СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1–15.06)

2014 № 11

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1–15.06)
№ 11

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 12
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 15
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 25
Інформаційно-психологічний вплив мережевого спілкування на особистість 25
Маніпулятивні технології 28
Зарубіжні спецслужби і технології «соціального контролю» 33
Проблема захисту даних. DDOS та вірусні атаки 47

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компанія Gemius Україна оприлюднила ТОП-20 сайтів Уанета за показником охоплення аудиторії у квітні 2014 р.

До першої п'ятірки ввійшли Google.com (70,4 %), Vk.com (62,6 %), Mail.Ru (54,1 %), Yandex.ua (49,6 %) і Youtube.com (46,2 %).

Facebook збільшує відрив від «Одноклассников», частка відвідувачів яких становила, відповідно, 29,9 і 26,9 %.

Згідно з даними gemiusAudience (fusion panel), розмір інтернет-аудиторії у квітні 2014 р. становив близько 18,5 млн осіб (real users, 14+).

Соцдем звіт складений на підставі 6959 анкет software-панелістів і 43 809 анкет cookie-панелістів.

*Охоплення – процентне співвідношення кількості відвідувачів (реальних користувачів), що здійснили принаймні один перегляд сторінки на вибраному сайті за часовий інтервал, до загальної кількості інтернет-користувачів за цей часовий інтервал ***(Facebook збільшує відрив від Одноклассників // UkrainianWatcher (http://watcher.com.ua/2014/06/05/facebook-zbilshuye-vidryv-vid-odnoklassnykiv/). – 2014. – 5.06).***

***

Нашумевшее мобильное приложение И. Панченко «Правый сектор» собирает деньги на краудфандинговой платформе Na-Starte. Всего И. Панченко планирует собрать 327 103 грн (250 000 грн на проект плюс 77 103 грн – налоги и 8 %-комиссия площадки). Деньги нужны на реализацию амбициозных планов по превращению новостного агрегатора в мобильную социальную сеть. До этого планировалось сделать из приложения «самый защищенный координационный мессенджер в мире», пишет AIN.UA (http://ain.ua/2014/06/02/526737).

Работа над переквалификацией приложения уже началась. И. Панченко рассказал AIN.UA, что изначально кампанию хотели запустить на более известной украинской платформе Big Idea, однако из-за проблем с модерацией решили не ждать и запуститься на Na-Starte.

На сегодняшний день в команде И. Панченко четыре человека: он сам, а также дизайнер, Android-разработчик и iOS-разработчик. «Версия для iOS выйдет 26.06.2014 – в день, когда нашему приложению исполнится три месяца», – пообещал И. Панченко. Возможно, «Правый сектор» придется переименовать, чтобы суровые модераторы Apple дали добро. А пока приложение доступно только в Google Play, где пользуется завидной популярностью – более 50 000 загрузок и около 35 000 активных пользователей в сутки.

Команда существует на деньги родственников, друзей и пожертвований пользователей приложения, а также прибыль от рекламы в push-

уведомлениях. Однако монетизацией И. Панченко пока не обеспокоен. «Я не гонюсь за тем, чтобы в пик популярности напичкать приложение рекламой, заработать 10 000–20 000 дол. и просто похоронить его. Я хочу создать хороший продукт для потребителя, который останется на долгое время. Зачем пытаться заработать миллион, если можно заработать миллиард?» – говорит он.

Несмотря на то что пока денег у разработчиков немного, приложение постоянно дополняется новым функционалом. Недавно в «Правом секторе» появился раздел «Поиск Людей» для помощи в розыске пропавших. «Мы считаем, что появление этой функции в настоящее время крайне необходимо, ведь десятки людей пропадают каждый день, особенно в восточных регионах Украины», – прокомментировал И. Панченко.

Для того, чтобы объявление появилось в приложении, нужно отправить письмо с данными о пропавшем: ФИО, дата рождения, фотография, особые приметы, обстоятельства, при которых пропал. Объявление будет опубликовано в приложении в течение суток.

Кроме технических задач, перед командой также стоят юридические – в настоящее время разработчики решают вопрос с регистрацией своей компании. «Пока не можем определиться с выбором территории, на которой будет открыто предприятие – США, Украина или ЕС. Я думаю, что в ближайшее время мы откроем предприятие на территории Украины, а затем еще где-то», – рассказал И. Панченко.

Регистрация за рубежом мотивирована в первую очередь тем, что заинтересованные в разработках И. Панченко люди – не украинцы. «Очень хотелось бы, что бы инвестиции в наш проект поступали именно от украинских компаний и предпринимателей, но пока, увы, ни одного предложения от украинцев не поступало. Из-за рубежа конкретно выделить кого-то сложно, в основном пишут частные инвесторы и предприниматели, которым интересна IT-сфера», – пояснил он.

Напомним, краудфандинговая платформа Na-Starte запустилась в Одессе 1 февраля 2014 г. Правила сбора средств такие же, как на Kickstarter: проект получит деньги только в том случае, если соберет 100 % суммы или более в установленный срок ***(Приложение «Правый сектор» запустило краудфандинговую кампанию // AIN.UA (http://ain.ua/2014/06/02/526737). – 2014. – 2.06).***

***

Всего за неделю соцсеть Secret стала феноменом в России. H&F разобрался, в чём причина бума анонимных сервисов и какой должна быть идеальная социальная сеть 2014 г.

Из-за чего шум?

Из-за сливов: за пару минут в анонимном приложении Secret можно узнать, что «Газпром» будет продавать газ Китаю всего по 250 дол. за тысячу кубометров, услышать все слухи российского медиарынка и без последствий

написать что-то гадкое о личной жизни своих любимых друзей. О философской стороне вопроса лучше прочесть в отличной колонке Г. Биргера, но если в двух словах – это всё так плохо, что даже хорошо. И очень затягивает: ничего проверить невозможно, доверять ничему нельзя, никто ни в чём не виноват, никто никому ничего не должен – и стоит лишь получать удовольствие от происходящего.

Это круто?

В общем, да. Secret является частью новой волны анонимных сервисов, которые пришли вслед за Snapchat и набрали дополнительную популярность на фоне прошлогоднего скандала вокруг АНБ и разоблачений Э. Сноудена. Запущенный ещё в 2012 г. Whisper куда масштабне, Wut – лаконичнее и скорее напоминает текстовый Snapchat; Confide и Yik Yak – в догоняющих. Все они популярны в США, но не то чтобы кому-то нужны в России. А Secret, в котором с начала февраля стартаперы Кремниевой долины сливают технологические инсайды, всего за одни выходные попал в первую десятку социальных приложений российского App Store.

Почему? В Secret вы не просто общаетесь анонимно – вы обмениваетесь информацией со своими обычными знакомыми из телефонной книжки, но при этом все условности отброшены, и это целиком меняет коммуникацию. Социальным сетям и мессенджерам давно была нужна встряска, и анонимные приложения как раз и дают её. Локальность, конфиденциальность, отсутствие иерархий – всё, что нужно в 2014 г.

Зачем было городить эту анонимность?

Она раскрепощает и облегчает общение. В прошлом году все отказывались от скевоморфизма в дизайне, в этом – от скевоморфизма в коммуникации. Настольные социальные сети подобны официальной почтовой переписке, аккуратно перенесённой в новую среду. Способы взаимодействия между людьми изменились, и многие разработчики уже пару лет пытались освежить свои технологии. Зачастую их эксперименты были безуспешны.

В 2011 г. Б. Нгуен из Color получил 41 млн дол. инвестиций, но сервис, в котором можно было обмениваться фотографиями с находящимися поблизости людьми, оказался никому не нужен и громко закрылся через год. Создатели Path искусственно ограничили максимальное число друзей в социальной сети, чтобы подтолкнуть пользователей к ответственному выбору. Впрочем, это не сделало общение более живым и откровенным, и в настоящее время сервис стагнирует. Идея «социальной близости» казалась отличным решением для новых приложений в 2012 г., но кто сегодня вспомнит Circle (или Highlight)?

Новым сервисам удалось избежать этого проклятия. Эфемерный Snapchat имитирует живое общение, анонимные приложения повторяют механику распространения слухов в толпе, и все они делают коммуникацию непринуждённой. Snapchat, Whisper и Secret не похожи на Facebook , и это прекрасно. В конечном счёте, Facebook – самая большая соцсеть на планете,

но вовсе не канон. Для многих людей в развивающихся странах первый личный компьютер – это дешёвый смартфон на Android, на котором стоит WeChat или другой популярный азиатский мессенджер.

Я слишком стар для такого?

И да, и нет – всё дело в личном выборе. Ещё пару лет назад раздавались предсказания о грядущем буме локальных социальных сетей, и он наступил, правда не в том виде, в котором его можно было представить. Самый явный пример – Pinterest . Запущенный как рабочий инструмент дизайнеров, сервис довольно быстро стал любимой социальной сетью домохозяек: спустя четыре года существования 85 % активных пользователей – женщины.

Социальные группы приспосабливают существующие механизмы для своих нужд. Например, подростки из США захватили Snapchat или Whisper не только потому, что в них легко заниматься секстингом или обсуждать знакомых. А ещё потому, что это удобная незанятая поляна, на которой нет взрослых (или тех других, от кого хочется отмежеваться). Все другие – в Facebook, и оттого он больше не в моде.

Secret не заточен специально под какую-то определённую аудиторию, но в Калифорнии в нём обосновались стартаперы, а за неделю в России – журналисты и работники рекламы.

У подобного феномена есть и неожиданное следствие. Кажется, что в 2014 г. социальным сервисам больше не обязательно быть очень большими: пользователи хотят скрыться от посторонних глаз в мессенджерах и специализированных соцсетях для своих. А инвесторам пора смириться, что Twitter никогда не догонит по аудитории Facebook, несмотря на 3,5 млн ретвитов у самого популярного селфи в истории.

За анонимными сервисами стоит ФСБ?

Инвестиции в социальные сервисы – не самое глупое решение для спецслужб. Но в случае с анонимными приложениями это не тот случай: Whisper получил 55 млн дол., а Secret –10 млн дол. от известных инвесторов, включая Э. Катчера и Google Ventures (основатели Secret Д. Байтау и К. Бадер-Векселер являются выходцами из Google).

А что с монетизацией?

Б. Гарли, один из партнёров венчурной компании Benchmark, вложившейся в Snapchat и Uber, убеждён, что анонимные сервисы будет трудно монетизировать. По его словам, пользователи слишком часто жалуются на свою жизнь или травят других и вряд ли какая компания захочет, чтобы её реклама находилась рядом с постами о насилии или суициде. Но на практике не всё так плохо: почти сразу после запуска Secret свою рекламу в сервисе разместил Gap (а в России моментом уже воспользовался МТС). К тому же Whisper и Secret собирают данные о своих пользователях, как и другие соцсети: это ваш коллега не узнает, что именно вы не любите котиков, а анонимные приложения со временем воспользуются этим для таргетированной рекламы. И потом – ходят слухи, что Facebook собирается купить Secret за 100 млн дол.

Как в Facebook относятся к новым сервисам?

Facebook является заложником собственной огромной аудитории: невозможно провести радикальные изменения, не разозлив кого-то из 1,3 млрд активных пользователей. Но зачем что-то менять целиком, если можно запустить ещё одно приложение для новой аудитории или купить существующее? Так, в рамках стратегии mobile first Facebook разрабатывает клон Snapchat. О новом приложении под временным названием Slingshot известно лишь то, что в его создании активно участвует сам М. Цукерберг. Неясно, станет ли он конкурентом анонимным сервисам или окажется чем-то кардинально новым.

Сможет ли П. Дуров принять участие в этой игре после отъезда?

Мобильная социальная сеть на базе Telegram П. Дурова может составить конкуренцию анонимным приложениям. Подробностей ещё меньше, чем в случае с Facebook, но высокая скорость, шифрование переписки, самоуничтожающиеся сообщения, чаты на 1000 пользователей – это звучит как описание идеального социального сервиса. К тому же П. Дуров фактически имеет готовое решение для корпоративных клиентов, заботящихся о быстром и безопасном способе коммуникации внутри компании. В общем, П. Дуров действует в духе последних трендов, и у него точно всё будет хорошо ***(FAQ SECRET: Всё, что нужно знать о скандальной соцсети // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/faq_secret_vsyo_chto_nuzhno_znat_o_skandalnoy_sotsseti). – 2014. – 6.06).***

***

Mail.ru Group, що володіє 52 % «ВКонтакте», запропонувала на пост гендиректора соціальної мережі сина керівника ВГТРК (Всероссийская государственная телерадиокомпания) О. Добродєєва – Б. Добродєєва.

Поки що призначення не погодив інший акціонер «ВКонтакте» – фонд UCP, який володіє 48 % соцмережі.

На сьогодні Б. Добродєєв виконує обов'язки генерального директора «ВКонтакте». До керівного складу соціальної мережі він увійшов 23 січня 2014 р., зайнявши пост першого заступника гендиректора у зв'язках з інвесторами. До приходу у «ВКонтакте» Б. Добродєєв був членом ради директорів Mail.ru Group ***(Замість Дурова керувати ВКонтакте буде син керівника російської пропагандистської машини // InternetUA (http://internetua.com/zam-st-durova-keruvati-vkontakte-bude-sin-ker-vnika-ros-isko--propagandistsko--mashini). – 2014. – 6.06).***

***

Сервис микроблогов Twitter рассматривал возможность покупки популярных сервисов для прослушивания музыки онлайн Spotify и Soundcloud, что говорит о его готовности тратить миллиарды долларов на музыкальное направление. Об этом сообщает газета The Financial Times.

Изучение сделок шло последние несколько месяцев, а обсуждаемые суммы оценивались в миллиарды долларов, пишет FT. По данным источников издания, Twitter хочет добавить полноценный музыкальный сервис и обеспечить себе новые источники для роста.

Темпы прироста аудитории Twitter за последний год существенно сократились, за что компания подвергается критике инвесторов. С момента IPO в начале ноября 2013 г. по сегодняшний день акции Twitter потеряли более четверти стоимости. Добавление музыки потенциально позволит сервису стать более привлекательным для пользователей.

В ходе раунда инвестиций в январе сервис Soundcloud был оценен в 700 млн дол. Оценочная капитализация Spotify – 4 млрд дол., а сервис Pandora, который торгуется на бирже, стоит около 5 млрд дол. Для сравнения – до сих пор сумма наиболее крупной сделки Twitter по покупке рекламной платформы MoPub составляла 300 млн дол.

По данным FT, наиболее привлекателен для Twitter именно Soundcloud. Представители компаний от комментариев отказались.

Ранее Twitter экспериментировал с собственным приложением Twitter Music. Пользователи могли находить новые треки через персонализированные рекомендации, основанные на их общении в Twitter. Однако проект оказался неудачным, и Twitter закрыл его в марте этого года. После этого Twitter в партнерстве с Billboard договорился об составлении чарта наиболее обсуждаемых на сервисе групп ***(Twitter готов потратить миллиарды долларов на музыкальные сервисы // InternetUA (http://internetua.com/Twitter-gotov-potratit-milliardi-dollarov-na-muzikalnie-servisi). – 2014. – 6.06).***

***

В начале года появилась информация о том, что социальная сеть Facebook ведет разработку нового приложения для обмена фотографиями или короткими видеороликами, которые будут исчезать после просмотра. В ночь с 9 на 10 июня приложение под названием Slingshot неожиданно появилось в App Store, после чего так же неожиданно исчезло. Однако пользователи успели зафиксировать описание и скриншоты программы.

Slingshot призван составить конкуренцию популярному мессенджеру с самоуничтожающимися сообщениями Snapchat. Ранее сам Snapchat отверг предложение Facebook о покупке за 3 млрд дол. – по словам его основателей, они предпочли долгосрочные перспективы сиюминутной выгоде.

Мобильный сервис разрабатывался в Facebook несколько месяцев непосредственно под руководством М. Цукерберга. Приложение позволит отправлять фотографии и короткие видеоролики друзьям, которые могут прочитать их лишь однажды, после чего сообщения автоматически будут удалены. Предыдущая попытка создать аналог Snapchat компании не удалась – в мае Facebook удалила из магазинов приложений сервис Poke.

Slingshot будет независимым от Facebook, подобно новостному Paper или сервису для сообщений Messenger, однако связанным с профилем пользователя в соцсети. Как сообщил представитель Facebook, релиз Slingshot состоялся по ошибке. Официальный запуск мессенджера состоится в ближайшие дни.

Slingshot продолжит стратегию развития Facebook как мобильной компании, а также позволит соцсети вернуть внимание аудитории тинейджеров. По оценкам аналитиков, число пользователей конкурирующего сервиса Snapchat превышает 50 млн, и средний их возраст составляет 18 лет, тогда как топ-менеджеры Facebook ранее официально признали небольшое снижение численности подростковой аудитории соцсети.

Сервисы с самоуничтожающимися сообщениями являются одним из трендов рынка. Ранее компания Yahoo! приобрела приложение Blink – мобильный мессенджер с той же функциональностью ***(В Сети появились скриншоты нового мессенджера Facebook с самоуничтожающимися сообщениями // InternetUA (http://internetua.com/v-seti-poyavilis-skrinshoti-novogo-messendjera-Facebook-s-samounicstojauasximisya-soobsxeniyami). – 2014. – 10.06).***

***

Пользователи «ВКонтакте» получили возможность читать и отвечать на сообщения из специального окна диалогов, открывающегося на главной странице аккаунта. Об этом 8 июня сообщил разработчик «ВКонтакте» О. Илларионов.

Открыть диалоговое окно можно, нажав на значок в правой нижней части, показывающий число находящихся онлайн друзей.

Переписке с одним пользователем или одному чату соответствует отдельная вкладка, которую можно разворачивать и, наоборот, сворачивать или закрывать, освобождая место на странице.

Внешне окно с сообщениями напоминает вкладки диалогов, реализованные в Facebook.

По словам О. Илларионова, нововведение станет «первым шагом в череде запланированных серьёзных обновлений на сайте». Какие ещё обновления появятся в соцсети в ближайшее время, разработчик не уточнил ***(Во «ВКонтакте» появились вкладки диалогов // InternetUA (http://internetua.com/vo--vkontakte--poyavilis-vkladki-dialogov). – 2014. – 9.06).***

***

Во время WWDC 2014 компания Apple представила миру новый язык программирования Swift, который призван упростить разработку и сделать её более наглядной. Этот язык получил поддержку компании Parse, которая предлагает различные облачные службы для разработчиков приложений.

«Здесь, в Parse, мы очень рады появлению Swift, потому что язык приносит массу новых функций для разработчиков iOS и OS X, – отметил в официальном блоге программист компании Ф. Маротто. – Интерфейс классов Swift позволит разработчиков сэкономить массу времени на создании кода. И в целом снизит число ошибок времени исполнения…».

Крупнейшая социальная сеть в мире Facebook поглотила Parse в апреле 2013 г. с целью усилить свои позиции в мире мобильных приложений и платных служб «бизнес для бизнеса».

Стоит отметить, что Swift совместим с существующими библиотеками Objective-C, включая сторонние вроде Parse, так что интеграция языка не должна стать большой проблемой. Подробнее о том, как использовать каркас приложений Parse в проекте Swift, можно узнать в детальной инструкции Stackoverflow ***(Facebook Parse будет использовать новый язык программирования Apple Swift // InternetUA (http://internetua.com/Facebook-Parse-budet-ispolzovat-novii-yazik-programmirovaniya-Apple-Swift). – 2014. – 10.06).***

***

Во «ВКонтакте» появился сервис vk BLACK list, который может стать панацеей для администраторов сообществ против ботов и троллей. С его помощью администраторы могут делиться своими черными списками, тем самым не давая шансов злостным нарушителям «шалить» в других группах. В настоящее время сервис уже имеет базовый функционал для управления черными списками, но создатели утверждают, что все самые интересные функции еще впереди, пишет AIN.UA (http://ain.ua/2014/06/12/528328).

Приложение запрашивает доступ к общедоступной информации администратора и списку его групп. Оно не взаимодействует с личными сообщениями, друзьями, публикациями, медиафайлами и т. д. Для связи со страницей во «ВКонтакте» приложение использует код доступа – токен. Токен не содержит логин и пароль, поэтому делиться им, как утверждают создатели приложения, безопасно.

Между тем буквально на следующий день после запуска администрация «ВКонтакте» насторожилась и присвоила vk BLACK list статус небезопасного ресурса. Переход из социальной сети на сайт сервиса блокируется.

Впрочем, вряд ли этого достаточно, чтобы отпугнуть администраторов, уставших от произвола троллей на страницах порядочных сообществ. Учитывая противостояние между Россией и Украиной, в сети, и в частности, во «ВКонтакте» активизировались комментаторы, многие из которых не внушают доверия. В СМИ их называют «ботами Кремля». Возможно, vk BLACK list поможет с ними справиться по крайней мере администраторам украинских сообществ. А для россиян все «неугодные» страницы в соцсети давно заблокированы ***(Во «ВКонтакте» теперь можно делиться черными***

списками троллей и ботов // AIN.UA (http://ain.ua/2014/06/12/528328). – 2014. – 12.06).

***

Официльный мессенджер социальной сети Facebook запустил новую функцию Instant Video Sending, которая позволяет пользователям отправлять предварительно записанные видеосообщения. Такая возможность появилась в версии приложения Facebook Messenger для мобильной платформы Apple.

Вместе с официальным мобильным клиентом Facebook продвигает и отдельную программу Messenger, предназначенную для пользователей чата соцсети. Благодаря мессенджеру можно отправлять сообщения и общаться со своими друзьями в отдельном приложении. Клиент упрощает обмен сообщениями, поставив в центре внимания непосредственно интерфейс чата.

В обновлении Messenger 6.0, дебютировавшем 13 июня, появилась функция мгновенной отправки видео. Пользователи могут снимать и воспроизводить 15-секундные видеосообщения своим знакомым и близким, не выходя из клиента. Доставка ролика состоится после входа пользователя на сервис.

Среди других нововведений обновленного клиента разработчики отмечают большие отметки «Нравится». «Нажмите и удерживайте, чтобы отправить еще большее изображение руки с поднятым вверх большим пальцем, когда вам что-то действительно нравится», – говорится в описании функции.

В предыдущем обновлении, напомним, Messenger упростил отправку фотографий, голосовых сообщений и другого контента. У пользователей программы появилась возможность передавать видеозаписи из памяти мобильного устройства и просматривать ролики в самом приложении. Для любителей «селфи» была добавлена функция мгновенной отправки фото: теперь передавать снимки можно из окна чата, не покидая переписку ***(В мессенджере Facebook появились бесплатные видеосообщения // InternetUA (http://internetua.com/v-messendjere-Facebook-poyavilis-besplatnie-videosoobsxeniya). – 2014. – 14.06)***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Патриотический флешмоб запустили в соцсетях проукраинские настроенные жители Славянска и других городов Востока.

Они фотографируют свои паспорта, развернутые на странице с пропиской. Фотографии сопровождают подписью – спасите народ Донбасса от русских террористов.

Также активисты выкладывают фото в социальные сети. К флешмобу приобщаются все больше неравнодушных жителей Востока Украины.

Это – ответ украинских патриотов на российскую пропаганду – россияне в последнее время активно распространяют в соцсетях призывы вроде «спасите народ Донбасса от хунты» ***(Жители Востока устроили флешмоб в соцсетях: спасите народ Донбасса от русских террористов // PRESIDENT.org.ua (http://president.org.ua/news/news-352455/). – 2014. – 2.06).***

***

5 июня в некоторых украинских группах в социальной сети «ВКонтакте» появилось обращение к киевлянам, которое содержит просьбу явиться в переулок Госпитальный, 18, чтобы сдать кровь для раненых военных.

В сообщении говорится, что для ребят-военных, которые находятся в госпиталях Киева, необходима кров. Приходить можно в военные госпитали и сдавать кровь. Сдача крови является добровольной, а обращение в социальных сетях – это просто клич о помощи ко всем неравнодушным гражданам, которые готовы и по состоянию здоровья могут помочь.

Также сообщается, что необходима кровь всех групп, а особенно ценен отрицательный резус-фактор.

Многие пользователи в комментариях к посту положительно и с пониманием отнеслись к просьбе ***(Киевлян просят сдать кровь для раненых военных // NovostiUA.net (http://novostiua.net/oss/56944-kievlyan-prosyat-sdat-krov-dlya-ranenyh-voennyh.html). – 2014. – 5.06).***

***

Центральное разведывательное управление США обзавелось аккаунтом в сети микроблогов Twitter.

«Мы не можем ни подтвердить, ни опровергнуть, что это наш первый твит», – так звучит первый твит ЦРУ в профиле @CIA, который был ретвитнут 130 тыс. человек.

Профиль управления уже верифицирован (отмечен галочкой, означающей, что он действительно принадлежит ЦРУ).

На аккаунт уже подписаны более 170 тыс. человек.

Отметим, что само ЦРУ подписано лишь на 25 аккаунтов, среди них – ФБР, Белый дом и АНБ.

Также ЦРУ зарегистрировало свой профиль в соцсети Facebook.

«Расширяясь на эти платформы, ЦРУ сможет более непосредственно общаться с народом и обеспечивать информацией о миссии ЦРУ, его истории и других событиях», – заявил директор управления Д. Бреннан в пресс-релизе.

Напомним, что ранее ЦРУ обзавелось профилями на видеохостинге Youtube и сервисе обмена фотографиями Flickr ***(ЦРУ официально***

зарегистрировалось в социальных сетях // Подробности.UA (http://podrobnosti.ua/power/2014/06/07/979417.html). – 2014. – 7.06).

***

Дізнатися про ключові події лісової галузі Буковини відтепер можна і за допомогою соціальної мережі Facebook. Чернівецьким обласним управлінням лісового та мисливського господарства створено сторінку під назвою «Лісівник Буковини» за посиланням https://www.facebook.com/lisivnyk.buk.

Як повідомили БукІнфо в прес-службі Чернівецького обласного управління лісового та мисливського господарства, на цій сторінці, як і на офіційному сайті Чернівецького ОУЛМГ, буде розміщено інформаційні матеріали про лісове господарство області, анонси подій, фото- та відеоматеріали з метою найоперативнішого інформування громадськості про стан справ у галузі ***(Буковинські лісовики вирішили підкорити соціальні мережі: з новинами лісової галузі відтепер можна ознайомитися на Facebook // Bukinfo (http://www.bukinfo.com.ua/show/news?lid=46334). – 2014. – 2.06).***

***

Ув'язнені зможуть користуватися електронною поштою і соціальними мережами за умови контролю листування з боку співробітників виправних установ. Про це 13 червня під час онлайн-конференції заявив голова Державної пенітенціарної служби України (ДПтС) С. Старенький, передає zn.ua.

«Що стосується доступу до соцмереж і електронної пошті, то він буде організований таким чином, що відправляти і приймати повідомлення і листи буде можливо тільки після перегляду цих повідомлень співробітниками адміністрації колонії», – заявив С. Старенький.

Глава Державної пенітенціарної служби також зазначив, що відомство розробило «європейський» проект закону «Про попереднє ув'язнення» та проект правил внутрішнього розпорядку СІЗО.

«ДПтС розробила проект правил внутрішнього розпорядку слідчого ізолятора і проект нового закону про попереднє ув'язнення. Там будуть враховані всі рекомендації європейських установ із захисту прав людини, а також вимоги законодавства України», – заявив С. Старенький ***(В українських в'язницях дозволять користуватись соцмережами // InternetUA (http://internetua.com/v-ukra-nskih-v-yaznicyah-dozvolyat-koristuvatis-socmerejami). – 2014. – 14.06).***

***

Соцсеть Facebook разрешила выкладывать фото грудного вскармливания после онлайн-акции протеста пользователей. Это следует из правил ресурса.

В обновленных правилах соцсети говорится, что Facebook согласен с тем, «что кормление грудью естественно и прекрасно». Соцсеть признает, что «матерям важно поделиться своим опытом с другими пользователями на Facebook». При этом большая часть этих фотографий, по утверждению ресурса, не противоречит его правилам.

«Имейте в виду, что фотографии, которые мы просматриваем, почти всегда оказываются в нашем поле зрения из-за того, что другие пользователи пожаловались на их появление на Facebook», – объясняется в правилах соцсети.

Смягчение правил последовало после акции протеста Free the nipple (англ. «Свободу соску»). Участники кампании выступают за свободу грудного вскармливания и отсутствие цензуры на фотографии этого процесса. Основной площадкой для протеста стал Twitter, где фото кормления грудью публиковались с хэштегом #FreeTheNipple.

Частичный запрет на снимки грудного вскармливания в фотосервисе Instagram, принадлежащем компании Facebook, сохраняется. Публикация любых фотографий, на которых фигурируют обнаженные интимные участки тела, включая женскую грудь во время лактации, «если только в это время ребенок не задействован активно в процессе кормления», была запрещена в Instagram в апреле ***(Facebook разрешил выкладывать фото грудного вскармливания // InternetUA (http://internetua.com/Facebook-razreshil-vikladivat-foto-grudnogo-vskarmlivaniya). – 2014. – 15.06).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Социальная сеть «ВКонтакте» запустила новый вид рекламы – специальные предложения. Об этом говорится в сообщении соцсети. Любой рекламодатель может создавать определенные задачи для пользователей сети, за выполнение которых они могут получать от него «голоса» (внутренняя валюта «ВКонтакте»). Инструмент доступен в рекламном кабинете.

С помощью системы специальных предложений можно стимулировать пользователей к выполнению определённых действий, вознаграждая их бесплатными голосами. Рекламные акции очень просты в управлении: система сама отслеживает выполнение пользователями условий акции, рекламодателю нужно лишь определиться с условиями акции и ее оформлением. «С помощью рекламных акций вы не просто покупаете действия за голоса, вы добиваетесь глубокого погружения аудитории в рекламируемый объект в процессе выполнения условий», – говорится в сообщении.

Среди задач, которые можно купить за голоса, например, призыв поделиться с друзьями каким-либо контентом рекламодателя, установка приложения, вступление в группу в соцсети, оформление заказа в интернет-магазине, проведение исследований и т. д.

«Голосами» ежедневно пользуется около 1,5 млн пользователей «ВКонтакте», которые расплачиваются ими за виртуальные подарки и используют их в качестве оплаты в играх и сервисах внутри соцсети.

С 1 июня вводится ряд изменений в ценообразование: снижается стоимость каждого «голоса» до 11,8 р. с НДС. Минимальная ставка вознаграждения пользователя составит два голоса. Бюджет рекламных кампаний в кабинете отображаются в российских рублях с учетом НДС 18 %.

Список рекламных акций, доступных пользователю, доступен через интерфейс сайта и внутренних приложений: меню («Мои Настройки» – «Баланс» – «Получить голоса»), окна пополнения баланса.

О желании развивать рекламные форматы «ВКонтакте» заявила еще в апреле. Тогда А. Новосельский, руководитель рекламной биржи Sociate, перешел на работу в соцсеть и заявил, что собирается «заниматься развитием и улучшением рекламных продуктов, делать рекламу не только эффективной, но и полезной пользователям».

По прогнозам экспертов, рынок онлайн-рекламы России в 2014 г. возрастет на 37,4 %. При этом социальные сети могут стать основным драйвером роста российского рынка онлайн-рекламы в этом году. В частности, прогнозируется, что в этом году сами рекламодатели увеличат свои траты на продвижение в «ВКонтакте». Ежегодно этот рост может составлять до 20 %. Этому способствует и «взросление» аудитории «ВКонтакте» ***(ВКонтакте запустила необычный формат рекламы // Marketing Media Review (http://mmr.ua/news/id/vkontakte-zapustila-neobychnyj-format-reklamy-39906/). – 2014. – 3.06).***

***

Компания Mail.ru Group исследовала статистику платежей в социальной сети «Одноклассники» и оценила популярность каждого из существующих способов оплаты услуг.

Возможность оплачивать услуги появилась в «Одноклассниках» в 2008 г. Из-за отсутствия альтернативных способов, вплоть до начала 2010 г. все платежи приходились на SMS. После ввода альтернативных способов платежей – банковских карт, электронных денег и терминалов – доля платежей, осуществляемых через SMS, начала стагнировать, упав до 41 %. В то же время с помощью банковских карт осуществляется около 39 % от всех платежных операций.

Рост проникновения банковских карт сказался и на платежах в Интернете, осуществленных с их помощью. Так, например, количество операций связанных с банковскими картами в «Одноклассниках», за прошедший год возросло на 16 % ***(Как и чем расплачиваются***

пользователи Одноклассников // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/kak_i_chem_rasplachivayutsya_polzovateli_odnoklassnikov). – 2014. – 5.06).

***

Представители социальной сети Facebook сообщили, что индийский рынок стал для площадки вторым крупнейшим, после американского.

На сегодняшний день в соцсети зарегистрировано 114 млн пользователей из Индии. По данным Facebook, подавляющее большинство индийской аудитории – молодые люди, многие из которых имеют или получают техническое образование.

Если рост пользовательской базы в Индии не остановится, к 2017 г. эта страна по количеству пользователей социальной сети превзойдёт даже родину Facebook – США.

Рост количества пользователей в Индии был более, чем стремительным: в 2010 г. компания выпустила локальную версию социальной сети, и уже за первый год к ней присоединились 8 млн человек.

Кроме того, Facebook регистрирует значительный рост количества заявок на мобильную рекламу от индийских рекламодателей. Так, 84 % индийских пользователей Facebook выходят в социальную сеть с мобильных телефонов ***(Вторым после США рынком для Facebook стала Индия // Блог Imena.UA (http://www.imena.ua/blog/facebook-india-for-growth/). – 2014. – 5.06).***

***

Facebook обнародовал данные о присутствии в социальной сети представителей малого предпринимательства. Число заведенных ими бизнес-страниц составляет 30 млн. Отметим, что в ноябре 2013 г. число страниц составляло 25 млн.

Почти две трети из существующих страниц (19 млн) управляются через мобильные устройства. Это говорит о том, что роль мобильного маркетинга становится более значимой. «Если у вас есть мобильный гаджет и страница на Facebook, то считайте, что у вас есть мобильная маркетинговая стратегия», – заявил Д. Леви, курирующий в Facebook рекламодателей из малого и среднего бизнеса.

Ряд представителей бизнеса считают, что Facebook специально снижает органический охват их страниц, с целью «вытащить» из рекламодателей больше денег. Такое утверждение появилось после изменений алгоритмов выдачи материалов в новостной ленте. Это вызвало уменьшение количества просмотров тех страниц, в которые не вливались «рекламные» деньги.

Недовольство рекламодателей объяснимо – зачем платить за то, что пользователи соцсети могут увидеть бесплатно? Однако просто показывать страницу в выдаче и не продвигать её за дополнительную плату – путь малоэффективный. Именно такого мнения придерживается Д. Леви.

На своём выступлении в Нью-Йорке Д. Леви сказал, что цель Facebook вовсе не «срубить» больше денег с рекламодателей, а помочь тем самым повысить отдачу от бизнес-страниц. Иначе без дополнительного продвижения страницы растворятся в «белом шуме». Их просто будут «механически» лайкать люди, не придавая им особого значения ***(В Facebook уже 30 миллионов страниц малого бизнеса // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_facebook_uzhe_30_millionov_stranits_malogo_biznesa). – 2014. – 5.06).***

***

Маркетологи, запускающие рекламу на Facebook, получили возможность таргетировать свои объявления на пользователей, переходивших на их сайты по объявлениям в поиске Google. Данный тип таргетинга уже доступен для ряда стран в инструменте «Пользовательские аудитории» (Custom Audience), пишет Marketing Media Review (http://mmr.ua/news/id/reklamodateli-facebooka-mogut-otslezhivat-vzaimodejstvie-auditorii-s-reklamoj-v-google-39961/).

Кроме того, внедрение новой технологии отслеживания cookie позволяет рекламодателям Facebook анализировать вовлечённость пользователей во взаимодействие с рекламой на сторонних ресурсах, в частности, на сайтах Google. Ещё ранее Facebook предоставил маркетологам возможность отслеживать вовлечённость пользователей Bing и Yahoo во взаимодействие с их рекламой.

Функционал был реализован компанией Kenshoo и социальной сетью совместно. Представители пресс-службы Facebook подтвердили появление новой возможности для рекламодателей.

«Теперь вы получаете максимально полную картину о своих потенциальных потребителях, которые когда-либо взаимодействовали с вашей рекламой. Если реклама в Google кажется вам слишком дорогой, вы можете активировать новую функцию таргетинга на Facebook, и ваши затраты на рекламу оправдают себя», – комментирует У. Мартин-Гилл, старший вице-президент по продукту компании Kenshoo.

Напомним, что в январе 2014 г. Facebook также внёс обновления в функционал «Пользовательские аудитории» (Custom Audience). Усовершенствования позволяют рекламодателям таргетировать рекламу на пользователей, которые совершали целевые действия в строго ограниченный промежуток времени. Видимо инструмент предоставляет рекламодателям обширные возможности таргетинга ***(Рекламодатели Facebook'а могут отслеживать взаимодействие аудитории с рекламой в Google // Marketing Media Review (http://mmr.ua/news/id/reklamodateli-facebooka-mogut-otslezhivat-vzaimodejstvie-auditorii-s-reklamoj-v-google-39961/). – 2014. – 6.06).***

***

Б. Боланд, глава отдела маркетинга и рекламы продуктов в Facebook, дал подробные разъяснения касательно того, как происходит подсчет органического охвата для страниц, и объяснил, какие факторы влияют на величину метрики Organic Reach, пишет Marketing Media Review (http://mmr.ua/news/id/glava-reklamnoj-sluzhby-facebook-objasnil-pochemu-snizhaetsja-organicheskij-ohvat-auditorii-39963/).

Публикация подробных объяснений от одного из ключевых специалистов по онлайн-рекламе в Facebook была вызвана растущим числом обращений в техподдержку от обеспокоенных рекламодателей и администраторов страниц. В связи с изменениями работы некоторых механизмов распространения и отображения новостного и рекламного контента у целого ряда Facebook-страниц снизились показатели органического охвата. Б. Боланд дал подробные разъяснения и ряд рекомендаций по работе с этой метрикой.

Почему падает органический охват

По словам Б. Боланда, причин может быть две. Первая причина – рост количества публикуемого контента по сравнению с тем, которое публиковали бренды и компании пару лет назад. С развитием рынка смартфонов и планшетов число постов и типов публикуемого контента существенно возросло, равно как изменился характер взаимодействия с ним.

Чем больше стало публиковаться контента, тем меньше времени остается у пользователей на его просмотр. В среднем в ленте у пользователя Facebook публикует до 1,5 тыс. постов ежесуточно. Для пользователей с большим количеством друзей это число возрастает до 15 тыс. потенциальных публикаций в сутки.

Как результат, растет уровень конкуренции за внимание пользователя, и не все публикации на страницах компаний и брендов получают достаточное внимание аудитории. Ведь люди стали не только больше публиковать собственного контента, но и больше «лайкают» страниц, что в конечном итоге приводит к снижению органического охвата. Рост страниц, на которые подписались пользователи в Facebook за минувший год, составил 50 % (по оценкам руководства департамента Facebook, который занимается новостной лентой социальной сети).

Вторая причина – механизм работы новостной ленты Facebook. После определенных изменений лента новостей социальной сети показывает не весь контент подряд, а наиболее релевантный интересам и активности пользователя. Из потенциальных 1,5 тыс. историй и ссылок пользователь в сутки видит около 300 постов с релевантными тематиками. Для каждого отображаемого поста происходит дополнительное ранжирование контента. За основу при этом берутся сотни факторов релевантности для каждого индивидуального пользователя.

Ключевыми изменениями, по словам руководителя рекламной службы Facebook, стали оптимизация новостной ленты в пользу

высококачественного контента и очистка общей ленты от спама и нецелевой рекламы.

Почему в ленте новостей от страниц не отображается абсолютно весь контент

Как утверждает Б. Боланд, отображение всего контента в режиме реального времени без фильтрации накладывает на работу платформы определенные ограничения. В частности – ограничение по времени потребления контента у пользователей. Когда в общую ленту «валится» поток новостей в реальном времени, часто наиболее важные и ценные публикации проходят мимо внимания целевых групп.

Поэтому в Facebook провели дополнительное тестирование юзабилити и вовлеченности пользователей в публикуемый конвент. В результате этих тестов и была создана существующая система оценки и показа постов в новостной ленте. Если же перейти к показу всех постов без фильтрации в режиме реального времени, то, согласно данным Facebook, органический охват снизится еще больше, чем сейчас.

Связано ли падение органического охвата с желанием Facebook больше зарабатывать

Б. Боланд категорически отрицает этот тезис и говорит, что основной задачей команды Facebook является постоянная оптимизация контента в интересах пользователей, а не в корыстных целях самой социальной сети. Потому что при активном вовлечении в релеватный контент растет и вовлеченность в рекламу от брендов, связанных с этим контентом. Так что, по его словам, нет никакого смысла снижать искусственно уровень органического охвата.

Является ли Facebook единственной маркетинговой платформой, для которой упал показатель органического охвата аудитории

Б. Боланд заявил, что падение органического охвата в настоящее время переживают не только социальные сети, но и онлайн-поисковики, поскольку им пришлось переработать механизмы поиска и отображения контента по релевантным запросам так, чтобы соответствовать растущему уровню конкуренции между различными бизнесами и брендами. Что касается Facebook, то все тенденции по органическому охвату аудитории и другим показателям команда всегда отображала в своих отчетах и собирается это делать и впредь.

Какую ценность имеют подписчики страницы в Facebook, раз органический охват всё равно упал

Б. Боланд настаивает, что большое число целевых подписчиков не утратило ценность для брендов, которые ведут Facebook-страницы. По его словам, «фаны» делают работу страницы эффективнее за счет формирования контекста для рекламных кампаний и получения оперативной отдачи от таких кампаний. Реклама с социально релевантным контекстом в социальной сети дает на 50 % больше отдачи и до 35 % больше продаж через Интернет.

Кроме того, изучение интересов, увлечений, тематик, которые интересуют поклонников страницы за пределами данного бренда, могут помочь компании в формировании релевантного информационного поля. Страницы, которые публикуют высококачественный контент для целевой аудитории, чаще отображаются у этой аудитории в ленте, собирают больше повторных публикаций и «лайков» и в итоге увеличивают органический охват естественным путем, а не через покупные посты или привлечением «ботов».

Для тех, кто хочет оптимизировать свою работу с аудиторией страницы в Facebook, Б. Боланд предлагает изучить раздел с кейсами успешных кампаний в соцсети. В частности, там есть и примеры того, как бизнес может добиться коммерческого успеха при помощи Facebook при сниженном показателе Organic Reach.

Будет ли меняться механизм и природа подсчета Organic Reach в будущем

По словам Б. Боланда, все инновации социальной сети направлены исключительно во благо пользователей Facebook. В частности, так было в апреле этого года, когда пользователей и рекламодателей подробно проинструктировали об изменениях в дизайне и верстке страниц и разъяснили, как работать с новым размером рекламных объявлений в блоке справа на странице пользователя. Поэтому никаких изменений, которые бы повредили интересам пользователей, в метрике Organic Reach не будет, отмечает Б. Боланд ***(Глава рекламной службы Facebook объяснил, почему снижается органический охват аудитории // Marketing Media Review (http://mmr.ua/news/id/glava-reklamnoj-sluzhby-facebook-objasnil-pochemu-snizhaetsja-organicheskij-ohvat-auditorii-39963/). – 2014. – 6.06).***

***

Уже найближчим часом реклама в соціальній мережі Instagram стане доступною для користувачів з усіх країн.

Як пише BBC, першими країнами стануть Великобританія, Канада та Австралія, а згодом реклама зявиться і для користувачів інших країн. Уперше вона зявилась у США, де з минулої осені в стрічці фотографій можна було побачити рекламні оголошення.

Instagram був придбаний Facebook у 2012 р. за більш ніж 1 млрд дол., а вже через рік сервіс вирішили монетизувати за рахунок реклами. На сьогодні в соцмережі – понад 200 млн користувачів, і запровадити рекламу для англомовних країн – логічний крок, вважають в офіційному блозі сервісу. Першими рекламодавцями Instagram стали Adidas, General Electric, та Levi's, і наразі цей список налічує близько 20 брендів. З розширенням ринку до рекламних кампаній зможе долучитися ще більше рекламодавців ***(Реклама в Instagram з'явиться для користувачів з усіх країн // UkrainianWatcher (http://watcher.com.ua/2014/06/11/reklama-v-instagram-z-yavytsya-dlya-korystuvachiv-z-usih-krayin/). – 2014. – 11.06).***

***

Facebook рассчитывает победить Twitter и телевизионные сети благодаря чемпионату мира по футболу, став лидером в маркетинге во время трансляций. В компании уверены, что аудитория может достичь 500 млн футбольных фанатов.

Социальная сеть позиционирует базу своих пользователей как самый большой стадион в мире и всемирную аудиторию для рекламодателей во время футбольного турнира, который начнется на этой неделе. Facebook готовится к борьбе с Twitter, который доминировал в освещении прямых трансляций событий, особенно после рекордного твита с церемонии вручения премии «Оскар», называя своими козырями гораздо больший охват и более точное демографическое выделение целевых аудиторий.

В Facebook считают, что первенство 2014 г. станет первым чемпионатом мира, за которым будут следить с помощью смартфонов. «В 2014 г. впервые появилась возможность носить мобильный стадион в кармане. Это позволяет смотреть матчи, узнавать обо всем: результатах, составах команд, изменениях, травмах, заменах – и делиться этим, – заявил У. Платт-Хиггинс, отвечающий в компании за учетные записи пользователей. – Это чрезвычайно интригующе для тех, кто занимается маркетингом». Facebook заявила, что 500 млн ее пользователей интересуются футболом, судя по ссылкам, на которые они переходили, и страницам, которые они отметили как понравившиеся. Это почти вдвое больше общего числа активных пользователей Twitter (255 млн в месяц).

Twitter позиционирует себя как сопутствующую с телевидением рекламную площадку и имеет договоры о разделении доходов с основными телевизионными сетями. Facebook считает, что может дополнить и, возможно, заменить телевидение как инструмент охвата аудитории фанатов. «500 млн – такую аудиторию очень сложно найти на телевидении», – заявил У. Платт-Хиггинс, добавив, что гораздо проще адаптировать рекламную кампанию в Facebook в середине матча по мере поступления результатов.

Twitter также пытается научить экспертов по маркетингу разрабатывать рекламу по ходу матча. Сервис проводит эксперимент, в рамках которого рекламные агентства попросили создавать рекламный контент при просмотре трансляций предыдущих чемпионатов мира.

Хотя нет единой социальной сети, которая была бы центром прямых трансляций, бренды создают более персонализированные рекламные продукты для их использования в интернет-сетях. Budweiser открывает студию социальных сетей в Сан-Паулу, где компания поможет вручную отобранным агентам влияния из разных стран снимать видео для размещения в Интернете, а McDonald’s воссоздаст некоторые основные моменты чемпионата, используя картофель фри в качестве игроков. Директор по маркетингу компании Visa, официального спонсора чемпионата мира, К. Бёрк заявил, что в настоящее время система тратит в среднем 30 % своего

маркетингового бюджета на цифровые средства коммуникации, что выше среднего показателя в мире (по данным E-Marketer –23 %).

Система платежей Visa будет использовать Facebook, чтобы охватить другие интересы футбольных фанатов – совместно с партнерами им будут предложены купоны. «Можно определить, если кто-то также интересуется музыкой, шопингом или модой, просмотрев профиль пользователя. Это в свою очередь улучшает информационный подход к каждому человеку», – отметил К. Бёрк.

Директора системы Visa из 32 стран, участвующих в финальной стадии чемпионата мира, будут задействованы в создании видео, в котором они расскажут, какая роль отводится футболу в их культуре. Coca-Cola напечатала фотографии фанатов, размещенные в Facebook и Twitter, на флаге размером с футбольное поле, который создал бразильский уличный художник. Флаг будет представлен на матче-открытии в четверг. Компания также экспериментирует с блогерским сайтом Tumblr, которым владеет Yahoo, китайскими социальными сетями Weibo и Renren и российской «ВКонтакте» ***(Facebook и Twitter столкнутся в решающем поединке на чемпионате мира по футболу // InternetUA (http://internetua.com/Facebook-i-Twitter-stolknutsya-v-reshauasxem-poedinke-na-csempionate-mira-po-futbolu). – 2014. – 10.06).***

***

В ближайшее время сеть Facebook планирует объявить, что она предоставляет своим пользователям возможность ознакомиться с их персональными «досье» и даже отредактировать их.

Почему Facebook показывает одним анонс новой игры для iPhone, а другим рекламирует дешевые авиабилеты на Бермуды? Потому что администрация сети анализирует интересы и предпочтения каждого пользователя, составляя на основе этого анализа специальное «досье» на каждого. И на его основе формируется адресная реклама, поясняет издание.

Теперь своё «досье интересов» не только можно будет увидеть, но и отредактировать. Мало того, если пользователю не понравятся какие-либо рекламные объявления в его ленте, он сможет сообщить, какие именно типы маркетинговых сообщений он предпочитает видеть.

The New York Times называет этот шаг «умным» и «революционным». По мнению газеты, изучение интересов пользователей – основа таргетирования бизнеса в социальной сети. Компании проявят готовность покупать больше рекламных услуг и платить дороже, если будут уверены, что предлагаемая ими бизнес-информация достигает целевой аудитории.

Правда, неясно пока, как отреагируют на нововведение Facebook защитники конфиденциальности в сети, оговаривается издание ***(Facebook откроет пользователям свои «досье» на них // Media бізнес (http://www.mediabusiness.com.ua/content/view/39677/126/lang,ru/). – 2014. – 13.06).***

***

Социальная сеть Facebook в ближайшее время начнет использовать данные о действиях пользователей на сторонних сайтах, включая нажатие кнопки «Мне нравится», для таргетинга рекламы в соцсети. Об этом говорится в официальном сообщении Facebook.

С помощью кнопок Like и других элементов кода Facebook интегрирована с множеством интернет-сайтов и мобильных приложений. Это позволяет Facebook собирать информацию о том, какие сайты посещают ее пользователи, какие приложения устанавливают и каким веб-контентом интересуются.

«Пока мы узнаем о ваших интересах преимущественно из того, что вы делаете в Facebook – например, на какие страницы вы подписаны. Однако в скором времени, начиная с США, мы также станем использовать для таргетинга рекламы информацию с некоторых веб-сайтов и приложений, которые вы используете», – говорится в сообщении Facebook.

Таким образом, раньше в распоряжении рекламодателей Facebook были лишь социально-демографические данные, которые пользователь оставил в публичном доступе. Теперь же маркетологи могут соотносить эту информацию с поведением пользователя за пределами соцсети. Например, если пользователь ищет на веб-сайте или мобильном ритейл-приложении телевизор, и эти ресурсы интегрированы с Facebook, то в скором времени пользователь увидит рекламу телевизоров и другой электроники в самой соцсети.

Поведение пользователей на сайтах для таргетинга рекламы отслеживают многие интернет-компании. Facebook в данном случае отличает сочетание личной информации и данных о поведении, а также масштабная аудитория более чем в 1,2 млрд пользователей.

В то же время пользователи могут отказаться от использования подобных данных о себе для таргетинга рекламы. Это можно сделать в настройках большинства популярных браузеров, а также в наборе настроек мобильных устройств на платформах iOS и Android ***(Facebook начнет использовать «лайки» пользователей вне соцсети для рекламы // InternetUA (http://internetua.com/Facebook-nacsnet-ispolzovat--laiki--polzovatelei-vne-socseti-dlya-reklami). – 2014. – 13.06).***

***

Продвигаемые рекламные сообщения в Twitter смогут подстраиваться под текущую погоду в месте нахождения пользователя. Об этом 11 июня сообщает газета The Wall Street Journal.

Сервис микроблогов заключил соглашение с компанией The Weather Company. Соглашение позволит новым партнёрам Twitter через API соцсети продавать таргетированную рекламу, отображающуюся в новостных лентах

тогда, когда погода в том или ином месте максимально располагает к покупке определённого товара.

К примеру, рекламный твит с предложением купить шампунь для кудрявых волос может показываться пользователям, находящимся в условиях высокой влажности, а твит с предложением купить всё для пикника – тем, у кого в конце рабочей недели ожидаются солнечные выходные.

Официальная презентация новых рекламных возможностей в ближайшее время будет проведена совместно представителями Twitter и The Weather Company. Когда состоится презентация, The Wall Street Journal не уточняет.

Вполне естественно, что различные внешние факторы не только могут служить поводами для общения между пользователями в Twitter, но и помочь в организации в соцсети маркетинговых кампаний.

Попытки использовать погоду в качестве одного из механизмов для рекламного таргетинга предпринимались Twitter и раньше. Так, в 2013 г. соцсеть заключила договор с телеканалом The Weather Channel. В рамках договора телеканал помогал ресурсу генерировать связанный с метеоусловиями контент, отображение которого в лентах у обсуждающих погоду пользователей оплачивалось заинтересованными рекламодателями. Тем не менее, сделка не получила серьёзного развития.

Предпринимали шаги в этом направлении и другие крупные интернет-компании. В 2012 г. Google удалось получить патент на механизм выборочного отображения рекламных объявлений у пользователей в зависимости от погоды в их регионе. В патенте, в частности, говорилось о возможности поисковика показывать рекламу кондиционеров, если температура в месте нахождения пользователя превышает определённую отметку ***(Реклама в Twitter будет подстраиваться под погоду // InternetUA (http://internetua.com/reklama-v-Twitter-budet-podstraivatsya-pod-pogodu). – 2014. – 13.06).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

86 % родителей признались, что следят за активностью своих детей в Интернете. Такие данные получила антивирусная компания ESET, разместив на своем сайте соответствующий опрос, передает RuNews24.

В различных социальных сетях зарегистрированы 82 % детей в возрасте от 14 лет. Наибольшей популярностью пользуется ресурс

«ВКонтакте». Аккаунты здесь имеются у 74 % опрошенных. Далее следуют Facebook, Twitter и Instagram.

Особо предприимчивые родители добывают пароли своих чад и регулярно проверяют их профили. В таком поведении сознались более 30 % родителей Великобритании. Еще 67 % достаточно анонимной слежки за активностью. Во вторжении в личную жизнь детей признались также и российские родители ***(86 % родителей тайно следят за несовершеннолетними детьми в соцсетях // EastKorr – Восточный кореспонденг (http://www.eastkorr.net/obshchestvo/86-roditelei-taino-sledyat-za-nesovershennoletnimi-detmi-v-sotssetyakh). – 2014. – 31.05).***

***

Розумна думка в соціальній мережі ніколи не викликає хвилю. Вона – пропозиція зупинитися й подумати.

Хвилю в мережі викликають ниці інстинкти, оскільки завжди заходять у резонанс і поширюються зі швидкістю ланцюгової реакції.

Тому наші очікування, що мережа – це великий стрибок людства, забезпечений доступом до бібліотек, фактів, відкриттів, інтелектуального багатства, поглинаються хвилею атавізмів. І замість того, щоб іти вперед, ми повертаємося назад.

У такій ситуації людство вже опинялося після винаходу лука та стріл. Тварин відстріляли, або вони розбіглися. Племена мисливців і збирачів узялися за самознищення, що привело людство на межу зникнення. Так усе й сталося б, якби не була виявлена й закріплена версія землеробства, накопичення і планування, що ще й забезпечило одомашнювання тварин (без накопичення цього б не сталося).

З мережами нам теж доведеться щось зробити. Це «щось» стосується вже не так фізичного виживання у світі, як координації в ньому.

Така координація – визначальна. Кортес і конкістадори не завойовували цивілізацій, це неможливо було зробити фізично. Вони їх дезорієнтували.

Тим самим загрожує мережа в її нинішньому вигляді: вона дезорієнтує людей сама (самоіндукція інстинктів), не беручи до уваги спроб окремих негідників навмисно зробити те ж саме на догоду запаленій свідомості.

Намагатися запровадити в мережі цензуру або сукупність норм – так само марно, як відібрати лук і стріли в мисливців. Цивілізація мусить знайти нову версію морального захисту, як свого часу знайшла землеробство – усвідомлену нову координацію в навколишній дійсності.

Чому тренди мережі в нинішньому їх вигляді ведуть до самознищення (як лук і стріли)? Та тому, що на самовідтворюваних інстинктах у мережі ніхто й ніколи мережу не створив би.

Розглянемо людину в координації запитань «чого хочу?», «що можу?», «що маю?», «звідки?» (минуле), «куди?» (майбутнє), «що є світ?» (світогляд) і «що є Я?» (моральний закон). Поява лука й стріл через гіпертрофоване

«можу» розірвала гармонійне співвідношення супероснов «хочу» – «можу» – «маю» (уявлення людини про успіх, легалізація) і привела його на межу занепаду.

Деструктивна роль конкістадорів стосовно цивілізації індіанців полягала в руйнуванні зв'язку відповідей на запитання «що є світ?» і «що є Я?» з відповідями на інші запитання. Таким чином була знищена координація неформальної складової суспільного договору (традиції, вірування, культура, забобони, етика) з формальною (закони і норми). Цим зазвичай займається бюрократія. Вона зосереджена в містах. Як результат – стрімкий занепад міст, зокрема, і цивілізації в цілому.

Сучасна мережа має особливий механізм деструкції. Відповіді на перелічені запитання вона пропонує (нав'язує) шукати в мережі. Людина перестає координувати себе з дійсністю, з навколишнім світом. Вона конституює себе через «коди доступу». Суспільний договір не стає договором між людьми на основі традицій і законів (сімейних та суспільних стереотипів), а перетворюється на правила користування мережею. Так свого часу первісна людина перестала піклуватися про одноплемінників, а почала дбати про лук та стріли: засіб виживання став її метою.

Коли людина перемістить пошук на зазначені сім запитань з дійсності в мережу, то вона в ній і буде себе координувати й конституювати. Людина стане просто елементом відтворення мережі, і вже її існування стане сенсом «її» існування. Це означатиме крах людської цивілізації у звичному для нас уявленні.

Уникнути цього буде дуже непросто, бо це не фізичний, а моральний вибір, і безвідмовні інстинкти, як це було у випадку з винаходом землеробства, тут не допоможуть ***(Ткач В. Торжество мережі як крах цивілізації // Дзеркало тижня. Україна (http://gazeta.dt.ua/socium/torzhestvo-merezhi-yak-krah-civilizaciyi-_.html). – 2014. – 30.05).***

***

Американские исследователи изучали воздействие социальных сетей на психику в течение трех лет и обнаружили, что положительные «посты» очень быстро распространяются по всему Интернету. Они проанализировали более миллиардов обновлений статуса Facebook у более чем 100 млн пользователей. Результат однозначен: весёлые и лёгкие сообщения вызывают цепную реакцию и генерируют подобные сообщения у друзей.

Эксперты пришли к выводу, что сообщения позитивного характера распространяются по сети быстрее и чаще, чем негативные.

«Наше исследование показало, что твой статус в соцсети может иметь сильное влияние на настроение и эмоциональное состояние твоих друзей», – заявил глава исследовательской группы Д. Фаулер, профессор политологии в Университете Калифорнии ***(Как статусы в соцсетях влияют на пользователей // InternetUA (http://internetua.com/kak-statusi-v-socsetyah-vliyauat-na-polzovatelei). – 2014. – 12.06).***

***

Многим пользователям сети Facebook хочется, чтобы их воспринимали как умных, ярких, интересных людей, наделенных многими положительными качествами. Ведь в социальных сетях очень важно, как тебя оценивают другие. Чтобы понять, каким человеком пользователь кажется со стороны, можно использовать полезное приложение Five Labs от американского мобильного разработчика Five, пишет AIN.UA (http://ain.ua/2014/06/13/528492).

Если пользователь дает приложению доступ к своему профилю, оно анализирует содержание его публичных постов, выявляя ключевые для анализа слова (причем ход анализа отображается на экране). В результате личность пользователя (конечно, виртуальная, а не настоящая) характеризуется по пяти параметрам: открытость, доброжелательность, добросовестность, эмоциональность и экстраверсия.

Приложение выделяет ключевые для личности характеристики (к примеру, любознательный, склонный анализировать, жесткий, открытый к общению, одиночка и т. д.), а также подбирает тех из ваших друзей, кто более всего похож на вас по психологическому портрету.

Можно также сравнить себя со знаменитостью.

Результаты исследования можно опубликовать в Facebook, Twitter, LinkedIn или Pinterest.

Приложение работает по методике, разработанной в Университете Пенсильвании. Это исследование о взаимосвязи лингвистических паттернов и характеристик личности. В нем принимало участие около 75 000 добровольцев, которые дали согласие на использование информации в своих Facebook-постах, а также заполнили анкеты о себе. Исследователи оценили лингвистические паттерны в постах социальной сети, и оказалось, что с помощью компьютерного моделирования можно довольно точно предсказывать возраст, пол и ответы в анкете ***(Карпенко О. Что ты за человек: приложение рисует портрет личности по постам в Facebook // AIN.UA (http://ain.ua/2014/06/13/528492). – 2014. – 13.06).***

Маніпулятивні технології

В социальных сетях молниеносно распространяется пост, в котором просят оказать помощь грудным детям из Алчевска:

«Требуется спонсорская или организационная помощь для эвакуации грудных детей (1–1,5 года) из Дома малютки в Алчевске, Луганской области. Нужна помощь в размещении детей в Ростовской области, оплата их размещения примерно из расчета 600–1000 рублей на ребенка в сутки. Плюс средства на автобус от границы.

Прошу распространить! Готовым помочь – обращаться в личку! Либо звоните напрямую Е. Кваснюку на номер +7-915-316-32-02».

Этот «клич о помощи» распространяется с помощью групп, которые якобы собирают добровольные пожертвования на помощь Народному ополчению Донбасса, беженцам и детям из Украины.

Исходя из сообщения, в Алчевском доме малютки, которого нет и никогда не было в городе, «находятся 30 малышей: отказники и дети погибших ополченцев. Во дворе дома разорвался боевой снаряд – здание находится на окраине города, на самом острие атаки войск хунты», – указывается в послании.

Алчевцы уже подняли шум по поводу такой бессовестной лжи в социальных сетях:

«Шум в социальных сетях по этому поводу подняли мамы детей-инвалидов, они же члены общественной организации “Журавушка”, – рассказывает директор центра социальной реабилитации детей-инвалидов Л. Малышева. – Они очень возмутились, когда увидели в социальной сети такую информацию, стали писать в ответ, что такого дома малютки у нас в городе нет, как и военных атак». На это некая А. Флорова, создатель группы, стала отвечать, что они сами не знают, что происходит у них в городе. Также она угрожала, чтобы женщины убрали свои записи и написали опровержения на посты.

«Видимо, сбор денег идет полным ходом, – говорит Л. Малышева. – Иногда невозможно собрать деньги на операцию ребенку, который остро в ней нуждается. А тут кто-то просто наживается на ситуации в стране. Никогда в Алчевске не было дома малютки, ближайший находится в Лотиково».

Опровергла ситуацию с пострадавшими детьми и главный врач Алчевской городской центральной больницы Л. Винникова: «Начнем с того, что никакого дома малютки в Алчевске нет, и военных действий тоже, слава Богу, нет. На улице Запорожской, кроме приюта, находится детская больница, где в каждом отделении в настоящее время находятся более 30 детей. Но это, конечно же, самые обычные дети, а не пострадавшие в боевых действиях, – сообщает главврач. – Медики работают круглосуточно в штатном режиме. Также хочу сказать ответственно, что нет ни одного такого пострадавшего и в хирургии. Не было и вызовов скорой помощи на подобные ситуации. Если есть отзывчивые люди, то лучше пусть оказывают адресную помощь больным детям, которых у нас в городе предостаточно и так. Можно обращаться прямо в больницу, и мы дадим координаты родителей больных детей».

По адресу, указанному в сообщении – ул. Запорожская, 148 – располагается здание Алчевского приюта для детей. Но и там никто не знает о грудных детях, нуждающихся в эвакуации ***(В соцсетях собирают деньги для эвакуации детей из несуществующего Алчевского дома малютки в Ростов. Алчевцам, возмущенным мошенничеством, угрожают // Неделя***

(http://nedelya.net.ua/news/socium/V-socsetjah-sobirajut-dengi-dlja-jevakuacii-detej-iz-nesushhestvujushhego-Alchevskogo-doma-maljutki-v-Rostov-Alchevcam-vozmushhennym-moshennichestvom-ugrozhajut). – 2014. – 2.06).

***

«Российская кампания по формированию отношения в мире к вторжению на Украину ширится: теперь она включает вербовку и подготовку новых штатных интернет-троллей, которых используют для распространения взглядов Кремля через разделы комментариев ведущих американских сайтов». Об этом сообщает журналист BuzzFeed М. Седдон.

В распоряжении издания оказались документы, которые содержат инструкции для комментаторов сайтов Fox News, Huffington Post, The Blaze, Politico и WorldNetDaily. В них также излагается ожидаемый от «троллей» объём работ: в среднем за день они должны оставлять до 50 комментариев к новостным статьям. Каждый блогер должен вести шесть аккаунтов в Facebook, публикуя минимум три записи в день и дважды участвуя в обсуждениях в сообществах. Другие сотрудники должны вести по 10 аккаунтов в Twitter, публикуя по 50 твитов ежедневно.

Согласно документам, прикреплённым к нескольким сотням писем, отправленным И. Осадчему, который предположительно является руководителем проекта, кампания началась в апреле и проводится санкт-петербургской фирмой «Агентство интернет-исследований». Сам И. Осадчий заявил, что никогда не сотрудничал с этой компанией, и назвал публикацию документов «неудачной провокацией», говорится в статье.

Доказать аутентичность документов и связи их авторов с Кремлём непросто, однако многие наблюдатели в России сомневаются, что речь может идти о чём-то другом.

…При этом российские «тролли», кажется, взяли на себя труд изучить политику модерации комментариев различных ресурсов: в документах перечислены запрещённые на ряде сайтов ругательства и типы оскорблений.

«Щедрое финансирование троллинг-проекта соответствует его довольно крупным масштабам, – говорится в статье. – В бюджете на апрель 2014 г. – первый месяц его существования – прописаны 25 сотрудников и расходы на общую сумму свыше 75 тыс. дол., – передаёт автор статьи. – В самом “Агентстве интернет-исследований”, которое основано прошлым летом, на сегодняшний день трудятся больше 600 человек, и, если расходы останутся на уровне декабря-апреля 2013–2014 гг., в этом году его бюджет, судя по документам, может превысить 10 млн дол.».

«Бизнес-газета “Ведомости”, ссылаясь на источники, близкие к президентской администрации В. Путина, написала на прошлой неделе, что кампания была напрямую срежиссирована властями, а участие в ней принимают российские блогеры-экспаты в Германии, Индии и Таиланде, – продолжает М. Седдон. – “Новая Газета” ранее сообщила, что кампанией

руководит Е. Пригожин – ресторатор, обслуживавший в 2012 г. инаугурацию В. Путина».

По словам журналиста, документы попали в распоряжение BuzzFeed от группы хакеров «Анонимный Интернационал». В предыдущие месяцы она прославилась тем, что выложила в сеть материалы о том, как готовился референдум в Крыму, список награждённых В. Путиным за освещение событий в Крыму журналистов и личный электронный адрес командира украинских повстанцев И. Стрелкова.

«Ни одна из утечек группы не была признана ложной», – подчёркивает М. Седдон.

«Тот факт, что активность сторонников Кремля возросла из-за кризиса на Украине, указывает, что Россия хочет разжечь недовольство в Америке и одновременно подавить его у себя дома, – полагает автор статьи. – Онлайн-наступление идёт вслед за чередой законов и сигналов, недвусмысленно дающих понять, что Россия намерена затянуть гайки в своём динамичном независимом интернет-пространстве».

В целом данные документы укладываются в новый интерес российских властей к онлайн-пространству. «В. Путин никогда не был большим поклонником Интернета, даже в начале 2000-х, – говорит журналист, эксперт по спецслужбам А. Солдатов. – Когда в ходе протестов он был вынужден задуматься об Интернете, он стал очень подозрительным, особенно к социальным сетям. Он уверен в существовании заговора, западных интриг, направленных против него. Он видит в этом большую опасность для себя и должен взять это под свой контроль».

«Интернет стал главной угрозой – сферой, которую Кремль не контролирует, – цитирует М. Седдон П. Чикова из Совета при президенте по правам человека. – Вот почему они за него взялись. Эти меры ставят под угрозу само его существование в том виде, к которому мы привыкли» ***(Кремль запустил армию российских троллей на американские сайты // InternetUA (http://internetua.com/kreml-zapustil-armiua-rossiiskih-trollei-na-amerikanskie-saiti). – 2014. – 4.06).***

***

Американські ЗМІ, натхненні хакерами, почали полювання на проплачених інтернет-тролів з Росії на своїх сайтах.

Журналісти The Washington Post відшукали в коментарях до статей на своєму сайті сліди російських інтернет-тролів, які заробляють за свою активність у мережі гроші і про існування яких стало відомо минулого тижня завдяки хакерам із групи «Анонімний інтернаціонал».

«Цих тролів легіон. Вони сваряться і викликають роздратування. Їх фінансує компанія з неочевидними зв'язками з Кремлем. Вони діють у коментарях до The Washintton Post, а також New York Times, CNN і The Huffington Post», – повідомляє видання. Відрізнити «російських тролів»

можна через їх погану англійську, нісенітниці, вигуки, гордість за Росію і імперські амбіції, визначили американці.

Справа дійшла до того, що, наприклад, газета The Guardian змушена була визнати проблеми з модеруванням коментарів, оскільки зіткнулася з «організованою кампанією на підтримку Кремля».

Наприкінці травня група хакерів з «Анонімного інтернаціоналу» почала публікацію масивів документів, отриманих із зламаних електронних поштових скриньок О. Дзалби, фінансиста Агентства інтернет-досліджень (АІД), структури, заснованої в передмісті Петербурга-Ольгіно влітку 2013 р. за, як стверджується, замовлення глави компанії «Конкорд» Є. Пригожина. Крім того, у відкритому доступі виявилися звіти про виконану роботу, адресовані людині на прізвище Володін.

«Ведомости», до речі, пов'язують прийняту Кремлем на озброєння стратегію маніпулювання суспільною свідомістю через нові медіа з ім'ям В. Володіна, першого заступника глави адміністрації президента.

Як випливало з документів, які проаналізувала «Фонтанка.ru», під єдиним керівництвом вибудувана схема з інтернет-агентств із сотнями платних блогерів і коментаторів, а також кількох засобів масової інформації в Росії та Україні. На їх утримання передбачено кошторис у 33,5 млн р. на місяць, з яких понад 17 млн – готівкою. Фінансові документи рясніють позначками «Не оф.» – наймовірніше «не офіційно».

У звітах про виконану роботу за, наприклад, початок січня йдеться про пости на тему волгоградських терактів, п'яного водіння О. Навального і новорічне звернення В. Путіна. При цьому тролі скаржаться, що, виводячи звернення В. Путіна до топ Twitter, їм довелося конкурувати з хештегами про серіал «Шерлок».

Опитані «Фонтанкою» «гуру блогосфери» зійшлися на тому, що ефективність інтернет-тролів не найкраща. «Чи змінюють політичні настрої в суспільстві платні тролі? Ні, звичайно, це просто крадіжка бюджету замовника в чистому вигляді. Блогер отримує за пост 11 р. 80 коп., проміжний рахунок виставляється за той же пост вже 800 р., замовник оплачує 850 р.. І нічого в світі не змінюється», – вважає А. Носик.

«Суспільну свідомість змінює не Інтернет, а телебачення. Телевізор дивиться найменш інформована частина населення, у якої немає можливості або бажання отримувати інформацію з інших джерел. Ті зусилля, з якими платна тусовка створює псевдо патріотичний і продержавний фон у мережі, пропадають намарно. Замовники бачать, що це ні до чого не призводить і починають діяти іншим чином. Наприклад, за допомогою заборонної законотворчості в інформаційній сфері», – додає Р. Адагамов.

У Кремлі, як повідомляється, відмовляються коментувати інформацію, згадані в листуванні люди заявляють про провокації і фальсифікації або уникають відповідей, але вартість проекту, масштаб і коструватість реалізації змушують спостерігачів сумніватися в тому, що така армія тролів могла б бути створена в іншій країні, крім Росії.

The Washington Post, однак, не погоджується з тим, що платні інтернет-тролі – це російський винахід, оскільки в Держдепартаменті США, наприклад, існує Digital Outreach Team – команда, створена для ведення полеміки з джихадистами арабською, сомалійською а іншими мовами на форумах і в соцмережах. Утім, зазначає видання, результати роботи цієї команди у 2012 р. були визнані досить посередніми: збити градус антиамериканських висловлювань тролінгом не вдалося, пише «Украина Криминальная» ***(Американці розпочали полювання на проплачених Кремлем інтернет-тролів // Західна інформаційна корпорація (http://zik.com.ua/ua/news/2014/06/05/amerykantsi_rozpochaly_polyuvannya_na_proplachenyh_kremlem_internettroliv_495048). – 2014. – 5.06).***

Зарубіжні спецслужби і технології «соціального контролю»

Секретная служба США, отвечающая за безопасность президента страны и других высокопоставленных чиновников, намерена приобрести программное обеспечение, которое позволит отслеживать сарказм в соцсетях

Об этом пишет «Лента.ру».

Так, в заказе, размещенном на сайте госзакупок, уточняется, что необходимая программа должна иметь возможность анализировать большие объемы информации в социальных сетях и визуально представлять полученные результаты. Агентство готово заключить с производителем контракт сроком на пять лет.

Кроме того, заказчик заинтересован в способности ПО распознавать лидеров общественного мнения в соцсетях, анализировать потоки информации в реальном времени и подключаться к архивным данным Twitter. Программа должна быть совместима с браузером Internet Explorer 8.

По словам пресс-секретаря Секретной службы Э. Донована, такая технология позволит упростить анализ соцсетей и отслеживать наиболее важные проблемы, волнующие пользователей Интернета.

«Нашей задачей является автоматизация мониторинга социальных медиа. Мы анализируем Twitter. Это происходит в режиме реального времени», – сказал он. По его словам, способность улавливать сарказм является лишь одной из 16 или 18 целей программы агентства ***(Охрана президента США начнет отслеживать сарказм в соцсетях // Комментарии: Харьков (http://comments.ua/world/471586-ohrana-prezidenta-ssha-nachnet-otslezhivat.html). – 2014. – 4.06).***

***

С 1 августа в России начнет действовать «антитеррористический пакет поправок в законодательство», согласно которому спецслужбы получат доступ к логинам и паролям пользователей соцсетей.

Новые нормы обязывают интернет-компании в течение полугода хранить данные о своих пользователях и по первому требованию передавать их уполномоченным органам.

Согласно новому законодательству, спецслужбы РФ смогут получать практически всю информацию о действиях пользователей в сети.

«Это идентификатор пользователя (логин), все адреса электронной почты (как основной, так и той, что используется для переадресации), список всех его контактов, категории контактов (друзья, подписчики), количество и объем полученных и переданных пользователем сообщений, все изменения в аккаунте и попытки его удаления», – сообщает издание.

Чтобы полиция и спецслужбы знали, у кого запрашивать данные, интернет-компании будут уведомлять о своей работе Роскомнадзор. По информации издания, Facebook, Twitter, «ВКонтакте» и другие соцсети вынуждены будут предоставлять данные о своих пользователях ***(Российские спецслужбы получат доступ к паролям соцсетей // InternetUA (http://internetua.com/rossiiskie-specslujbi-polucsat-dostup-k-parolyam-socsetei). – 2014. – 3.06).***

***

Китайские власти заблокировали большую часть сервисов Google. По предварительным данным, блокировка осуществлена в связи с приближением годовщины событий на площади Тяньаньмэнь – в 1989 г. там была жестоко разогнана студенческая демонстрация.

Недоступными для китайских пользователей оказались практически все ресурсы Google, включая поиск, просмотр изображений, сервис электронной почты Gmail. Китайцам они недоступны не только на китайском домене, но и на гонконгской и зарубежных версиях.

Комментируя блокировку, представители Google отметили, что затрудняются объяснить её причины – со стороны корпорации никаких технических проблем не возникало.

Добавим, что 4 июня 1989 г. во время подавления студенческой демонстрации в Пекине на площади Тяньаньмэнь по официальным данным погибло около 200 человек, и 7000 были ранены.

Очевидно, правительство страны на период 25-й годовщины трагических событий решило заблокировать сервисы Google, чтобы контролировать распространение информации. Никаких официальных заявлений от властей не поступало ***(Китай заблокировал Google, чтобы контролировать информацию о Тяньаньмэнь // Блог Imena.UA (http://www.imena.ua/blog/google-blocked-in-china/). – 2014. – 4.06).***

***

Китайские эксперты подготовили отчет, в котором указывается, что операционная система компании Microsoft Windows 8 несет в себе угрозу безопасности китайских пользователей. Отчет был подготовлен

специалистами центрального телевидения Китая, а его положения всецело поддерживаются правительством государства.

Так, в подготовленном материале указывается, что ОС Windows 8 используется для похищения личной информации граждан Китая. Напомним, что совсем недавно правительство страны запретило использовать Windows 8 на компьютерах государственных учреждений.

«Microsoft больше не намерена открывать исходный код Windows 8 для китайского правительства. Однако схема безопасности Windows 8 настроена таким образом, чтобы обеспечить Microsoft более широкий доступ к базе данных пользователей», – отметил профессор Я. Мин из университета Фудань.

В отчете также указывается, что именно Windows 8 использовалась для вывода данных из Китая. «Ваша личность, счет, список контактов, номера телефонов, со всей этой информацией можно проводить обширный анализ данных. Именно такие данные позволяют США следить за другими странами», – заявил Н. Гуангнан, член Китайской академии наук.

Представители Microsoft в свою очередь заявили, что они «активно сотрудничают» с китайским правительством для того, чтобы развеять опасения по поводу небезопасности продуктов компании.

Напомним, что многие другие крупные американские компании также столкнулись с критикой со стороны Китая за сотрудничество с АНБ. Yahoo, Cisco, Facebook, Apple, Google и других называли «пешками правительства США», которые помогали следить за китайскими гражданами и воровать секреты ***(Китай жестко раскритиковал безопасность Windows 8 // InternetUA (http://internetua.com/kitai-jestko-raskritikoval-bezopasnost-Windows-8). – 2014. – 6.06).***

***

ФСБ России разработало и опубликовало на портале regulation.gov.ru проект указа, согласно которому компании и их клиенты, желающие шифровать свои данные, могут делать это только при помощи сертифицированных службой средств криптографии. Эти средства должны использоваться в зависимости от уровня угроз безопасности информации, прописанных в Законе «О персональных данных», который каждая компания определяет для себя сама.

Примечательно, что ФСБ сертифицирует исключительно те технические средства, в которых применяются отечественные алгоритмы шифрования. Проблема состоит в том, что ни Android, ни iOS такое шифрование не поддерживают. Более того, эти средства защиты являются платными. Например, установка на один компьютер «КриптоПРо CSP» обходится в 1,8 тыс. р.

В документе, разработанном ФСБ, также описываются обязательные требования к безопасности помещений, в которых находятся серверы криптозащиты. Так, окна и двери должны быть оборудованы

металлическими решетками, охранной сигнализацией или «другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения».

Помимо прочего, съемный носитель с конфиденциальными пользовательскими данными, находящимися в незашифрованном виде, в нерабочее время необходимо хранить в специальном сейфе. Отметим, что для некоторых компаний, работающих практически круглосуточно (например, online-магазинов), это требование невыполнимо, поскольку никто не будет вынимать из компьютеров жесткие диски ***(ФСБ обяжет хранить серверы за решеткой и шифровать данные только при помощи отечественных средств // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2014/06/06/fsb-states-infosecurity-measures.html). – 2014. – 6.06).***

***

В Таджикистане четвертый раз за год блокировали доступ к видеохостингу YouTube. Об этом сообщает РИА «Новости» со ссылкой на председателя Ассоциации интернет-провайдеров в Таджикистане А. Атоева.

«Сейчас доступ к видеохостингу ограничили как минимум четыре интернет-провайдера», – отметил А. Атоев. По его словам, провайдеры отреагировали таким образом на распоряжение регулятора службы связи Таджикистана. При этом служба связи блокировку видеохостинга пока не прокомментировала.

Блокировка популярных сайтов в Таджикистане происходит не впервые. В мае 2013 г. Служба связи Таджикистана уже предписывала провайдерам заблокировать YouTube. В качестве возможной причины блокировки тогда называлось размещение на YouTube видео из передачи оппозиционного телеканала К+, посвященной свадьбе старшего сына президента Р. Эмомали.

В разное время таджикских пользователей также лишали доступа к таким ресурсам, как Facebook, Twitter и «ВКонтакте», а также сайтам vesti.ru, gazeta.ru, fergana.ru, сайтам РИА «Новости» и британской корпорации BBC ***(Власти Таджикистана вновь заблокировали доступ к YouTube // InternetUA (http://internetua.com/vlasti-tadjikistana-vnov-zablokirovali-dostup-k-YouTube). – 2014. – 10.06).***

***

Пользователи платёжной системы «Яндекс.Деньги» стали сообщать о визитах полицейских и следователей в связи с финансированием ими деятельности оппозиционера А. Навального. Это произошло через несколько дней после обысков в офисе «Яндекс.Денег».

Бывший гендиректор издательского дома «Коммерсантъ» Д. Кудрявцев сообщил у себя в Facebook, что его пригласили в «отдел по экономическим преступлениям» (видимо, имеется в виду отдел по борьбе с экономическими

преступлениями МВД России). Он пояснил, что там будет устанавливаться, финансировал ли Д. Кудрявцев избирательную кампанию А. Навального, который выдвигался на пост мэра Москвы, и зачем он это делал.

М. Якубов из «Яндекса» написал в комментариях к записи Д. Кудрявцева, что он тоже получил аналогичное приглашение.

В ещё одном посте, который позднее был удалён или скрыт, Д. Кудрявцев пишет, что он обнаружил только один перевод в пользу Навального – в 2011 г. через систему «Яндекс.Деньги». «Яндекс выгрузил просто всю историю кошельков А. Навального и его коллег по фонду, без срока давности и без связи с конкретным делом», – сделал из этого вывод Д. Кудрявцев.

О визите полиции к одному из знакомых рассказал и пользователь Facebook Я. Черняк. В его записи говорится, что полицейский напрямую спрашивал у знакомого, посылал ли он деньги через «Яндекс» А. Навальному, пояснив, что информация об этом получена от интернет-компании.

Спрашивает: «Вы ему деньги с Яндекса посылали?». «А что?». «А они там часть потратили на кампанию, а часть просто распилили. Вот, у нас от Яндекса информация, что Вы (паспортные данные, адрес) посылали ему деньги» – Я. Черняк.

О визите сотрудников правоохранительных органов по аналогичному вопросу к фотографу Д. Смирнову рассказал журналист А. Красовский, а психолог М. Рабинович написала в ЖЖ, что её пригласили на опрос в качестве свидетеля. Об аналогичном приглашении в Следственный комитет сообщил и технический директор компании РН-РН Ф. Казаков.

За две недели до похода полицейских по жертвователям в пользу А. Навального следователи приходили в офис «Яндекс.Денег». Они действовали в рамках уголовного дела о мошенничестве в отношении трёх сторонников оппозиционера, которые собирали через платёжную систему средства на его избирательную кампанию.

В пресс-службе «Яндекс.Денег», 75 % которых владеет «Сбербанк», заявили TJournal, что закон обязывает их выдавать сведения о своих клиентах по первому требованию ряда организаций, в том числе судов и органов предварительного следствия.

Кредитная организация в данном случае – инструмент, который используется в целях расследования, взыскания задолженности и т. п. в зависимости от обращающегося органа, информация попадает в руки указанных лиц, а уж как они ее используют – вопрос компетенции соответствующих служащих.

Мы занимаемся своей работой – осуществляем переводы физических лиц в рамках действующей лицензии, при этом, учитывая сущность данного вида расчетов, как кредитная организация, мы не можем знать характер экономических отношений между отправителем и получателем. Расследования, судебные решения и другие оценки деятельности – это

прерогатива уполномоченных органов, требования которых мы не можем не исполнять в рамках российского законодательства. Единственное, что мы можем делать и делаем в данных условиях – оценивать легитимность запросов, чтобы защитить себя и своих клиентов от произвола – пресс-служба «Яндекс.Денег» ***(Полиция пришла к пожертвовавшим Навальному пользователям «Яндекс.Денег» // InternetUA (http://internetua.com/policiya-prishla-k-pojertvovavshim-navalnomu-polzovatelyam--yandeks-deneg). – 2014. – 10.06).***

***

Управление делами президента России обновило план собственных госзакупок на 2014 г., включив в него сразу несколько заказов на научно-исследовательские работы, посвящённые Интернету. Новая версия утверждённого документа появилась на официальном сайте управления.

Большая часть обозначенных Кремлём тем связана с социальными сетями и обеспечением информационной безопасности страны.

Так, чуть более миллиона рублей планируется выделить на изучение того, как воспринимает распространяемую через соцсети информацию «молодёжная аудитория российского сегмента сети Интернет».

Около 330 тыс. р. администрация президента готова заплатить за работу, посвящённую аспектам регулирования в сети различных агитационных кампаний. В особенности Кремль интересует мировой опыт по регулированию агитации в электронных СМИ.

Гораздо большая сумма – почти два с половиной миллиона рублей – зарезервирована для исследования международно-правовому регулирования использования Интернета в целом. Что именно подразумевается под этой формулировкой, в документе не уточняется.

Ещё два с половиной миллиона управление делами президента потратит на изучение способов борьбы с «информационными кампаниями зарубежных государств». Заказ на работу в этой сфере идёт с пометкой о том, что изучение вопроса необходимо с позиций обеспечения международной безопасности.

Несмотря на то что траты на анализ Интернета и социальных сетей кажутся внушительными, самыми масштабными статьями в документе являются заказы, никак не связанные с IT ***(Кремль потратит миллионы на исследования в области соцсетей и контроля за интернетом // InternetUA (http://internetua.com/kreml-potratit-millioni-na-issledovaniya-v-oblasti-socsetei-i-kontrolya-za-internetom). – 2014. – 10.06).***

***

Частная американская компания CrowdStrike, занимающаяся проблемами интернет-безопасности, обвинила китайских военных в проведении масштабных хакерских операций, целью которых были американские спутниковые и воздушно-космические программы.

9 июня CrowdStrike опубликовала отчет, в котором, в частности, сообщается, что одна из воинских частей Народно-освободительной армии Китая, № 61486, расположенная в Шанхае, вела хакерские атаки против правительственных учреждений и фирм-подрядчиков Министерства обороны США, начиная с 2007 г.

По данным аналитиков, основной целью кибершпионажа со стороны Китая стали космическая и воздушно-космическая отрасли, а также сфера информационных технологий. Так, для кибершпионажа использовались популярные офисные приложения, например Adobe Reader и Microsoft Office, с помощью которых хакерские программы устанавливались на компьютеры пользователей.

Напомним, что в мае власти США уже обвиняли китайских военных в кибершпионаже. Тогда генпрокурор США Э. Холдер сообщил, что его ведомство предъявило обвинения пятерым военным из КНР, которые похищали данные с компьютеров ряда американских коммерческих фирм. Китайская сторона отвергла обвинения, выдвинула собственные и приняла ряд ответных мер в области поставок коммуникационного оборудования ***(В США вновь обвинили Китай в кибершпионаже // InternetUA (http://internetua.com/v-ssha-vnov-obvinili-kitai-v-kibershpionaje). – 2014. – 11.06).***

***

Агентство национальной безопасности США (АНБ) использует уязвимость в iPhone от Apple, которая позволяет следить за людьми, даже если мобильное устройство выключено.

Э. Сноуден сообщил, что АНБ может получить доступ к iPhone, дистанционно включить его и запустить приложения. Пресс-служба компании Apple опровергла заявление, ссылаясь на то, что iPhone был разработан С. Джобсом и является невзламываемым и безопасным. Представители компании никоим образом не прокомментировали тот факт, что экспертам необходимо меньше минуты, чтобы проникнуть в iPhone.

Некоторые хакеры заявляют, что получить доступ к iPhone очень легко. Все, что нужно сделать злоумышленникам – это заставить пользователя обманным путем установить вредоносное ПО на iPhone. Вредоносная программа имитирует выключение телефона, демонстрируя уведомление «проведите по экрану для выключения».

Вместо выключения, телефон переходит в режим низкого энергопотребления, оставляя функционирующей интегральную микросхему, которая ответственна за передачу данных.

АНБ может установить программное обеспечение еще до покупки мобильного устройства. Напомним, что АНБ уже обвинялось в установке бэкдоров на роутерах Cisco.

Как бы там ни было, полностью отключить iPhone возможно. Для этого необходимо включить обновление девайса до заводских настроек (DFU),

чтобы позволить мобильному устройству переустановить прошивку или восстановить операционную систему после неоднократных ошибок.

В режиме DFU все элементы телефона, за исключением USB порта, который разработан для приема сигнала iTunes, чтобы установить новое программное обеспечение, выключаются ***(АНБ США следит за пользователями iPhone // InternetUA (http://internetua.com/anb-ssha-sledit-za-polzovatelyami-iPhone). – 2014. – 11.06).***

***

Руководство непризнанной Донецкой республики потребовало от местных провайдеров предоставить регистрационные данные своих пользователей, сообщил «Изданию» один из представителей рынка, сообщают «Экономические известия» (http://news.eizvestia.com/news_politics/full/646-v-dnr-trebuyut-ot-provajderov-informaciyu-ob-internet-polzovatelyah).

По словам провайдера, ему и его коллегам было разослано письмо за подписью одного из лидеров ДНР Д. Пушилина, в котором содержится требование указать практически всё о действиях пользователей в Интернете: логин, адреса электронной почты, списки контактов, действия по удалению аккаунтов.

«Делается это с целью выявить противников ДНР, тех, кто критикует происходящее на Донбассе, и каким-то образом наказать их. А также, мы так понимаем, составить список потенциальных рекрутов, которых можно “обработать” и привлечь на выполнение каких-то задач», – говорит представитель провайдера. Кроме того, от интернет-компаний требуют сведения о том, когда и какие именно интернет-форумы и социальные сети посещают пользователи, какие ведут блоги и какие программы и DNS-серверы при этом используют.

Со своей стороны собеседник «Издания» выразил нежелание нарушать права пользователей и намерен бойкотировать требования сепаратистов, однако при этом подчеркнул, что опасается за свой бизнес и за свою жизнь. Как известно, ранее руководство ДНР потребовало прекратить с 1 июня ретрансляцию шести украинских телеканалов «в связи с распространением …информации, направленной на разжигание вражды между русским и украинским народом». В случае отказа выполнить это требование представители сепаратистов, как говорится в официальном обращении, не гарантируют «сохранность имущества Вашего предприятия и безопасность персонала» ***(В «ДНР» требуют от провайдеров информацию об интернет-пользователях // Экономические известия (http://news.eizvestia.com/news_politics/full/646-v-dnr-trebuyut-ot-provajderov-informaciyu-ob-internet-polzovatelyah). – 2014. – 13.06).***

***

Блог-платформа «Живой Журнал» заморозила аккаунт украинской блогерши, бывшего редактора украинского ЖЖ, которая собирала средства в поддержку украинской армии, передает корреспондент proIT.

Конфликтная комиссия LiveJournal от лица владельца российского LiveJournal «Рамблер-Афиша-СУП» заблокировала аккаунт бывшего редактора украинской блогосферы – Д. Макаровой и перевела ее блог в режим «только для чтения». Причиной блокировки блога стал якобы «сбор финансовых средств на незаконные цели и публикация инструкций по обращению с оружием».

Под «сбором средств на незаконные цели» подразумевается финансовая помощь вооруженным силам Украины, которая координировалась через блог Д. Макаровой (в ЖЖ – Леди Ди). В частности, экс-редактор украинского ЖЖ публиковала реквизиты для сбора денег в помощь Майдану, украинской армии, Национальной гвардии, Самообороне востока и юга Украины, пострадавшим во время противостояний, а также полные отчеты по финансовой помощи и закупкам.

СУП направил на почту Д. Макаровой три «письма счастья», в которых предупреждал о блокировании записей и запрещал разглашать любые сведения из этих писем (смотреть ниже).

Уважаемый пользователь,

Нам стало известно, что в своей записи http://diana-ledi.livejournal.com/909251.html вы осуществляли сбор финансовых средств на незаконные цели. Такие действия являются нарушением Пользовательского соглашения Живого Журнала (http://www.livejournal.com/abuse/policy-russian-translation.bml#illegal). По этой причине запись была заблокирована администрацией ресурса. Пожалуйста, учтите, что повторение подобного нарушения приведет к принятию более серьезных мер в отношении вашего аккаунта.

С уважением,

Конфликтная комиссия Живого Журнала

ПРЕДУПРЕЖДЕНИЕ: В этом письме содержится конфиденциальная информация, и публикация его в Живом Журнале является нарушением Пользовательского соглашения. Любое воспроизведение этого письма вместе с этим предупреждением или без него может служить основанием для немедленного прекращения действия журнала, в котором оно будет опубликовано, а также вашего собственного журнала» .

Экс-редактор украинского ЖЖ настаивает, что после первого предупреждения СУПа не опубликовала ни одной записи, а также отрицает публикацию каких-либо инструкций по использованию оружия. Д. Макарова также заявляет, что не нарушала пользовательских соглашений с ЖЖ и приводит примеры блогеров, собирающих средства на финансирование сепаратистов. «Это ты [Конфликтная Комиссия] о посте, где говорится о коллиматорных прицелах? – посте, построенном на вытяжках из Википедии

и страйкбольного опыта? Или это ты о постах, в которых я рассказываю о бронежилетах? Хорошенькое оружие», – пишет Д. Макарова в Facebook.

Отметим, Конфликтная комиссия в письме ссылается на нарушение в части публикации незаконных материалов, а именно попыток приобрести или продать товары, распространение которых запрещено законом или публикация записей с призывами нарушать закон. «В случае публикации материалов, незаконных по своей природе, таких как, попытки приобрести или продать товары, распространение которых запрещено законом, доступ к этой записи будет прекращен. Публикация материалов, в которых автор призывает, инструктирует или поощряет других нарушать закон, приведут к блокировке доступа к записи. Если Конфликтная комиссия принимает решение, что незаконные действия, описанные в журнале, могут нанести необратимый вред, действие аккаунта может быть прекращено навсегда», – сообщается в правилах работы комиссии.

В настоящее время Д. Макарова скопировала архивные записи блога на dreamwidth.org и объявила об уходе из ЖЖ ***(«СУП» заблокировал аккаунт экс-редактора украинского ЖЖ за содействие ВСУ // proIT (http://proit.com.ua/news/internet/2014/06/11/115707.html). – 2014. – 11.06).***

***

6 июня в Вашингтоне, округ Колумбия, состоялась презентация операционной системы Tails 1.0, призванной бороться со слежкой, цензурой и блокировкой сайтов. Корреспондент TJournal побывала на мероприятии и выяснила особенности операционной системы.

Благодаря Tails, новой операционной системе, разработанной международной командной волонтёров, активисты по всему миру получат простой и безопасный инструмент, дающий доступ к заблокированным сайтам и охраняющий приватность пользователей.

Если какой-либо сайт заблокирован в определённой стране, Tails (The Amnesic Incognito Live System) позволяет просмотреть его, перенаправляя трафик через несколько стран по сети Tor, так что изначальное местоположение пользователя теряется в процессе. В результате все сайты открываются без проблем, а вычислить, кто на них заходил, не представляется возможным.

6 июня активистам и журналистам довелось увидеть Tails в действии на мероприятии по случаю релиза версии 1.0, организованном Национальным демократическим институтом (NDI) в Вашингтоне, округ Колумбия.

Tails – это операционная система, которая загружается прямо с флешки, DVD или даже карточки SD. У неё есть встроенный браузер, клиенты электронной почты и мгновенных сообщений, пакет офисных программ и графические редакторы. Таким образом, в Tails пользователи могут решать большинство задач, к которым они привыкли в обычной операционной системе, но намного безопаснее.

Ради удобства пользователя, Tails может даже замаскироваться под Windows XP. При загрузке системы можно выбрать нужную опцию, и тогда экран будет выглядеть как старый добрый XP (включая классические обои «Безмятежность»). Это полезно, когда систему нужно использовать в публичном месте – например, в кафе – и не привлекать лишнего внимания.

Тем не менее, используя Tails, рекомендуется следовать общим правилам интернет-безопасности. Например, в то время как система позволяет войти в Facebook или Twitter, даже если они заблокированы в стране, государство всё ещё может отследить, что люди пишут в сети. В этом случае ответственность за сохранность анонимности пользователя в социальных сетях полностью ложится на него самого. Кроме того, хотя сама система и не оставляет следов использования на компьютере, все файлы придётся сохранять на отдельную флешку – в идеальном случае, которую можно легко спрятать или уничтожить.

Программное обеспечение создано на базе GNU/Linux и доступно для бесплатно загрузки. Создатели Tails очень гордятся тем, что использование системы не требует специальных навыков программирования: если пользователь имел опыт с Windows или Mac OS, он сможет работать с Tails. Эта система – современное и всеобъемлющее решение для журналистов, гражданских активистов и пользователей, желающих получить беспрепятственный доступ к информации и одновременно сохранить приватность ***(В США выпустили «антиправительственную» операционную систему Tails // InternetUA (http://internetua.com/v-ssha-vipustili--antipravitelstvennuua--operacionnuua-sistemu-Tails). – 2014. – 10.06).***

***

Специалисты из Oxford Internet Institute нанесли на карту данные Tor о том, сколько пользователей со всего мира используют эту анонимную сеть. Данные были получены на основе открытых источников Tor Metrics Portal за период с августа 2012 г. по июль 2013 г., после которого вредонос Sefnit начал использовать Tor для своих коммуникаций, что мешает сбору статистики реальных пользователей Tor.

По этим данным, украинцы достаточно активно используют Tor. Наша страна находится в третьем ряду стран по количеству пользователей сети на 100 тыс. интернет-пользователей, с показателем от 50 до 100 анонимных пользователей. По абсолютным показателем Украина отстает только от нескольких лидеров с около 10 тыс. пользователей Tor в день.

Самыми «анонимными» странами оказались Италия, Молдова и Израиль (более 200 пользователей Tor на 100 тыс.), меньше всего заботятся об анонимности жители Японии, Бразилии, Мексики, Турции и Китая. По абсолютному числу пользователей Tor лидируют США, Германия, Италия, Франция и Испания ***(Сетью Tor пользуется около 10 тыс. украинцев в день // InternetUA (http://internetua.com/setua-Tor-polzuetsya-okolo-10-tis--ukraincev-v-den). – 2014. – 13.06).***

***

Иракские власти закрыли доступ к социальной сети Facebook. Как сообщил телеканал «Аль-Арабия», на такой шаг правительство пошло в связи с обострившейся обстановкой в стране. Экстремисты могут использовать соцсеть в своих целях, уверены власти.

Всего за несколько дней боевики-сунниты из группировки «Исламское государство Ирака и Леванта», воюющие против шиитского правительства, захватили Тикрит, Мосул и другие города на севере Ирака ***(Власти Ирака закрыли доступ к Facebook из-за боевиков // InternetUA (http://internetua.com/vlasti-iraka-zakrili-dostup-k-Facebook-iz-za-boevikov). – 2014. – 15.06).***

***

Существуют ли программы анти-шпионы для мобильных устройств? Да, существуют, и при этом очень даже эффективные, а начнем мы с бесплатных приложений для iOS и Android, а также попробуем разобраться, где их действительно стоит применять, а где не нужно этого делать.

1. RedPhone (Android)

Бесплатное приложение с открытым кодом, которое позволяет совершать нерегистрируемые телефонные звонки на другие номера пользователей RedPhone через канал передачи данных. Программа шифрует голос так, что даже, если перехватить разговор, например, это может сделать госслужба с помощью СОРМ (Система технических средств для обеспечения функций оперативно-розыскных мероприятий), его невозможно будет расшифровать. Однако RedPhone работает только с телефонами на которых она установлена, то есть у собеседника также должно быть активировано приложение. Таким образом, вы получаете безопасное зашифрованное соединение при звонке, для которого не нужны излишние «проволочки» типа PIN-кодов, идентификаторов и прочих инструментов. Самые параноидальные пользователи даже могут просмотреть код RedPhone, если сами хотят убедиться в его безопасности.

2. TextSecure (Android)

TextSecure является хорошим дополнением к RedPhone – это текстовый мессенджер на основе открытого кода, который позволяет пользователям приложения посылать шифрованные сообщения другим пользователям TextSecure по сети Wi-Fi или мобильному соединению. Кроме базовых текстовых сообщений, TextSecure также предлагает опцию группового чата и поддержку пересылки мультимедийных файлов, чтобы компенсировать функциональность MMS. Как и в случае с RedPhone, исходный код бесплатного TextSecure доступен для пользователей, которым нужно убедиться в его безопасности.

3.Wickr (Android, iOS)

Бесплатный секретный мессенджер Wickr обеспечивает пересылку секретных шифрованных и самоуничтожающихся сообщений (текст, фото, видео, голосовые данные) другим контактам сети Wickr. Сообщения, отправленные через Wickr, не содержат имен и геолокационных данных отправителя и получателя и не хранятся на серверах. Вы сами выбираете, через сколько секунд, минут или часов сообщение удалится с аппарата вашего адресата. Разработчик дорожит своей репутацией, поэтому серьезно относится к вопросу безопасности пользователей, используя шифрование военного уровня и удаляя такие метаданные, как время и место отправки сообщения. Инструмент Secure Shredder (Безопасный шредер) позволяет безопасным образом удалять файловые вложения, сообщения и другие данные, без возможности дальнейшего восстановления. В Wickr вы можете придумать себе любое имя пользователя и в целом остаетесь полностью анонимным при переписке. Однако немного удивительно, что секретный мессенджер интегрируется с Box, Dropbox и Google Drive. Если вы что-то скрываете, мало смысла хранить это в облачном сервисе Google.

4.Telegram (Android, iOS)

Бесплатное мобильное приложение-мессенджер П. Дурова предназначено для особо чувствительных к своей безопасности пользователей. Telegram применяет средства мгновенного шифрования сообщений в секретном чате, а для обычного чата предусмотрено шифрование соединения клиент-сервер. Режим Secure Chat предлагает полное шифрование, то есть читать текст сообщений может только пользователь и его собеседник. Сообщения можно настроить на самоуничтожение, и они будут доступны для прочтения только в течение короткого времени, после чего исчезнет с обоих телефонов. Можно также делиться документами и видео и устраивать групповые чаты с участием до 200 пользователей. Немного истории и статистики: количество пользователей сервиса на март 2014 г. составляет 35 млн человек. В США и некоторых прочих странах мессенджер от основателя «ВКонтакте» обогнал конкурента от Facebook и стал самым скачиваемым бесплатным приложением AppStore в 48 странах мира.

5. OrBot, OrWeb и ChatSecure (Android)

Orbot – это бесплатное прокси-приложение для подключения мобильного устройства к сети Tor. То есть, используя Tor, через прокси-соединение (например, в Facebook) можно выходить в сеть анонимно. Orbot можно комбинировать с Orweb для анонимного интернет-серфинга или с ChatSecure для приватного чата через сеть маршрутизаторов Tor. Кроме того, обладатели разблокированных (Root) устройств на Android могут пропускать весь интернет-трафик через Tor. Напомним, Tor – это кроссплатформенное ПО с открытым исходным кодом, задачей которого является защита от «прослушивания» и обеспечение конфиденциальности персональных и деловых данных, передаваемых в глобальной сети. Продукт обеспечивает полную анонимность клиентов при посещении веб-сайтов, публикации

материалов, отправке сообщений и работе с приложениями, использующими протокол TCP. Пользователям платформы Android уже предоставлялась возможность использования прокси-сетей Tor для анонимного серфинга – некоторое время назад группа исследователей из Кембриджского университета выпустила продукт под названием Shadow. Новое приложение Orbot представляет собой официальную версию Tor-клиента от создателей платформы, при этом абсолютно бесплатную.

6. Ghostery (iOS)

Дополнение к браузеру, которое предназначено для обеспечения конфиденциальности, мгновенно стало хитом среди пользователей ПК, которым важная анонимность. Также решение доступно в версии для устройств iOS в качестве альтернативного браузера. Ghostery позволяет пользователям просматривать то, что сам разработчик называет «невидимый Интернет»: отслеживающие cookie-файлы, веб-жучки, следящие пиксели и все вещи, которые есть на вооружении рекламных компаний для отслеживания активности интернет-пользователя. Помимо этого, Ghostery отображает дополнительную информацию об этих рекламных сетях, в том числе ссылки на политики конфиденциальности, используемые в компаниях и многие другие опции. Ghostery даже доступно как расширение мобильного браузера Firefox Mobile и Chrome. Вот, пожалуй, все самые интересные бесплатные приложения, защищающие вас от контроля извне и шифрующие данные. Однако существуют и платные сервисы, которые имеют более серьезный арсенал инструментов для вашей защиты.

7. Silent Circle (Android, iOS) от 9,95 дол. вмесяц

Silent Circle предлагает пользователям полный набор инструментов для пересылки защищённых приложений, совершения звонков и видеозвонков, а также отправки файлов. Silent Phone, доступный для устройств Android и iOS, предлагает шифрование звонков, как голосовых, так и по видеосвязи, а Silent Text обеспечивает передачу самоуничтожающихся сообщений и файлов объёмом до 100 Мбайт. Ключи шифрования хранятся только у пользователей, а не у разработчиков Silent Circle, то есть, даже если секретные сообщения и проходят через их сервера, прочитать их никто не сможет. Можно расширить тарифный план Silent Circle дополнительным приложением Out-Circle Access, которое позволит не только совершать и получать зашифрованные звонки от других подписчиков, но и добавит возможность соединения с остальными контактами на их сотовые и стационарные телефоны.

8. Onion Browser (iOS) от 0,99 дол.

Onion Browser – это мобильный браузер для iOS, позволяющий пользователю попасть в анонимную сеть Tor. Однако помните, что вам придется жертвовать скоростью интернет-соединения ради вашей безопасности. Приложение позволяет скрыть детали того, какое устройство использует владелец, а средства контроля за cookie-файлами и «быстрые» IP-адреса сделают пребывание в Интернете безопасным.

Заключение

В законности и должной эффективности RedPhone мы сомневаемся, но «побаловаться» можно. Однако увлекаться не стоит, так как, даже не имея корыстных намерений, вы можете привлечь внимание правоохранительных органов. TextSecure больше подойдет «заговорщикам» в пределах офисного помещения, то есть отлично зашифрует сплетни по поводу начальства или позволит сообщить, когда ваш босс «покинул здание».

Wickr тоже отлично подойдет для обмена конфиденциальной информацией с вашим деловым партнером или коллегой по работе, впрочем, как и Telegram. OrBot, OrWeb и ChatSecure для Android – оптимальный набор программ, удовлетворяющий потребности всех категорий пользователей. Ghostery – отличное решение, если вам надоели рекламные компании для отслеживания активности интернет-пользователя, а вот платный сервис Silent Circle на любителя, так как направлен в основном на зарубежного клиента. Мы, по крайней мере, в восторг от этого решения не пришли, как и не увидели особых преимуществ Onion Browser, за которые хотелось бы платить деньги.

В заключении хочется вам посоветовать, не использовать эти приложения в корыстных целях или скрывать преступления, а что еще хуже, их замышлять. Все-таки государственные службы не настолько наивны, чтобы не знать о этих ухищрениях и не иметь меры воздействия на разработчиков. Личная информация и коммерческая тайна, которая касается только вас – священное ваше право, которое не должно нарушать даже государство. В этом случае, эти приложения вам очень помогут, но не стоит быть излишне подозрительным – это портит нервы и вам, и другим. Есть отличная поговорка по этому поводу: «если хочешь что-то спрятать – оставь это на виду» ***(8 мобильных программ-антишпионов для избавления от назойливой опеки спецслужб // InternetUA (http://internetua.com/8-mobilnih-programm-antishpionov-dlya-izbavleniya-ot-nazoilivoi-opeki-specslujb). – 2014. – 8.06).***

Проблема захисту даних. DDOS та вірусні атаки

Злоумышленники эксплуатируют уязвимость в Adobe Flash Player для похищения финансовых данных пользователей из Японии. Кроме того, согласно информации Symantec, жертвы находятся и в ряде других стран, в том числе в США.

По данным ИБ-экспертов, в конце апреля текущего года брешь, позволяющая удаленному пользователю выполнить произвольный код на целевой системе, эксплуатировалась исключительно для атак на отдельные организации и предприятия.

В настоящее время атаки, как правило, осуществляются посредством скрытой загрузки и скомпрометированных сайтов, которые содержат

вредоносный код. Эти веб-сайты затем перенаправляют пользователей на созданный злоумышленником вредоносный ресурс с IP-адресом 1.234.35.42.

Известно, что на территории Японии злоумышленникам удалось взломать следующие три сайта: his-jp.com (туристическое агентство), jugem.jp (сервис блогов), pandora.tv (видео сервис). Кроме того, уязвимыми являются блоги, которые задействуют JUGEM.

Если на системе жертвы установлена устаревшая версия ПО, то будет выполнено несколько вредоносных файлов для компрометации компьютера вирусом Infostealer.Bankeiya.B, который похищает банковскую информацию от пользователей ***(Эксплоит для уязвимости в Adobe Flash используют для хищения финансовых даннях // InternetUA (http://internetua.com/eksploit-dlya-uyazvimosti-v-Adobe-Flash-ispolzuuat-dlya-hisxeniya-finansovih-dannih). – 2014. – 1.06).***

***

Антивирусная компания PandaLabs опубликовала отчёт за I квартал 2014 г. по количеству новых вирусов. Цифры поражают воображение: за три месяца зарегистрировано более 15 млн образцов новых зловредов, то есть каждый день создаётся около 16 000 штук!

Из этого количества 71,85 % составляют трояны, они ответственны за 79,9 % всех заражений на компьютерах пользователей.

По нформации PandaLabs, зловреды проникли на каждый третий телефон. По этому показателю лидирует Китай, где вредоносное программное обеспечение установлено более чем на половине устройств (52,36 %) ***(Установлен рекорд по числу новых зловредов: 160 000 в день // InternetUA (http://internetua.com/ustanovlen-rekord-po-csislu-novih-zlovredov--160-000-v-den). – 2014. – 2.06).***

***

Злоумышленники, используя вредоносное программное обеспечение Gameover Zeus и Cryptolocker, в течение длительного времени осуществляли хакерские атаки на сайты ведущих финансовых учреждений мира, в том числе и Украины. В результате похищали денежные средства их клиентов.

Работники Управления по борьбе с киберпреступностью недавно завершили проведение украинского этапа международной спецоперации по обезвреживанию данной группы.

Gameover Zeus, также известный как Peer-to-Peer Zeus – это последняя версия вредоносного программного обеспечения Zeus, что появилось в 2007 г. По имеющейся информации, разработчиком троянской программы является гражданин Российской Федерации. Злоумышленник организовал вокруг себя более 20 хакеров со всего мира и с помощью указанного ботнета похищал личные данные пользователей.

По выводам экспертов в области кибербезопасности, около миллиона компьютеров по всему миру, в том числе более 60 тыс. на территории

Украины, были инфицированы вирусом Gameover Zeus. Ущерб от противоправной деятельности оцениваются примерно в 75 млн евро.

Управление деятельностью указанной бот-сети было построено по новейшим технологиям и базировалось на сочетании иерархической и пиринговой структур – инфицированные узлы получали ключевые команды от управляющих серверов и массово распространяли эту информацию между собой. Указанная технология чрезвычайно затрудняла процесс документирования противоправной деятельности преступной группы и обезвреживания вредоносного программного обеспечения.

Во время расследования установлено, что управление бот-нетом осуществлялось посредством более 10 серверов, которые размещались на абюзозащищенной площадке одного из хостинг-провайдеров г. Одесса. С целью конспирации киберпреступники зарегистрировали указанную сеть на подставную компанию и, используя специфические протоколы маршрутизации, скрыли истинное место размещения сетевого оборудования.

7 апреля этого года сотрудники УБК начали проведение международной операции по обезвреживанию участников преступной группы Gameover Zeus. Вслед за Украиной аналогичные мероприятия проводились на территории Соединенных Штатов Америки, Великобритании, Нидерландов, Германии, Японии и ряда других стран.

В ходе проведения украинского этапа спецоперации был проведен ряд санкционированных обысков. Во время мероприятий изъято 13 единиц компьютерной техники и сетевого оборудования, которые использовались для администрирования и разработки вредоносного программного обеспечения, а также получены копии управленческих серверов бот-сети.

Впоследствии правоохранители установили, что один из граждан Украины был причастен к разработке ядра всей инфраструктуры бот-сети – серверу, который выполнял функцию инфицирования персональных компьютеров и сбора банковской информации из них. Также идентифицирован житель столицы, который организовал разветвленную сеть подставных лиц для легализации средств, полученных преступным путем.

30 мая этого года был проведен завершающий этап по обезвреживанию сети Gameover Zeus и Cryptolocker. Мероприятия проводились на территории Канады, Франции, Италии, Японии, Люксембурга, Германии, Новой Зеландии, Нидерландов, Украины и Великобритании. С целью координации и согласованных действий по спецоперации, на базе Европейского центра по противодействию киберпреступности (EC3) в Европоле была организована деятельность координационного штаба, участие в котором принял также сотрудник Управления по борьбе с киберпреступностью МВД Украины.

Проведение спецоперации началось с получения правоохранительными органами Великобритании и США контроля над более 2000 доменными именами, которые использовались для управления инфицированными компьютерами. После этого были заблокированы главные серверы и маршрутизаторы бот-нета, которые размещались на защищенном хостинге в

Украине. При таких обстоятельствах многомиллионная сеть инфицированных компьютеров осталась без командного центра. Следовательно, им было отправлено команду на самоликвидацию ***(Правоохранители обезвредили международную преступную группу хакеров // Час Пик (http://vchaspik.ua/kriminal/264200pravoohraniteli-obezvredili-mezhdunarodnuyu-prestupnuyu-gruppu-hakerov). – 2014. – 3.06).***

***

Українські хакери продовжують боротися проти російської пропаганди на терористичних веб-сайтах. Днями було здійснено DDoS-атаки на офіційні сайти терористичних організацій – ДНР та ЛНР.

Унаслідок кількаденної атаки, яка тривала з 28 до 31 травня, сайти істотно сповільнили свою роботу, а вже 31 травня хостер закрив donetsk-gov.su через великі навантаження на його інфраструктуру, яке виникло внаслідок постійних DDoS-атак на сайт ***(Внаслідок DDoS-атак українських хакерів, закрився офіційний сайт терористичної організації ДНР // InternetUA (http://internetua.com/vnasl-dok-DDoS-atak-ukra-nskih-haker-v--zakrivsya-of-c-inii-sait-teroristicsno--organ-zac---dnr). – 2014. – 3.06).***

***

Десятка мощных хакерских атак на российские сайты весной 2014 г.

За первые пять месяцев 2014 г. сайты российских госорганов, госкомпаний и банков подверглись рекордному числу хакерских атак. Всплеск DDoS-атак пришелся на март. Эксперты, опрошенные газетой «Ведомости», говорят, что активность хакеров вызвана ухудшением отношений между Украиной и Россией.

За два дня до проведения референдума о статусе Крыма, проходившего 16 марта, «упали» сайты президента России, Министерства иностранных дел и Роскомнадзора.

В «Лаборатории Касперского» сообщают, что в ходе весенней волны DDoS-атак в России пострадали более 15 организаций.

Вряд ли это заслуга только украинских программистов. В «Лаборатории Касперского» говорят, что атак с украинских IP-адресов в этом году не фиксировали. «Страну – первоисточник атак установить сложно, так как они зачастую идут с подменой адреса отправителя», – рассказал менеджер по развитию бизнеса Kaspersky DDoS Prevention Е. Виговский.

За большинство онлайн-нападений ответственность взяли группы хакеров Anonymous Russia и Anonymous Caucasus. «Когда правительство нарушает права народа, восстание для народа и для каждой его части есть его священнейшее право и неотложная обязанность», – написали Anonymous Russia в своем Twitter-аккаунте.

Кроме госорганов, силовых ведомств и госкомпаний атакам подверглись и ряд крупных российских СМИ: Первый канал, Russia Today, Lifenews, Комсомольская правда, Лента.Ру.

Для того чтобы провести DDoS-атаку на сайт, не нужно быть «матерым» программистом. Такую услугу можно заказать за 135 дол. даже в открытом сегменте Интернета. Стоимость зависит от длительности и мощности атаки, а также защиты, которую нужно преодолеть на сервере. В отличие от целенаправленного взлома с изъятием информации DDoS быстро и дешево нарушает работу крупных ресурсов.

Anonymous – международная группа хакеров, основанная в 2003 г. Ее участники устраивают кибератаки и взломы в знак протеста. В 2012 г. американский журнал Time включил Anonymous в список ста наиболее влиятельных людей года.

ЛІГАБізнесІнформ выбрала самые резонансные случаи DDoS-атак на российские сайты в 2014 г.

6 марта 2014 г.

Группа хакеров Anonymous Russia взломала серверы нескольких военных предприятий. Они выложили в сеть переписку руководителей Рособоронэкспорта с индийскими оборонными компаниями. Анонимусы также заявили, что завладели документами Оборонпрома, корпорации Сухой, Газфлота и РусАла.

14 марта 2014 г. – kremlin.ru

Сайт президента России kremlin.ru подвергся мощной DDOS-атаке, в результате которой несколько часов работал с перебоями. В этот же день под удар попал и сайт Центрального банка Российской Федерации. Ответственность на себя взяли хакеры Anonymous Russia.

14 марта 2014 г. – cbr.ru

Из-за мощной хакерской атаки сайт Центрального банка России перестал отображаться у пользователей. По данным банка, мощность ддоса превышала пропускную способность каналов связи сайта в 10 раз. Работа ресурса была восстановлена через час.

14 марта 2014 г. – iacis.ru

Сайт Межпарламентской ассамблеи государств – участников СНГ подвергся DDOS-атаке.

На сервер одновременно поступали порядка 3000 запросов, в результате ресурс не выдержал нагрузки и «лег». Для атаки были задействованы ботнеты – сеть зараженных компьютеров, расположенных в разных точках мира.

В этот же день жертвой DDoS-атак стал и сайт Министерства иностранных дел Российской Федерации (mid.ru). Ответственность взяли на себя Anonymous Russia.

14 марта 2014 г. – rkn.gov.ru

Сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций из-за мощной DDoS-атаки временно был отключен. Группа хакеров после атаки в своем Twitter пошутила, что Роскомнадзор запретил сам себя.

16 марта 2014 г. – referendum2014.ru

DDoS-атака на сайт, посвященный референдуму о статусе Крыма. Источник атак, по предположению пресс-службы, находился в Иллинойском университете в США. До этого хакеры «завалили» официальный сайт референдума referendum2014.org.ua. В настоящее время оба сайта не функционируют.

17 марта 2014 г. – alfabank.ru

Хакеры Anonymous Caucasus заддосили сайт российского Альфа-Банка и его провайдера. Была недоступна часть банкоматной сети и затруднен доступ к его интернет-сервисам, включая сайт.

Информацию о нарушении работы транслировали Anonymous Caucasus.

17 марта 2014 г. – vtb24.ru

В этот же день был атакован один из крупнейших российских банков ВТБ24. Хакерам удалось «положить» сайт, но на финансовых операциях атака никак не отразилась – все банкоматы и карты пользователей работали в обычном режиме. Ответственность за взлом взяли на себя Anonymous Caucasus.

11 апреля 2014 г. – komitet2-1.km.duma.gov.ru

В апреле был взломан сайт комитета Госдумы по региональной политике и проблемам Севера и Дальнего Востока. Взломщики разместили манифест, критикующий внешнюю политику России. Сообщение заканчивалось словами «Слава Украине!»

15 апреля 2014 г. – russian.rt.com

Сайт российского информационного телеканала Russia Today был выведен из строя из-за массированной DDoS-атаки. Сайт подвергался нападениям несколько раз в 2013 г., тогда ответственность за них брала хакерская группа AntiLeaks ***(Холодная весна – 2014: хакеры объявили России кибервойну // InternetUA (http://internetua.com/holodnaya-vesna---2014--hakeri-ob-yavili-rossii-kibervoinu). – 2014. – 3.06).***

***

Исследователи Государственного университета Северной Каролины, США, разработали систему, которая может централизованно управлять работой компьютеров, подключённых к сети, во время кибератак.

В первую очередь, система будет защищать от хакерского нападения компьютеры, управляющие энергосетью США. Такая сеть в Америке делится на секторы размером с муниципальные районы или штаты, и каждый управляется определённым компьютерным центром.

В случае успешного осуществления хакерской атаки, система может не только сама выйти из строя, но и повлиять на работу других элементов, подключённых к сети, что породит цепную реакцию.

Новое решение как раз поможет не допустить таких последствий – если один центр выходит из строя, вычислительная нагрузка будет распределена между системами в других центрах.

Таким образом, американцы нашли достаточно надёжный щит, закрывающий опасную цифровую уязвимость в одной из стратегических отраслей промышленности.

В настоящее время учёные ведут полевые испытания новой системы. Предполагается, что на оснащение она может встать уже с 2015 г.

Кстати, недавно эксперты из компании Black Lotus сообщили, что в течение следующих 12–18 месяцев мощность нового вида отражённых распределённых DDoS-атак достигнет 800 Гбит/с ***(В США появилась система защиты энергосетей от хакерских атак // Блог Imena.UA (http://www.imena.ua/blog/defense-cyberattacks-power-grids/). – 2014. – 3.06).***

***

Про появу в Інтернеті нового і небезпечного електронного вірусу попередило Національне бюро по боротьбі із злочинністю Великобританії

«Криптолокер» (Cryptolocker) був виявлений спільними зусиллями американського ФБР та європейськими службами, зокрема, «Європолом». «“Криптолокер” представляє собою нове покоління вірусів, які проникають в комп’ютер і захоплюють всі файли, що знаходяться в ньому, переводячи в особливий закодований формат, – зазначає ВВС. – У результаті власник комп’ютера не може ним більше користуватися і позбувається доступу до власної інформації».

Слідом за цим на уражений вірусом комп’ютер надходить від хакерів послання з пропозицією заплатити один біткоін (300 дол. США за поточним курсом) за те, щоб було відновлено його нормальну роботу.

Британський телеканал Sky News охарактеризував хакерську атаку як «колосальну».

Згідно з даними ФБР США, розробило «Криптолокер» злочинне угруповання, імовірно з однієї з країн Східної Європи, яке вже отримала від постраждалих понад 100 млн дол. При цьому за останні два місяці вірус вразив 234 тис. комп’ютерів у численних країнах світу. Серед інших атакам піддалася страхова компанії в Піттсбурзі, а також поліцейська дільниця в штаті Массачусетс.

Як повідомила інформаційна служба лондонської газети The Daily Telegraph, Міністерство юстиції США офіційно назвало 3 червня Є. Богачева як главу «злочинного угруповання», відповідального за створення й розповсюдження цього вірусу. Фахівці з кібербезпеки рекомендують власникам комп’ютерів терміново оновити свої операційні програми з тим, щоб підвищити ступінь захисту. При цьому слід чітко дотримуватися рекомендації і не відкривати підозрілі електронні листи, у яких найчастіше перебувають віруси ***(Авторам вірусу нового покоління вдалось отримати від жертв більше 100 мільйонів доларів // Espreso.tv (http://espreso.tv/news/2014/06/03/avtoram_virusu_novoho_pokolinnya_vdalos_otrymaty_vid_zhertv_bilshe_100_milyoniv_dolariv). – 2014. – 3.06).***

***

Как сообщил ИБ-исследователь @claudijd, несколько месяцев назад он хотел проэксплуатировать XSS-уязвимость CVE-2013-3414 в Cisco ASA WebVPN для сканера TrustKeeper Scan Engine. Он испробовал различные техники на разных версиях ASA, однако так и не добился желаемого результата. Исследователь обратился к своему коллеге из SpiderLabs П. Каролаку, который практически сразу после обращения @claudijd проэксплуатировал уязвимость.

Cisco описала брешь следующим образом: «Уязвимость на странице авторизации на портале WebVPN позволяет неавторизованному удаленному пользователю осуществить атаку межсайтового скриптинга или взломать сессию пользователя. Данная брешь является результатом неспособности правильно проверить вводимые пользователем данные на странице авторизации портала WebVPN. Атакующий может эксплуатировать эту брешь, заставив пользователя пройти по заранее созданному URL».

В ходе тестирования исследователи убедились, что полезная нагрузка XSS выполняет Javascript в Internet Explorer 6.0 (более новые версии браузера уязвимость не затронула). Они добавили TrustKeeper Scan Engine и посчитали, что дело завершено.

Тем не менее, через месяц с @claudijd связалась эксперт из SpiderLabs Х. Пилкингтон, которая в ходе своих тестов обнаружила эту же брешь в полностью обновленном Cisco ASA. Эксперты обратились в Cisco, однако в компании заявили, что уязвимость, обнаруженная Х. Пилкингтон, является новой (CVE-2014-2120) ***(Эксперт рассказал об обнаружении уязвимости нулевого дня в Cisco ASA // InternetUA (http://internetua.com/ekspert-rasskazal-ob-obnarujenii-uyazvimosti-nulevogo-dnya-v-Cisco-ASA). – 2014. – 3.06).***

***

Интернет-компания Google получила более 41 тыс. запросов от европейских пользователей на удаление их личных данных из поиска за четыре дня с момента запуска соответствующего сервиса. Об этом сообщает газета The Financial Times со ссылкой на информированные источники.

Специальная онлайн-форма, через которую европейцы могут указать конкретные нежелательные данные, появилась у Google 30 мая. По данным FT, только за первые сутки после появления инструмента пользователи отправили Google свыше 12 тыс. запросов. Большинство требований поступили из Германии и Великобритании.

Подобный наплыв запросов, многие из которых требуют детальной обработки, может потребовать от Google найма новых сотрудников, пишет издание. Ожидается, что Google начнет выполнять первые требования на удаление данных из поиска в середине июня.

Запустив форму, Google начала выполнять предписание Высшего суда Евросоюза от 13 мая. Это решение стало результатом борьбы сторонников

права на частную жизнь, которые добиваются для пользователей Интернета «права на забвение». Последнее означает возможность стереть информацию о себе в Интернете, которая зачастую может быть устаревшей, неверной или нежелательной к распространению. При отказе поисковика от содействия пользователь может обратиться в суд.

Сама Google относится к решению суда негативно. Главный юрист компании Д. Драммонд заявил, что разбирательство «зашло слишком далеко», и что европейский суд не учел влияние своего решения на свободу слова. По словам гендиректора Google Л. Пейджа, это решение может негативно отразиться на небольших интернет-стартапах и является серьезным ограничением онлайн-коммуникаций.

В то же время Google продолжила предпринимать шаги для защиты личных данных пользователей – на сей раз в переписке. Накануне Google предложила разработчикам протестировать расширение End-to-End для браузера Chrome, которое шифрует сообщения электронной почты. Они кодируются при отправке из браузера, а расшифровываются только при получении адресатом. В результате исключается возможность прочитать сообщение на промежуточных серверах ***(Google получила 40 тысяч запросов на удаление личных даннях // InternetUA (http://internetua.com/Google-polucsila-40-tisyacs-zaprosov-na-udalenie-licsnih-dannih). – 2014. – 4.06).***

***

Эксплоит, применяемый для Heartbleed, может использоваться для атаки на любое устройство с устаревшей версией OpenSSL.

С тех пор как стало известно об уязвимости Heartbleed в криптографической библиотеке OpenSSL, прошло уже около двух месяцев. Реакция сообщества безопасности, поставщиков программного и аппаратного обеспечения, владельцев веб-сайтов, а также интернет-провайдеров была практически незамедлительной.

В настоящее время ажиотаж вокруг бреши немного поутих, и многие уверены, что опасность миновала. Тем не менее, эксперт из SysValue Л. Грангейя сообщил, что забывать о Heartbleed пока рано. Он доказал, что эксплоит Cupid, применяемый для этой бреши, может использоваться для атаки на любое устройство с устаревшей версией OpenSSL. Эксперт сообщил, что атаки с его помощью можно успешно осуществлять как через проводные, так и беспроводные сети.

«Я назвал два исходных патча, которые могут применяться к программам hostapd и wpa_supplicant на Linux, Cupid. Эти патчи модифицируют поведение программы для эксплуатации уязвимости Heartbleed в TLS-соединении на определенных типах защищенных паролем беспроводных сетей», – объяснил Л. Грангейя.

Эксперт пояснил, что это фактически та же атака, что и Heartbleed, основанная на вредоносном пакете heartbeat. Как и при оригинальной атаке

на TLS-соединения через TCP, могут использоваться как клиенты, так и серверы, и память может быть считана на обоих концах соединения. Разница состоит в том, что TLS-соединение осуществляется через механизм EAP, используемый в беспроводных сетях.

«EAP – это всего лишь фреймворк, который используется в нескольких механизмах аутентификации. С этой точки зрения интересными (ред. – для осуществления атаки) являются EAP-PEAP, EAP-TLS и EAP-TTLS, использующие TLS», – отметил Л. Грангейя.

Эксплоит подходит для версий Android 4.1.0 или 4.1.1, Linux-систем, по-прежнему использующих устаревшие версии OpenSSL, а также большинства корпоративных беспроводных решений, поскольку они задействуют механизмы аутентификации, основанные на EAP ***(Эксплоит Cupid может использовать уязвимость Heartbleed в Android и сетях Wi-Fi // InternetUA (http://internetua.com/eksploit-Cupid-mojet-ispolzovat-uyazvimost-Heartbleed-v-Android-i-setyah-Wi-Fi). – 2014. – 4.06).***

***

Компания FireEye обнаружила волну атак, созданную группой злоумышленников из Ближнего Востока и направленную на несколько европейских государственных организаций и по крайней мере одно финансовое учреждение в США. Атаки зафиксированы в период с 29 апреля по 27 мая текущего года, известные как Operation Molerats.

Их жертвами стали правительственные ведомства Израиля, Словении, США, а также Британская вещательная корпорация BBC. «В своих предыдущих кампаниях хакеры Molerats использовали заурядные и доступные бэкдоры – CyberGate и Bifrost. В последнее время мы обнаружили, что злоумышленники используют PIVY (Poison Ivy) и Xtreme RATs», – сообщают в FireEye.

Свои предыдущие атаки злоумышленники осуществляли при помощи поддельных сертификатов Microsoft, это предоставляло исследователям безопасности возможность связать воедино отдельные атаки даже в тех случаях, когда злоумышленники использовали разные бэкдоры. Стоит отметить, что в таких атаках хакеры использовали приманки или ложные документы на английском или арабском языке, в которых содержалась информация о конфликтах на Ближнем Востоке. В документы также внедрялись вредоносные файлы.

За последние несколько лет число кибератак на Ближнем Востоке возросло. В частности, иранские злоумышленники разработали более десятка сайтов, имитирующих такие социальные сети как Facebook и Twitter, использовав их для кибершпионажа ***(Хакеры из Ближнего Востока совершают кибератаки на правительственные ведомства по всему миру // InternetUA (http://internetua.com/hakeri-iz-blijnego-vostoka-sovershauat-kiberataki-na-pravitelstvennie-vedomstva-po-vsemu-miru). – 2014. – 4.06).***

***

Эксперты компании Eset обнаружили вредоносную программу-вымогателя Simplocker для устройств под управлением ОС Android, который шифрует файлы пользователя, а затем требует денежный выкуп за их расшифровку. Такой тип приложений-вымогателей широко распространен на платформе Windows, однако для Android обнаружен впервые, говорится в блоге компании.

Как пояснили «Ленте.ру» в Eset, ранее эксперты обнаружили несколько программ-вымогателей, которые просто блокировали устройство, не зашифровывая файлы на нем. В одном из случаев злоумышленники требовали для разблокировки «купить и установить антивирусное приложение», встречалась также модификация с требованием внести штраф за просмотр нелегального контента, посещение запрещенных сайтов и т. п.

После заражения устройства пользователя вредоносная программа проверяет карту памяти на предмет присутствия картинок, документов или видео, после чего каждый из таких файлов зашифровывается, а доступ к устройству пользователя блокируется.

Далее на экране отображается сообщение о блокировке устройства. Сообщение написано на русском языке, однако требует выплаты выкупа в украинских гривнях, что, по мнению экспертов Eset, предполагает нацеленность вымогателя на Украину.

Злоумышленники предлагают пользователю, устройство которого заблокировано, заплатить выкуп, используя сервис MoneXy, поскольку клиентов этого сервиса не так просто отследить, в отличие от клиентов обычных платежных систем, которые работают с кредитными картами. В сообщении указывается, что после поступления денежных средств на счет злоумышленников устройство будет разблокировано в течение 24 часов.

В случае с Simplocker программа уже содержит код расшифровки файлов, за который пользователю предлагается заплатить, что, однако, не означает, что после оплаты «выкупа» владелец вернет управление устройством.

Вредоносное программное обеспечение (ПО) Simplocker распространялось в виде приложения с именем Sex xionix. Оно не было обнаружено в магазине приложений Google Play и, по мнению экспертов, имеет небольшой уровень распространенности на сегодняшний день, однако платформа Android допускает установку ПО со сторонних ресурсов, где пользователи могли случайно наткнуться на него.

Программа-вымогатель взаимодействует с удаленным сервером и отправляет ему некоторую опознавательную информацию об устройстве, например, идентификатор IMEI. Эксперты отмечают, что адрес сервера относится к домену .onion, который принадлежит анонимной сети TOR, что позволяет злоумышленникам обеспечивать должный уровень скрытности.

«Наш анализ этой угрозы показал, что в случае с Simplocker злоумышленникам удалось приблизиться к реализации концепции

известного вымогателя Cryptolocker, который наделал много шума в мире Windows», – уточнили в Eset ***(Вирус-вымогатель для Android научился шифровать файлы // InternetUA (http://internetua.com/virus-vimogatel-dlya-Android-naucsilsya-shifrovat-faili). – 2014. – 6.06).***

***

Эксперт по вопросам информационной безопасности Д. Броссар заявил о том, что ему удалось обнаружить способ удаленного взлома систем автомобилей. Эксперт уверяет, что в настоящее время еще ни один хакер не использовал его, но «его компания уже делает это для производителей автомобильных средств в Европе».

На конференции Black Hat, которая пройдет в августе текущего года, Д. Броссар расскажет о существующем бэкдоре, позволяющем контролировать компьютерную систему автомобиля удаленно. По словам эксперта, жертвами бэкдора уже стали 2 млн компьютеров по всему миру, включая автомобили австралийских производителей.

Большинство обнаруженных ранее атак на системы автомобилей проводятся через сеть контроллеров Controlled Area Network или электронные блоки управления. В частности, исследователи Ч. Миллер и К. Валашек в прошлом году продемонстрировали, как получить контроль над автомобилем, подключив ноутбук к приборной панели.

Помимо этого, в недавнем отчете CNN Money значатся несколько систем автомобилей с очень низким уровнем безопасности. Эти системы контролируют руль транспортного средства, тормоза и ускорение.

Эксперты отмечают, что основная проблема безопасности компьютерных систем для автомобилей в том, что они не особо отличаются от обычных компьютеров, точно также подключаясь к беспроводной сети и являются мишенью для киберпреступников. Помимо этого, производители автомобилей встраивают надлежащий механизм защиты в программное обеспечение, которым оснащено транспортное средство ***(Ученые нашли способ удаленно взламывать системы автомобилей // InternetUA (http://internetua.com/ucsenie-nashli-sposob-udalenno-vzlamivat-sistemi-avtomobilei). – 2014. – 6.06).***

***

В библиотеке шифрования OpenSSL, которую используют две трети интернет-ресурсов, обнаружили критическую уязвимость, появившуюся еще в первой версии программного пакета – в 1998 г. О баге и его исправлении сообщается 5 июня в бюллетене OpenSSL Foundation, курирующего разработку библиотеки.

Уязвимость нашел японский программист М. Кикути, который написал в своем блоге, что занялся исследованием кода библиотеки после обнаружения другого критического бага – Heartbleed – в начале апреля 2014 г.

Найденный баг позволяет злоумышленнику принудительно менять политику шифрования двух пользователей (или пользователя и сервера) OpenSSL. В этом случае библиотека использует ненадежные ключи для шифрования данных. Если поток таких данных перехвачен (например, прослушиванием трафика беспроводных соединений Wi-Fi), то злоумышленник может впоследствии расшифровать всю переданную информацию.

М. Кикути подчеркнул, что эта серьезная уязвимость не была найдена в течение 16 лет, поскольку исходный код OpenSSL не проходит должную проверку перед открытым распространением для всех желающих.

Ранее значительному количеству интернет-сайтов пришлось обновлять свои версии OpenSSL из-за уязвимости Heartbleed, которая появилась в коде в 2012 г. и в течение двух лет оставалась незамеченной. Баг позволял злоумышленнику отправлять на сервер такие запросы, что в ответ он получал не только данные, касающиеся своего соединения, но и информацию о соединениях других пользователей, в том числе логины, пароли и ключи шифрования.

На момент обнаружения Heartbleed уязвимости были подвержены около 17 % серверов, тогда как библиотеку OpenSSL в том или ином виде используют до 65 % серверов, в том числе и поисковик Google ***(В OpenSSL нашли критическую уязвимость 16-летней давности // InternetUA (http://internetua.com/v-OpenSSL-nashli-kriticseskuua-uyazvimost-16-letnei-davnosti). – 2014. – 6.06).***

***

Представители сообщества Anonymous заявили, что следующей целью атак станут спонсоры Чемпионата Мира по футболу.

Хакер Che Commodore сделал угрожающее заявление в знак солидарности с протестующими против проведения чемпионата мира в Бразилии. Негодование объясняется использованием и вложением финансовых средств в ненужные стадионы, чтобы продемонстрировать образцово-показательный футбольный чемпионат вместо того, чтобы направить их на развитие инфраструктуры и транспортной системы в Бразилии.

«Мы уже провели ряд тестов, согласно данным которых сделали выводы о том, какие веб-сайты являются уязвимыми. У нас есть план атак», – об этом сообщил Reuters Che Commodore.

Он также добавил в беседе по Skype: «Мы планируем осуществить атаку против спонсоров чемпионата мира». Среди потенциальных жертв Che Commodore выделил такие компании как Adidas, авиакомпанию Emirates, Coca-Cola Co и Budweiser.

Предполагается, что Che Commodore является самопровозглашенным участником движения Anonymous Brazil и его учетная запись в Twitter содержит ссылку на англоязычное видео Anonymous # OpHackingCup.

Вице-президент Cloud Solutions в компании SafeNet Д. Харт заявил, что компании, вещатели, а также потребители будут подвергаться кибератакам разного рода.

Он добавил, что этот чемпионат мира будет «самым технологически-ориентированным в мире, поэтому он также станет предметом кибератак и утечек данных, с момента проведения этого спортивного мероприятия в Лондоне в 2012 г.».

Региональный директор McAfee по безопасности сетей А. Патель сообщил, что злоумышленники предположительно внедряют вредоносное ПО в сети спонсоров на протяжении несколько недель, для их дальнейшего запуска ***(Anonymous планирует кибератаки против спонсоров Чемпионата Мира по футболу // InternetUA (http://internetua.com/Anonymous-planiruet-kiberataki-protiv-sponsorov-cempionata-mira-po-futbolu). – 2014. – 10.06).***

***

В ходе исследования эксперты обнаружили очень сложный и эффективный способ заражения большого количества компьютеров вредоносным ПО.

Эксперты из компании Cisco сообщили о том, что в доменах, принадлежащих компаниям Disney и Facebook, а также изданию The Guardian, размещается реклама, которая заражает компьютеры пользователей вредоносным ПО, использующимся для вымогательства денег. Исследователи обнаружили это после масштабной операции по ликвидации ботнета, распространявшего ПО для вымогательства, которую провели американские правоохранители совместно с технологическими компаниями.

В ходе исследования эксперты обнаружили технически очень сложный и эффективный способ заражения большого количества компьютеров вредоносным ПО. Бывший агент секретной службы США Л. Гундерт, который в настоящее время является аналитиком в Cisco, охарактеризовал этот способ как «очень хитрый».

Эксперт сообщил, что у его компании есть инструмент Cloud Web Security (CWS), который следит за тем, какие ресурсы посещают пользователи, и оповещает о том, когда они заходят в подозрительные или вредоносные домены. По словам Л. Гундерта, CWS анализирует миллиарды запросов к различным веб-страницам в день.

В компании сообщили о блокировке запросов к 90 доменам. Исследование экспертов показало, что многие пользователи CWS оказывались в этих доменах после просмотра рекламы на сайтах с большим объемом трафика – apps.facebook.com, awkwardfamilyphotos.com, theguardian.co.uk и go.com (собственность компании Disney).

По словам экспертов, вредоносная реклама является проблемой уже довольно давно. Рекламные сети предприняли шаги, чтобы попытаться обнаружить размещенные в них вредоносные рекламные объявления, но

проверки безопасности не являются абсолютно надежными ***(Реклама в доменах Disney, Facebook и The Guardian является источником вредоносного ПО // InternetUA (http://internetua.com/reklama-v-domenah-Disney--Facebook-i-The-Guardian-yavlyaetsya-istocsnikom-vredonosnogo-po). – 2014. – 8.06).***

***

Збиток, заподіяний світовій спільноті різними кіберзлочинами оцінюється експертами в колосальну суму, що перевищує ВВП багатьох країн. Дослідний центр CSIS (Center for Strategic and International Studies) на замовлення компанії McAfee у сприянні з командою економістів та експертів у галузі інтелектуального права опублікував дослідження, згідно з яким загальний збиток від кіберзлочинів перевищує 400 млрд дол. на рік.

При цьому збиток, що наноситься економіці США, дорівнює 100,4 млрд дол. Ці цифри значно відрізняються від опублікованих раніше в 2013 р., коли загальний збиток для США налічував 781,8 млн дол. Автори дослідження спробували порахувати не тільки прямі втрати, заподіяні кіберзлочинами, але також непрямі, як наприклад, наслідки витоку даних, втрату робочих місць. Згідно з дослідженням, через успішно проведених атак у Європі близько 150 тис. осіб позбулися робочих місць. У США ця цифра досягає 200 тис.

Можливо, це дослідження зможе вплинути на політику багатьох компаній щодо власної безпеки ***(Експерти оцінюють збитки від кіберзлочинів в $400 млрд // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ua/news/2014/06/10/loss-from-cybercrime.html). – 2014. – 10.06).***

***

Хакер, взломавший несколько электронных дорожных табло в США за последние две недели, обратил на себя внимание организаций, занимающихся сетевой безопасностью, посчитавших, что он вдохновлялся игрой Watch Dogs. Об этом сообщает специалист по кибербезопасности Б. Кребс в своём блоге.

Начиная с конца мая, неизвестный злоумышленник под псевдонимом Sun Hacker взламывал дорожные табло, выводя на них своё имя, и даже однажды пригласил очевидцев поболтать с ним в Twitter. По информации департамента транспорта Северной Каролины, всего таким образом хакер взломал пять дорожных знаков по всей стране, а первый случай произошёл 27 мая.

Согласно отчёту организации MS-ISAC (подразделения некоммерческой организации «Центр интернет-безопасности», CIS, анализирующей сетевые угрозы для правительства США), табло были модифицированы выходцем из Саудовской Аравии, ставшим известным за последние несколько лет по серии взломов зарубежных сайтов при помощи

SQL-инъекций. Помимо сайтов, Sun Hacker активно интересуется «интернетом вещей»: он публиковал инструкции по тому, как взломать «умные» лампочки и радио в автомобилях.

По словам экспертов, частично мотивацию злоумышленника подогревало то, что взломать табло было несложно из-за примитивной системы защиты протокола SNMP. Одни из исследователей считают, что он получил доступ через порт 23 по Telnet, так как пароль был несложным для подбора; другие утверждают, что он поменял пароль на модеме, заставив техников сбросить его и вернуться к заводским настройкам.

Однако в отчёте MS-ISAC есть другая, более неожиданная деталь: эксперты считают, что действия Sun Hacker непосредственно связаны с компьютерной игрой Watch Dogs, главный герой которой обладает технологиями взлома практически любого электронного устройства – в том числе светофоров и дорожных табло.

Деятельность [Sun Hacker], скорее всего, связана с выходом 27 мая 2014 г. игры Watch Dogs, геймплей которой построен на «взломах» с фокусом на критические инфраструктурные электронные решения в частности. Watch Dogs позволяет игрокам взламывать электронные дорожные знаки, камеры наблюдения, светофоры, мобильные телефоны и другие системы. 27 мая злоумышленник опубликовал в своём Twitter изображение из Watch Dogs, показав свою заинтересованность игрой. CIS считает, что небольшой процент игроков Watch Dogs попробует свои силы в компрометировании компьютеров и электронных систем за пределами игры, и эта активность повлияет на государственные системы в частности – Отчёт MS-ISAC

Это не первый случай, когда хакеры взламывают дорожные табло в США. В 2012 г. неизвестные злоумышленники проделали нечто подобное со знаками в штате Вашингтон, сменив служебные надписи на предупреждение «Осторожно, впереди зомби» ***(Watch Dogs обвинили в провоцировании серии взломов дорожных табло в США // InternetUA (http://internetua.com/Watch-Dogs-obvinili-v-provocirovanii-serii-vzlomov-dorojnih-tablo-v-ssha). – 2014. – 11.06).***

***

Twitter пытается устранить уязвимость в популярном приложении TweetDeck, которая дает хакерам возможность показывать пользователям странные всплывающие сообщения и распространять потенциально вредоносный код. Об этом сообщает издание USA Today.

Так называемая XSS-уязвимость (cross-site scripting – межсайтовый скриптинг) является достаточно распространенной в веб-приложениях. Она позволяет внедрить в интернет-страницу, которую сервис выдает пользователю, тот или иной произвольный код, возможно – вредоносный. Цели хакеров при эксплуатации такой уязвимости могут варьироваться – от

неавторизованного размещения рекламы до перехвата логинов и паролей пользователя.

В случае с TweetDeck, который с 2011 г. принадлежит компании Twitter, пользователи видят всплывающие сообщения, к примеру Yo! или Please close now TweetDeck, it is not safe. Кроме того, сервис в случайном порядке ретвитит сообщения с потенциально вредоносным кодом. Масштабы инцидента не уточняются.

«Мы временно закрыли доступ к сервису TweetDeck после выявления уязвимости», – объявили администраторы TweetDeck накануне в своем Twitter-аккаунте. Под угрозой оказались десктопное Windows-приложение TweetDeck и веб-версия.

Предполагается, что инцидент спровоцировал 19-летний австрийский программист. Он экспериментировал с символами в коде и обнаружил уязвимость, которая позволяла вставлять компьютерные команды в твиты. Программист оповестил администрацию Twitter и рассказал о находке в онлайн-блоге. Однако другие хакеры успели воспользоваться ошибкой до того, как Twitter ее устранил.

По словам представителей TweetDeck, уязвимость была ликвидирована и пользователям рекомендовалось выйти из сервиса и снова зайти, используя свои данные. Однако, по словам эксперта по инфобезопасности из компании Rapid7 Т. Форда, последствия ошибки в виде твитов с вредоносным кодом по-прежнему распространяются на сервисе. Поэтому до полного устранения проблемы пользователям рекомендуется «отвязать» сервис TweetDeck от своего Twitter-аккаунта.

TweetDeck – это бесплатный сервис-клиент для публикации и чтения сообщений в Twitter. Он доступен для компьютеров Mac и ПК, смартфонов iPhone, Android-устройств и в виде приложения для браузера Google Chrome. Сервис был самым популярным из сторонних приложений для работы с Twitter, и сам Twitter его купил в 2011 г. за 40 млн дол. ***(Уязвимость в сервисе TweetDeck создала угрозу для пользователей Twitter // InternetUA (http://internetua.com/uyazvimost-v-servise-TweetDeck-sozdala-ugrozu-dlya-polzovatelei-Twitter). – 2014. – 12.06).***

***

Корпорация IBM сообщила о получении патента на технологию по борьбе с онлайн-преступлениями, которая мониторит и анализирует поведенческие факторы. Технологию назвали «Система обнаружения мошенничества на основе анализа взаимодействия пользователя и браузера».

Новая система анализирует работу пользователя в Интернете, включая такие сайты как интернет-магазины и банковские ресурсы. Предполагается, что пользователь Интернета имеет характерное только ему поведение, то есть, использование набора горячих клавиш, частое посещение конкретных веб-ресурсов. В случае, когда девайсом управляет бот, линия поведения в корне меняется. Разработанная IBM система отслеживает это, и, в случае

несовпадения привычной работы в сети, запрашивает у пользователя информацию для его идентификации.

Поведение пользователя может измениться под влиянием ряда причин – проблемы со здоровьем, использование другого девайса, но пройти дополнительную идентификацию ради безопасности не составит труда.

Разработчики подчеркивают, что резкие изменения поведения пользователя в Интернете происходят именно из-за перехвата девайса ботами. Злоумышленникам будет тяжело пройти дополнительную идентификацию ***(IBM разработала систему, отслеживающую перехват девайса ботами // InternetUA (http://internetua.com/IBM-razrabotala-sistemu--otslejivauasxuua-perehvat-devaisa-botami). – 2014. – 13.06).***

***

Согласно статистике «Лаборатории Касперского» за 2013 г., 22 % срабатываний модуля «Антифишинг», входящего в состав продуктов компании, приходятся на фальшивые страницы и поддельные уведомления Facebook. При этом срабатывания на имитации других социальных сетей и блогерских площадок в сумме составляют 13,5 %. Всего же за прошлый год зарегистрировано более 600 млн фишинговых инцидентов.

Киберпреступники используют ряд устоявшихся способов заманить жертву на фишинговые ресурсы. Как правило, ссылки на такие страницы злоумышленники распространяют в письмах, имитирующих оповещения от социальной сети. Также популярны рассылки по электронной почте со взломанных аккаунтов по адресному листу – к примеру, сообщения друзьям с предложением перейти по ссылке для просмотра интересного контента. При этом мошенники часто прибегают к запугиванию и в письмах-подделках грозят получателю блокировкой аккаунта, избежать которой можно, перейдя по ссылке в письме и введя персональные данные на открывшейся странице, – расчет идет на всплеск эмоций и сопутствующую потерю бдительности.

Владельцы смартфонов и планшетов, посещающие социальные сети через свои мобильные устройства, также не застрахованы от фишинга – мошенники создают специальные веб-страницы, имитирующие вход в аккаунт через мобильное приложение Facebook. При этом на руку мошенникам играет то, что некоторые мобильные браузеры скрывают адресную строку при открытии страницы, затрудняя обнаружение подделки.

«Согласно данным за 2013 г., Facebook лидировал по числу фишинговых инцидентов. В начале 2014 г. ситуация несколько изменилась, и на первое место вышел Yahoo. Однако Facebook по-прежнему держится в топе мишеней фишеров: каждый день мы фиксируем более 20 тыс. попыток перехода пользователей на страницы, имитирующие эту социальную сеть. И неудивительно, доступ к аккаунтам пользователей Facebook может понадобиться мошенникам для множества преступных целей – от рассылки спама до вымогания денег у друзей жертвы. Со своей стороны мы рекомендуем обращать внимание на наличие защищенного соединения –

Facebook использует протокол HTTPS для передачи данных. Его отсутствие даже при правильном адресе страницы говорит о том, что вы, скорее всего, находитесь на мошенническом ресурсе», – советует Н. Демидова, контент-аналитик «Лаборатории Касперского» ***(Facebook – самый популярный ресурс среди фишеров // InternetUA (http://internetua.com/Facebook---samii-populyarnii-resurs-sredi-fisherov). – 2014. – 13.06).***

***

Всего 0,91 % украинских провайдеров способствовали ликвидации деятельности бот-сети GameOver ZeuS. При этом 90,09 % провайдеров вообще не известили своих пользователей о существующей проблеме.

Об этом говорится в сообщении CERT-UA, специализированного структурного подразделения Государственного центра защиты информационно-телекоммуникационных систем Государственной службы специальной связи и защиты информации Украины.

В течение мая – июня 2014 г. соответствующим подразделением компании Microsoft совместно с ФБР и правоохранительными органами других стран проведена международная операция по ликвидации деятельности бот-сети GameOver ZeuS. Почти все украинские провайдеры отказались содействовать данной операции.

«Командой реагирования на компьютерные чрезвычайные события Украины CERT-UA была получена информация относительно перечня IP-адресов национального сегмента сети Интернет, принадлежащие компьютерам, пораженным вышеупомянутым вредным программным обеспечением», – сказано в сообщении.

Также уточняется, что с целью ликвидации угрозы и защиты граждан Украины были приняты меры по информированию ответственных провайдеров Украины, в зоне ответственности которых находились упомянутые IP-адреса, с просьбой сообщить их абонентам о существующей угрозе и предоставить рекомендации по ее ликвидации.

Кроме того, при информировании было отмечено, что результаты отработки этого инцидента будут использованы CERT-UA для определения уровня содействия каждого из провайдеров в вопросах ликвидации угроз информационной безопасности на территории украинского Интернета.

Согласно полученным результатам, всего 0,91 % провайдеров способствовали решению инцидента, при этом 90,09 % провайдеров вообще не известили своих пользователей о существующей проблеме.

Напомним, GameOver ZeuS – троянская программа, предназначенная для кражи данных аутентификации (паролей), данных платежных карт, сертификатов, а также организации несанкционированного скрытого использования вычислительных ресурсов инфицированных компьютеров, например, для проведения DDoS-атак, генерации криптовалюты Bitcoin т. п. ***(Украинские провайдеры игнорируют безопасность своих пользователей***

// InternetUA (http://internetua.com/ukrainskie-provaideri-ignoriruuat-bezopasnost-svoih-polzovatelei). – 2014. – 13.06).

***

На нескольких подпольных форумах зафиксирована продажа вируса Pandemiya, которого эксперты из RSA Research Group называют альтернативой банковскому трояну Zeus. Новый вирус позволяет злоумышленникам похищать учетные данные, важную банковскую информацию и файлы с зараженных компьютеров.

Как и Zeus, Pandemiya имеет модульный дизайн, благодаря чему его легко использовать для расширения и добавления функциональности.

Помимо прочего, новый вредонос способен встраивать в веб-сайты поддельные элементы, делать скриншоты с компьютера жертвы, а также шифровать коммуникации между ним и C&C-сервером. Отличием Pandemiya от других банковских троянов является то, что его написали с нуля, не используя ни одной части исходного кода Zeus.

По словам У. Флейдера из RSA Research Group, подобное было зафиксировано впервые. Так, столь известные троянские вирусы, как Citadel/Ice IX и Carberp были написаны на основе исходника Zeus.

Всего на создание нового вируса у его автора/авторов ушло порядка года, подчеркивают ИБ-эксперты в блоге RSA Fraud Action. Так, троянец содержит свыше 25 тыс. строчек оригинального кода, написанного на языке программирования Си.

Базовое приложение Pandemiya содержит инструменты для осуществления инъекций (доступны версии для трех наиболее популярных браузеров), загрузчик с уникальными задачами и статистикой, а также поддержку подписи файлов, мешающей кому-либо похищать или анализировать их.

В настоящее время Pandemiya можно приобрести по цене от 1,5 тыс. дол. (базовое приложение) до 2 тыс. дол. (базовое приложение и дополнительные плагины) ***(На подпольных форумах продается альтернатива знаменитому трояну Zeus // InternetUA (http://internetua.com/na-podpolnih-forumah-prodaetsya-alternativa-znamenitomu-troyanu-Zeus). – 2014. – 13.06).***

***

Ізраїльські вчені розробили програмне забезпечення, яке здатне за допомогою мобільного телефону виявити електричні імпульси і встановити шкідливе ПЗ на комп’ютер, фізично відключений від мережі Інтернет.

Професор з університету ім. Бен-Гуріона Ю. Еловіці розповів виданню The Times of Israel, що його команда змогла встановити шкідливе ПЗ і успішно перехопила дані з віддаленого комп’ютера. За словами дослідника, атака може здійснюватися на відстані до 6 м.

Атака на віддалений комп’ютер являє собою реалізацію програми АНБ TEMPEST, призначену для перехоплення даних за допомогою електромагнітного випромінювання.

Сценарій атаки, описаний у дослідженні ізраїльських учених, передбачає наявність спеціального додатка на мобільному телефоні, який створює мережеве підключення до комп’ютера за допомогою FM-частот. Використовуючи це підключення, зловмисник може встановити довільне ПЗ на віддалений комп’ютер і використовувати його для обміну даними з додатком на мобільному телефоні ***(Ізраїльські вчені продемонстрували бездротовий злом комп’ютера, відключеного від мережі // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ua/news/2014/06/13/hackind-unplugged-comp.html). – 2014. – 13.06).***