторые уязвимости, в том числе StageFright 2.0. На анонсированные на этой неделе смартфоны Nexus 5X и Nexus 6P установлена версия Android, в которую уже включены эти патчи.

Google также отправила патчи другим производителям смартфонов и планшетов, но далеко не все из них добросовестно относятся к постпродажной поддержке своих устройств. В прошлый раз уязвимость StageFright 1.0 была устранена только в новых моделях Samsung, HTC, Motorola, в некоторых устройствах Asus, Alcatel, Nvidia и в смартфоне OnePlus One.

Как избежать проблем?

До тех пор, пока производитель вашего устройства не выпустит очередное обновление безопасности (что может никогда не случиться), следует избегать посещения сомнительных сайтов и скачивания музыки и видео из непроверенных источников.

Все настолько плохо?

Уязвимости StageFright действительно опасные, но паниковать пока рано. Как только хакеры поймут, как их можно использовать – можно начинать волноваться. Зараженными потенциально могут оказаться более миллиарда

устройств по всему миру ***(Насколько опасна уязвимость, позволяющая атаковать Android через mp3-файлы? // InternetUA (http://internetua.com/naskolko-opasna-uyazvimost--pozvolyauasxaya-atakovat-Android-cserez-mp3-faili). – 2015. – 3.10).***

***

В рамках конференции Virus Bulletin 2015 ИБ-эксперт из HP Security Research О. Петровски рассказал о методах, которые могут быть использованы для осуществления кибератак на беспилотные летательные аппараты. Несмотря на то что существуют разные модели дронов, все они, как правило, оснащены одинаковыми основными компонентами, в том числе двигателями, электронными контроллерами скорости, аккумуляторами и пр. В одном из своих исследований специалист проанализировал потенциальные атаки на контроллер полета, систему, состоящую из датчиков и встроенного процессорного блока. В анализе О. Петровски использовал такие популярные модели контроллеров полета, как ArduPilotMega и Pixhawk от 3D Robotics, MultiWii, OpenPilot и DJI Naza.

По словам эксперта, то, что производители используют одну и ту же базовую технологию, является выгодным для развития данного сегмента, однако это также упрощает хакерам пути совершения кибератак. В своей презентации О. Петровски описал несколько сценариев нападения, направленных на дроны, которые летают по запрограммированному пути. Траектория полета таких беспилотников программируется с помощью программного обеспечения наземной станции. Такая система широко используется по всему миру для доставки медикаментов, а в России даже для доставки пиццы.

В своем эксперименте О. Петровски использовал контроллер полета ArduPilotMega в дроне, который эксперт сконструировал сам. Наземная станция, созданная для обмена данными с беспилотником, может использоваться для загрузки новых параметров и команд, что позволяет управлять дроном в полете. По мнению эксперта, проблема заключается в том, что реализация телеметрии и командного протокола не является безопасной. Протокол не использует никаких специальных аутентификаций, что позволяет злоумышленнику устанавливать вредоносное ПО на систему наземной станции для того, чтобы подключиться к телеметрической линии. Телеметрические данные могут передаваться с помощью Wi-Fi, Bluetooth, ZigBee или собственного радиоканала, которые могут быть скомпрометированы злоумышленниками.

О. Петровски рассказал журналистам издания SecurityWeek о том, что большинство методов атаки могут быть реализованы из-за недостатков в конструкции устройства, а не уязвимостей в самой системе. Специалист настоятельно рекомендует производителям дронов обеспечить устройства механизмами аутентификации и шифрования, использовать безопасные загрузчики и пр. ***(Недочеты в конструкции могут быть использованы в***

кибератаках на дроны // InternetUA (http://internetua.com/nedocseti-v-konstrukcii-mogut-bit-ispolzovani-v-kiberatakah-na-droni). – 2015. – 3.10).

***

В сети появился вирус, который защищает роутеры

Компания Symantec обнаружила вирус, который заражает устройства и защищает их от вредоносного программного обеспечения, сообщается в отчете Symantec.

Поскольку пользователи редко обновляют роутеры и никогда не сканируют их на вирусы, то взломать их оказывается очень просто. Появившийся в сети еще год назад вирус Linux.Wifatch делает роутеры безопаснее. Он ведет себя как обычный вирус: заражает устройство, скрывает свои операции и координирует действия по p2p-сети, однако вместо DDoS-атак и поиска важных данных Linux.Wifatch «ограждает» роутеры от других вирусов.

Вирус был обнаружен еще в 2014 г., но не имел вредоносных сообщений в коде. По сообщениям Symantec, вирус обнаружен на десятках тысяч устройств, преимущественно в Бразилии, Китае и Мексике. Чтобы устранить вирус, необходимо перезагрузить роутер, но и после этого он может вновь появиться ***(В сети появился вирус, который защищает роутеры // InternetUA (http://internetua.com/v-seti-poyavilsya-virus--kotorii-zasxisxaet-routeri). – 2015. – 4.10).***

***

Злоумышленники снова начали использовать банковский троян Dridex

Представитель ИБ-компании Palo Alto Networks Р. Олсон сообщил о том, что 1 октября началась и продолжается до сих пор фишинговая кампания, направленная в основном на пользователей из Великобритании. Отправляемые хакерами фишинг-письма содержат документ Microsoft Word, в котором жертве обманным путем предлагают активировать макрос, предназначенный для отображения подконтрольных злоумышленникам интернет-ресурсов и загрузки банковского трояна Dridex.

Напомним, в сентябре текущего года были арестованы главные подозреваемые в создании и применении сложного банковского вредоносного ПО Citadel и Dridex. Гражданин России и гражданин Молдовы были задержаны за пределами своих стран проживания, и теперь их ждет экстрадиция в США.

В конце прошлого года использование Dridex было замечено в масштабных кибератаках, в ходе которых злоумышленники похищали банковские данные жертв. Наибольший интерес у ИБ-экспертов вызвал способ, которым вредонос инфицирует ПК. Dridex содержится в макросе документа Microsoft Word, скрытом в электронном спам-сообщении. Стоит отметить, что киберпреступники начали использовать макросы более десятилетия назад, однако после того, как Microsoft усилила средства защиты против подобных атак, практика перестала быть популярной.

В новой вредоносной кампании фишинговые письма созданы хакерами так, что не вызывают особого подозрения. Чаще всего они касаются бизнес-предложений, розничных заказов и способов их оплаты. Для того чтобы просмотреть счет-фактуру, пользователю в диалоговом окне предлагают активировать макрос. В новой фишинговой кампании макрос связан с URL-адресами, которые инфицируют систему вредоносом Dridex. Palo Alto опубликовала список URL-адресов, C&C-доменных имен и других показателей, которые могут указывать на потенциальную компрометацию ***(Злоумышленники снова начали использовать банковский троян Dridex // InternetUA (http://internetua.com/zloumishlenniki-snova-nacsali-ispolzovat-bankovskii-troyan-Dridex). – 2015. – 4.10).***