СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(1–15.02)

2015 № 3

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(1–15.02)
№ 3

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 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компанія Gemius Україна представила дані щодо 20 найбільш популярних сайтів, які відвідували українці в грудні 2014 р. Лідирує, як і раніше, Google.

76 % українців принаймні один раз відвідали Google в грудні. Далі за кількістю аудиторії ідуть Mail.Ru, «ВКонтакте», YouTube і Yandex.

Facebook займає шосту позицію і охоплює 35 % десктопної інтернет-аудиторії країни. «Одноклассники» опустилися на восьму позицію з охопленням 31 %.

Згідно з даними gemiusAudience, розмір ПК інтернет-аудиторії в грудні 2014 р. – 18 млн осіб (real users, 14+). Соц-дем. звіт складений на підставі 8385 анкет software-панелістів і 48 628 анкет cookie-панелістів ***(ТОП-20 сайтів українського інтернету: Одноклассники продовжують здавати позиції // Watcher (http://watcher.com.ua/2015/02/02/top-20-saytiv-***

ukrayinskoho-internetu-odnoklasnyky-prodovzhuyut-zdavaty-pozytsiyi/). – 2015. – 2.02).

***

Twitter заключил сделку с поисковым гигантом о показе твитов в поисковой выдаче Google, сообщает Bloomberg со ссылкой на источники, знакомые с ситуацией, пишет Marketing Media Review (http://mmr.ua/news/id/google-pokazhet-tvity-v-rezultatah-poiska-43111/).

По слухам, уже в первой половине этого года твиты начнут быть видимыми в результатах поиска Google сразу же после публикации: в результате соглашения интернет-корпорация получит доступ к информационному потоку, генерируемому 284-миллионной аудиторией микроблогового сервиса. Ранее механизму поисковой выдачи Google приходилось самостоятельно извлекать нужные данные из Twitter, теперь же они будут поступать автоматически.

Информация о договоренности между двумя крупными интернет-компаниями только подчеркивает те существенные усилия, которые CEO Twitter Д. Костоло прилагает для показа коротких сообщений большему числу людей, не являющихся пользователями сервиса, и как следствие увеличения рекламных доходов благодаря расширению аудитории.

По данным источников, которые пожелали остаться анонимными в связи с негласным характером сделки, разработчики Twitter и Google уже приступили к совместной работе ***(Google покажет твиты в результатах поиска // Marketing Media Review (http://mmr.ua/news/id/google-pokazhet-tvity-v-rezultatah-poiska-43111/). – 2015. – 5.02).***

***

Англоязычные пользователи заметили, что Twitter тестирует новый дизайн главной страницы для пользователей, которые не авторизированы в сервисе. Представитель компании подтвердил эту информацию.

Новая версия страницы предлагает посетителям взглянуть на то, что их ожидает, если они зарегистрируются. Она включает несколько лент твитов из разных категорий, отобранных из популярных в социальной сети аккаунтов.

На конференции Twitter для аналитиков Analyst’s Day в ноябре 2014 г. руководители компании сообщили, что сайт Twitter.com посещает более 500 млн неавторизированных пользователей. Это огромная аудитория потенциальных участников, которую компания пытается удержать. Также вероятно, что Twitter будет использовать новую главную страницу для показа рекламы её посетителям.

В русскоязычной версии Twitter главная страница пока отображается в старом дизайне ***(Twitter тестирует новый дизайн главной страницы для незарегистрированных пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_testiruet_novyy_dizayn_glavnoy_stranitsy_dlya_nezaregistrirovannyh_polzovateley). – 2015. – 10.02).***

***

Facebook – YouTube будущего?

Если вы пользуетесь Facebook и у вас создалось впечатление, что в этой сети все больше видео, это неспроста. Последнее время Facebook делает большой упор на видео. И эта политика приносит свои плоды.

По самым свежим данным, каждый день в Facebook осуществляется около 3 млрд просмотров видеороликов в день. Только в период с мая по июль число просмотров возросло на 50 %. Компания сообщила об этом в последнем квартальном отчете.

Конечно, пока Facebook далеко до YouTube, который еще в 2012 г. прошел отметку в 4 млрд в день, однако этот результат все равно впечатляет. Если учесть активную ежедневную аудиторию сайта в 890 млн человек в день, это значит, что каждый посетитель в среднем просматривает три ролика, и делает он это на Facebook, а не переходит на YouTube. Если так пойдет дальше, соцсеть вполне сможет бросить вызов видеопроекту Google.

В отчете Facebook говорится, что за прошлый год соотношение выложенных видеороликов к общему числу пользователей возросло на 75 % в мире и на 94 % – в США.

Мощный толчок популярности видео на Facebook сделала прошлогодняя благотворительная акция ALS, в которой знаменитостям предлагалось обливаться холодной водой. Кампания базировалась именно на Facebook, а не YouTube.

65 % всех просмотров видео на YouTube происходит на мобильных устройствах – еще одна мощная тенденция последнего времени ***(Facebook – YouTube будущего? // InternetUA (http://internetua.com/Facebook---YouTube-budusxego). – 2015. – 3.02).***

***

Компания Facebook включила в свой проект Internet.org Индию, обеспечив бесплатными базовыми онлайн-сервисами шесть индийских штатов. Об этом гендиректор Facebook М. Цукерберг сообщил на своей странице в соцсети.

«Мы только что запустили Internet.org в Индии, обеспечив людей в шести штатах бесплатным доступом к интернет-сервисам для здравоохранения, образования, поиска работы и общения. Более миллиарда человек в Индии не имеют доступа к Интернету – и это означает, что они не могут использовать те же возможности, которые многие из нас принимают как данность, а мир лишен их идей и креативности», – пишет М. Цукерберг.

По словам главы Facebook, жители шести индийских штатов получат бесплатный доступ к более чем трем десяткам интернет-сервисов, включая Wikipedia, новости BBC, а также саму Facebook.

«За последний год мы запустили бесплатные сервисы Internet.org в странах с общим населением в 150 млн человек в Африке и Латинской

Америке. Более 6 млн человек, которые раньше не имели доступа к Интернету, получили его. Настанет день, и мы сможем подключить всех, и возможностями Интернета смогут пользоваться все люди как в Индии, так и по всему миру», – отмечает М. Цукерберг.

Ранее к проекту подключились Гана, Замбия, Кения, Колумбия и Танзания. Однако Индия – крупнейший на сегодняшний день развивающийся рынок, с которым начал работать Internet.org. По прогнозу аналитиков, Индия вскоре опередит США по числу пользователей Facebook.

Целью благотворительной инициативы Internet.org является подключение к Интернету 5 млрд человек по всему миру (в основном речь идет о населении бедных африканских стран). В рамках проекта Facebook при помощи партнеров планирует предоставлять бесплатный доступ к базовым онлайн-сервисам, увеличить эффективность передачи электронных данных и снизить стоимость подключения к Интернету в 100 раз ***(Facebook обеспечила Индию бесплатным интернетом // InternetUA (http://internetua.com/Facebook-obespecsila-indiua-besplatnim-internetom). – 2015. – 11.02).***

***

Социальная сеть Facebook ввела возможность оставить завещание, которое оговаривает условия использования аккаунта после смерти пользователя. Об этом сообщается на сайте компании.

«Когда человек уходит, его аккаунт становится памятью о его жизни, друзьях и впечатлениях», – говорится в сообщении.

Завещание позволяет передать управление аккаунтом члену семьи или другу. Если кто-то сообщает, что владелец аккаунта умер, то страница ушедшего получает мемориальный статус. Наследник сможет делать сообщения в хронике (например, сообщить о дате похорон), а также отвечать на запросы о дружбе членам семьи и друзьям, которые не «зафрендились» с покойным при его жизни.

Кроме того, предусмотрена возможность замены аватарки и фона аккаунта, одобрение фотографий и постов, в которых отмечен умерший владелец аккаунта. При этом указанный в завещании не сможет заходить в аккаунт под логином умершего и узнать информацию, которая скрыта от просмотра посторонними настройками безопасности.

Владелец аккаунта может выбрать полное удаление данных после его смерти.

Для того, чтобы получить доступ к функции завещания аккаунта надо открыть настройки и выбрать Security, затем Legacy Contact в нижней части страницы и прописать подробности условий управления аккаунтом после смерти пользователя.

В русскоязычном аккаунте это будет эквивалентно выбору опций Настройки – Конфиденциальность. Однако в аккаунте корреспондента

«Ленты.ру» функция завещания еще не появилась, поэтому непонятно, как она будет называться.

Ранее аккаунты умерших оставались видимыми в соцсети, однако никто не мог управлять ими ***(Facebook разрешил пользователям наследовать аккаунты // InternetUA (http://internetua.com/Facebook-razreshil-polzovatelyam-nasledovat-akkaunti).– 2015. – 12.02).***

***

Microsoft разрабатывает социальную видеосеть Skype Cam

Компания Microsoft готовит к выпуску приложение Skype Cam. Оно выйдет на платформе Windows Phone (или Windows 10) и позволит пользователям делиться с другими людьми фотографиями и видеороликами.

Фотоснимки или видео можно объединять в альбомы, а доступ к ним могут получать либо друзья пользователя, либо кто угодно. Приложение Skype Cam уже опубликовано в магазине Windows Phone, но доступ к нему закрыт. Вероятно, оно проходит внутреннее тестирование среди сотрудников Microsoft ***(Microsoft разрабатывает социальную видеосеть Skype Cam // InternetUA (http://internetua.com/Microsoft-razrabativaet-socialnuua-videoset-Skype-Cam). – 2015. – 8.02).***

***

Очередное обновление мобильного приложения «ВКонтакте» лишило пользователей возможности проигрывать музыку из социальной сети на устройствах под управлением iOS, пишет Imena.UA (http://www.imena.ua/blog/iosupdate-no-audio/).

Принять соответствующие меры социальная сеть была вынуждена по требованию Apple. Предполагается, что запрет на онлайн-проигрывание музыки носит временный характер и администрация соцсети обещает оперативно решить вопрос.

В свою очередь представители Apple не стали комментировать ситуацию. Отметим, что в правилах Apple, опубликованных на сайте, сказано, что разработчики приложений не должны нарушать права третьих лиц, в том числе авторские и смежные.

Как известно, правообладатели уже больше двух лет жалуются Apple на приложения «ВКонтакте». Их раздражает, что сеть даёт свободный доступ к нелицензионной музыке. Тем не менее, в Apple впервые обратили внимание на эти жалобы только в 2014 г., после того как в РФ заработал iTunes.

Кроме того, существует версия, что «ВКонтакте» убрала из приложения музыкальный плеер, чтобы впоследствии продавать пользователям подписку на музыкальный сервис через отдельное приложение ***(«ВКонтакте» убрала стриминг музыки из iOS-приложения // Imena.UA (http://www.imena.ua/blog/iosupdate-no-audio/). – 2015. – 13.02).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В Україні створили форум для обговорення антитерористичної операції. На сайті у відповідних розділах можна обговорити все, що стосується воєнних дій та кризи в Україні. Форум АТО.com.ua відкрився 1 лютого 2015 р.

«Форум є незалежним ресурсом. Він не є проектом якоїсь політсили або якогось чиновника, – сказано в описі ресурсу. – Ми хочемо допомогти людям обмінюватися необхідною інформацією щодо АТО, тому створили АТО.com.ua як єдине для цього місце в Інтернеті, якого до цього часу не було».

Сайт запустили двоє киян, пише AIN.UA. Домен вони зареєстрували ще 7 січня, потім вирішили створити форум, де люди могли б обмінюватися необхідною інформацією щодо АТО. Ресурс має стати українською альтернативою обговорення у Facebook.

Теми структуровані, зокрема в розділі АТО є «Передова», «Батальйони», «Мобілізація», «Біженці», «Розшук», «Волонтерський рух». У розділі «Наше життя» – «Політика», «Україна vs. Росія», «ЛНР, ДНР», «Крим».

Для боротьби з ботами, адміністратори передбачили спеціальний вбудований плагін антиспаму, також будуть модерувати вручну, аби захистись від тролів, сказав співзасновник ресурсу С. Ткачук.

На форумі транслюється Twitter-стрічка з хештегами про АТО. Проект фінансується на власні кошти розробників, поки що в команді їх двоє і форумом автори займаються у вільний час ***(В Україні створили форум для обговорення антитерористичної операції // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/online_media/v_ukraini_stvorili_forum_dlya_obgovorennya_antiteroristichnoi_operatsii/). – 2015. – 3.02).***

***

Користувачі Твіттера активно поширюють «твіт миру» вбитого журналіста Кендзі Гото

Після смерті японського репортера К. Гото в мережі набрав популярності його твіт про мир, який він написав ще чотири роки тому.

«Закриваю очі і заспокоююсь. Це те, що я роблю, якщо серджусь та кричу. Це схоже на молитву: Ненависть не для людей. Судити може тільки Бог. Це те, чому я навчився від моїх арабських братів та сестер», – написав К. Гото 7 вересня 2010 р.

Станом на 4 лютого твіт набрав 36 тис. ретвітів.

Інше повідомлення, яке також стало популярним, це твіт від журналіста ВВС Д. Лонгмена, який застерігає користувачів соціальних мереж від поширення пропаганди ISIS.

«Не діліться відео. Не грайте в їх гру. Поширюйте фотографії, на яких Кендзі робить свою роботу», – написав він.

Нагадаємо, що 1 лютого екстремісти з «Ісламської держави в Іраку і Леванті (ISIS) розмістили відео із зображенням обезголовленого тіла 47-річного японського журналіста К. Гото.

Відомий британський журналіст Г. Трікс, який знав страченого ісламістами К. Гото особисто, називає його «нетиповим репортером» і «нетиповим японцем». У своєму блозі на сайті Комітету захисту журналістів (CPJ) він пише, що «мужність та відданість цього журналіста, гуманному висвітленню подій у найнебезпечніших конфліктах могла б висунути його на вершину професії у будь-якій точці світу. Мужність привела його торік до Сирії, де він став заручником».

1996 р. К. Гото заснував незалежну медіа-компанію, він висвітлював конфлікти в Чечні, Албанії, Косово, Сьєрра-Леоне, Ліберії, Афганістані, Іраку та Сирії, в інших гарячих місцях.

На DVD і в книзі «Ласкаво просимо до нашої школи» (Welcome to Our School), виданій 2003 р., К. Гото зосереджував увагу на дітях Іраку й Афганістану, які прагнуть до знань. К. Гото видав також книги про СНІД, дітей-вояків у Сьєрра-Леоне, геноцид у Руанді, школярок в Афганістані.

У серпні терористи опублікували відео, на якому у такий же спосіб вбивають американського журналіста Д. Фоулі, та у вересні С. Сотлоффа ***(Користувачі Твіттера активно поширюють «твіт миру» вбитого журналіста Кендзі Гото // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/media_law/world_journalists/koristuvachi_tvittera_aktivno_poshiryuyut_tvit_miru_vbitogo_zhurnalista_kendzi_goto/). – 2015. – 4.02).***

***

Официальная страница Заречного районного суда г. Сумы была зарегистрирована в Facebook.

Пока информации там не много: фотографии, сообщение об избрании меры пресечения экс-прокурору Сумщины Р. Белоконю, а также отчет суда о внедрении электронных и компьютерных технологий в 2014 г. В суде уверяют, что в ближайшее время наполнение страницы будет более объемным и информативным, в том числе в Facebook будет размещаться информация о резонансных делах.

В планах суда и создание интернет-приемной, где граждане смогли бы задать свои вопросы и получать ответы от руководства и ответственных работников суда.

«В декабре прошлого года в целях упрощения доступа граждан к информации о деятельности судебной власти в помещении Заречного

районного суда г. Суми на третьем этаже установили программно-аппаратный комплекс “Информационный киоск”. – сообщила руководитель аппарата суда А. Ковтун. – С помощью комплекса посетители суда могут самостоятельно проверить список дел, назначенных к рассмотрению, осуществить электронный поиск дела по номеру телефона, дате назначения или участнику процесса, получить информацию о состоянии рассмотрения дела, узнать банковские реквизиты для уплаты судебных сборов» ***(Заречный райсуд Сум вышел в «Фейсбук» // Данкор онлайн (http://www.dancor.sumy.ua/news/newsline/146315). – 2015. – 5.02).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Пока маркетологи изучают, какая соцсеть наиболее пригодна для продвижения брендов, Facebook разработал новый инструмент для рекламодателей, позволяющий сделать дорогостоящие рекламные объявления более релевантными и эффективными, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-prezentuet-rejting-relevantnosti-reklamy-minimum-88-kotoroj-klikajut-boty-43210).

Как заявляет сам Facebook, с помощью этого инструмента рекламодатели смогут отслеживать рейтинг рекламы и, в соответствии с этим, улучшать свои рекламные сообщения, делая их более подходящими для своей аудитории. Соцсеть будет оценивать эффективность рекламы по шкале от 1 до 10 (10 будет означать самую высокую релевантность сообщения).

Релевантность сообщения определяется позитивной реакцией пользователей, включая просмотры видео, «шеры» и «лайки», и негативной, включая количество кликов, сделанных людьми, чтобы скрыть сообщение или пожаловаться на него как на спам.

Facebook начнет отслеживать релевантность рекламы после 500 просмотров и будет обновлять информацию при увеличении количества просмотров.

За последние два года рекламные объявления на Facebook только росли в цене и уменьшались в количестве показов. Так, в последнем квартале 2014 г. средняя цена за объявление возросла на 335 %, а количество показов рекламы упало на 65 %. С помощью нового инструмента Facebook надеется сделать рекламу более эффективной.

Реклама в социальной сети – это игра на тонком льду. Пользователей раздражают навязчивые объявления или глупые сообщения, а значит, их легко потерять, тем более, когда вокруг есть конкуренты, пока избегающие рекламы.

Но рейтинговая оценка рекламных сообщений эффективна еще и потому, что может повлиять на снижение цены рекламы. При оценке релевантности объявления система Facebook учитывает, сколько рекламодатель готов заплатить за то или иное сообщение, и если оно будет релевантным, то его увидит большее количество людей из целевой аудитории, а денег на это уйдет меньше. Также будет учитываться тип рекламы. Например, если это продвижение приложения, которое нужно скачать, кликнув по объявлению, то первым делом, будет подсчитываться количество «кликов».

Что касается «кликов», то интересное исследование недавно опубликовала Oxford BioChronometrics, люксембургская компания, специализирующаяся на технологиях распознавания человека. По результатам исследования выяснилось, что от 88 до 98 % взаимодействия с рекламными сообщениями онлайн – подделка. Команда Oxford BioChronometrics изучила digital-рекламу на Google, Yahoo, Facebook и LinkedIn. Выяснилось, что на LinkedIn 88 % реакций на рекламные сообщения исходила от ботов. На платформах Google их количество увеличилось до 98 %, тогда как «средние» показатели у Yahoo и Facebook – 94 %. Пугающая информация, если учитывать, что на каждый такой «клик» рекламодатель попусту тратит деньги.

Для исследования применялись новые, ранее недоступные, технологии. По словам одного из членов команды С. Кувенховена, «существовавшие до этого программы просто не могли отслеживать ботов до такой степени».

Команда классифицирует ботов по шести категориям продвинутости, которые не перестают совершенствоваться. Самые опасные среди них – так называемые «гуманоиды», их можно выявить только в ходе глубокого анализа поведения, которое очень напоминает человеческое.

«Нам нелегко было выпустить этот пресс-релиз и мы осознаем, сколько злости он вызовет», – говорит президент компании Э. Нил.

«Но мы верим, что сплоченное онлайн-сообщество должно знать, что у нас не было выбора. Рекламодатели делают возможными существование многих онлайн-сообществ и очень важно сохранить целостность их пребывания онлайн, если мы хотим, чтобы они и дальше участвовали в этом. Мы можем достичь этого только за счет прозрачности и пришло время пролить свет на область, которую многие не хотят замечать».

Это исследование по сути стало ответной реакцией на документ от Google за ноябрь 2014 г. под названием «Важность быть увиденным». В нем утверждалось, что рекламодатели должны стремиться не к простым метрическим показателям, а к тому, чтобы достичь более 50 % просмотров своей рекламы пользователями. Oxford BioChronometrics утверждает, что их новая технология защиты онлайн-рекламы (Digital Ad Protection Technology) поможет достичь почти 100-процентных «человеческих кликов» ***(Facebook презентует рейтинг релевантности рекламы, минимум 88 % которой кликают боты // Marketing Media Review (http://mmr.ua/news/id/facebook-***

prezentuet-rejting-relevantnosti-reklamy-minimum-88-kotoroj-klikajut-boty-43210). – 2015. – 12.02).

***

Twitter планирует показывать свои объявления за пределами соцсети. Первыми партнерами сервиса микроблогов в новой программе стали мобильное приложение для чтения новостей Flipboard и Yahoo Japan.

«Twitter уникален благодаря тому, что твиты могут легко переходить из соцсети на другие носители, как телевидение, веб-сайты и мобильные приложения, – говорит старший директор по продукту А. Ранадив. – Для тысяч брендов, уже рекламирующихся в Twitter, новое партнерство открывает значительные возможности расширения охвата аудитории. Объявления Twitter будут видны пользователям в разделах контента Twitter на сторонних сайтах, а также в разделах стороннего контента».

«Например, Nissan запускает кампанию Продвигаемых твитов в Twitter и пытается достичь аналогичной аудитории с помощью мобильного приложения вроде Flipboard, – добавляет А. Ранадив. – Flipboard уже интегрировал органические твиты в приложение, поэтому Продвигаемые твиты будут выглядеть так же и предоставлять нативный опыт Flipboard».

В Twitter считают, что новый продукт поможет специалистам по маркетингу увеличить потенциал крупномасштабных рекламных кампаний на «почти бесконечной» основе. Чем больше Twitter заключит партнерских соглашений, тем более правдивым окажется это утверждение.

Продвигаемые твиты в общем потоке Twitter появились 28 июля 2011 г.

В апреле 2014 Twitter предоставил возможность автоматизированной закупки нативной рекламы. Реализовать технологию удалось благодаря функционалу платформы MoPub, которая была приобретена компанией в сентябре 2013 г.

В августе 2014 г. сервис микроблогов заявил о бета-тестировании продвигаемых видео ***(Продвигаемые твиты выходят за пределы Twitter'a // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/prodvigaemye_tvity_vyhodyat_za_predely_twitter_a). – 2015. – 9.02).***

***

Твиттер двукратно увеличил показатель вовлеченности в кампании брендов

Simply Measured, компания, занимающаяся аналитикой в социальных медиа, выяснила, что общий показатель вовлеченности для рекламных Twitter-активностей крупных компаний возрос на 105 % в последней четверти прошлого года по сравнению с аналогичным отчетным периодом в 2013 г., пишет Marketing Media Review (http://mmr.ua/news/id/tvitter-dvukratno-uvelichil-pokazatel-vovlechennosti-v-kampanii-brendov-43194/).

Изучив рейтинг Interbrand «100 лучших мировых брендов» за период с 1 октября по 31 декабря 2014 г., специалисты Simply Measured также

обнаружили, что компаниями было опубликовано на 11 % больше твитов, чем в том же промежутке годом ранее. В целом за 2014 г. число фоловеров крупных брендов увеличилось на 38 %.

Д. Буллас, независимый диджитал-стратег, отмечает, что такие данные говорят о «повышении комфорта пользовательского взаимодействия с брендами на площадке микроблогового сервиса». Вот несколько ключевых моментов, которые он обнаружил по итогам рейтинга Interbrand:

Из 100 топовых компаний 95 размещали твиты хотя бы раз в день;

Прирост числа ретвитов и ответов, связанных с клиентским сервисом, повлиял на общее увеличение количества брендированных постов на 25 % в отчетном периоде;

Почти половина компании (48 %) отвечают хотя бы на один твит в день;

91 % брендов хотя бы один раз за отчетный квартал ответили пользователю;

Показатель вовлеченности для брендированных твитов возрос с усредненной 91 интеракции в IV квартале 2013 г. до 168 интеракции в том же периоде 2014 г. ***(Твиттер двукратно увеличил показатель вовлеченности в кампании брендов // Marketing Media Review (http://mmr.ua/news/id/tvitter-dvukratno-uvelichil-pokazatel-vovlechennosti-v-kampanii-brendov-43194/). – 2015. – 11.02).***

***

Социальная сеть Twitter приобрела стартап Niche – сервис, соединяющий бренды с интернет-знаменитостями, пишет Marketing Media Review (http://mmr.ua/news/id/socialnaja-set-twitter-soedinit-brendy-so-znamenitostjami-platformy-43216/).

Компания Twitter объявила о приобретении сервиса Niche, который с помощью проработанной стратегии и грамотной технологии обеспечит монетизацию рекламной деятельности брендов на платформе. Стоимость сделки не разглашается.

Суть метода Niche – соединение «влиятельных» аккаунтов в Vine и Twitter с брендами для создания спонсорского контента и его последующей публикации. Niche предоставляет и «кроссплатформеную аналитику», но пока сложно что-то сказать о подробностях её осуществления ***(Социальная сеть Twitter соединит бренды со знаменитостями платформы // Marketing Media Review (http://mmr.ua/news/id/socialnaja-set-twitter-soedinit-brendy-so-znamenitostjami-platformy-43216/). – 2015. – 12.02).***

***

Facebook анонсировал новый способ измерения роста конверсии, давая рекламодателям возможность оценить дополнительные бизнес-результаты от пользователей, охваченных объявлениями Facebook на различных устройствах. При измерении роста конверсии Facebook определяет объем

дополнительных продаж, вызванных просмотром рекламы, и не полагается на подсчет кликов и конверсий.

Это основано на функции Facebook, которая позволяет владельцам магазинов использовать аудиторию клиентов для измерения оффлайн-продаж.

«Специалисты по маркетингу по-прежнему часто используют клики для измерения все своих онлайн-медиа, – говорит пресс-секретарь Facebook, – но клики не коррелируют с продажами в традиционных магазинах. Исследования Datalogix показали, что 90 % людей, которые видели объявление Facebook и осуществляли приобретение в традиционном магазине, никогда не нажимали на объявление. С помощью измерения роста конверсии рекламодатель может оценить дополнительные продажи, связанные с показом объявлений, и, соответственно, сможет принимать обоснованные маркетинговые решения на основании этих результатов».

«Теперь рекламодатели Facebook во всем мире будут иметь возможность применять этот метод измерения как для онлайн, так и для оффлайн-продаж, – добавляет пресс-секретарь. – Суть измерения роста проста: при создании кампании в Facebook выбирают тестовую группу (люди, которые видят объявления) и контрольную группу (люди, которые не видят их). Когда кампания завершилась, рекламодатели могут определить, какие продажи были вызваны объявлениями, и увидеть дополнительный рост, который наблюдался в тестовой группе. Это методология определения причинно-следственной связи».

В Facebook утверждают, что это лучший способ доказательства эффективности рекламы, независимо от того, где она запущена. Это также помогает маркетологам избавиться от чрезмерной зависимости от цены за клик, устаревших технологий и неэффективных методов тестирования.

О том, что Facebook планирует представить новую рекламную сеть Atlas, которая позиционируется как конкурент Контекстно-медийной сети Google (Google Display Network), стало известно в сентябре 2014 г. Новый рекламный сервис работает по принципу платформы DSP (demand-side platform), предоставляющей возможность автоматизированной закупки рекламы, нацеленной на пользователей Facebook в Интернете ***(Facebook внедрил измерение роста конверсии объявлений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_vnedril_izmerenie_rosta_konversii_obyavleniy). – 2015. – 3.02).***

***

Фотохостинг Instagram выпустил обновление, после установки которого видеоролики в ленте пользователя по окончании будут повторяться вновь до бесконечности. Об этом сообщает техноблог Re/code.

При этом видео не ставится на паузу, пока пользователь не прокрутит экран, скрыв его.

Для предотвращения израсходования мобильного трафика в настройках можно выбрать предварительную загрузку роликов только по Wi-Fi, однако функцию нельзя полностью отключить.

Закольцовывание видео также присутствует и у сервиса Vine, на который можно выкладывать 6-секундные ролики. Однако, в отличие от Instagram, клипы на Vine зачастую рассчитаны именно на такой формат бесконечного воспроизведения, отмечает The Verge.

Данный шаг Instagram удовлетворяет интересы скорее рекламодателей, так как теперь пользователю стало тяжелее избегать видеорекламу, считает портал. Компания запустила показ видеорекламы в ленте новостей в октябре прошлого года ***(Instagram закольцевал видеоролики // InternetUA (http://internetua.com/Instagram-zakolceval-videoroliki). – 2015. – 4.02).***

***

Twitter объявил о запуске модернизированной рекламной кампании под названием «Быстрое продвижение» (Quick promote). Специалисты по маркетингу получили возможность продвигать твиты с помощью нескольких кликов в панели аналитики.

Процесс рассчитан на малые и средние предприятия и призван помочь им обойти более сложную рекламную платформу Twitter. Продвигаемые твиты будут автоматически таргетированы на пользователей с интересами, подобными подписчикам аккаунта.

После входа в панель активности твитов следует выбрать твит, который следует продвинуть. В сервисе микроблогов рекомендуют выбрать сообщение, которое уже имеет большой уровень вовлеченности. Затем следует выбрать бюджет. Сервис предоставит оценку охвата после продвижения твита.

Рекламодатели могут наблюдать вовлеченность в твит в режиме реального времени, а также оптимизировать стратегию контента для увеличения количества ретвитов или переходов по ссылкам.

Быстрое продвижение уже доступно для всех рекламодателей по всему миру.

Новый рекламный продукт призван изменить отношение инвесторов к соцсети накануне оглашения финансовых результатов за IV квартал 2014 г. Инвесторы недовольны замедлением роста количества пользователей и неопределенными перспективами бизнеса ***(Twitter запускает быстрое продвижение для малого бизнеса // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/twitter_zapuskaet_bystroe_prodvizhenie_dlya_malogo_biznesa). – 2015. – 13.02).***

***

Социальная сеть Pinterest начала добавлять продвигаемые пины в ленты пользователей. До сих пор Pinterest показывал рекламу только на страницах категорий и результатов поиска.

Компания намеренно медленно внедряла введение платных сообщений на сайте. Продвигаемые пины тестировались в течение шести месяцев 2014 г., и лишь с 1 января американские специалисты по маркетингу получили доступ к рекламному продукту.

В Pinterest называют добавление объявлений в ленты пользователей ксперимeнтом.

«Мы ускоряем процесс, потому что рекламодатели готовы, – говорит глава партнерских проектов в Pinterest Д. Брэдфорд. – Мы тяжело работали в период бета-тестирования и на основе всех полученных знаний построили очень агрессивный план на 2015 г.».

Рекламный продукт на основе цены за клик – продвигаемые пины – направлен на малые и средние компании. В настоящее время для соцсети главным приоритетом является рекламный продукт на основе цены за тысячу показов, который сохранит низкое количество и высокое качество рекламы и не будет раздражать пользователей.

Это значит, что рекламодатели не смогут приобрести размещение в лентах, но смогут ориентироваться на категорию, связанную с содержанием рекламы. Объявления будут отображаться в лентах пользователей, которых Pinterest определит заинтересованными в категории, но только если пины соответствуют определенным показателям представления (по-видимому некоторая комбинация ре-пинов и кликов). Pinterest будет обслуживать в лентах меньшее количество лучших объявлений, чем в категориях и на страницах результатов поисковой выдачи.

Pinterest запустил пилотную рекламную программу «Продвигаемые пины» в сентябре 2013 г. Создатели программы обещали избежать перегруженности баннерами и не раздражать пользователей ***(Pinterest добавил продвигаемые пины в персональные ленты пользователей // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/pinterest_dobavil_prodvigaemye_piny_v_personalnye_lenty_polzovateley). – 2015. – 5.02).***

***

Shareaholic: социальные медиа в Q4 2014 принесли треть трафика на сайты

Восемь крупнейших социальных медиа-платформ в декабре 2014 г. принесли 31,24 % от общего трафика на сайты по сравнению с 22,71 % в декабре 2013 г. Об этом свидетельствуют данные очередного исследования, проведённого платформой социальной аналитики Shareaholic.

На протяжении нескольких лет (и особенно в 2014 г.) способы потребления средств массовой информации значительно изменились. Пользователи меньше полагаются на главные страницы и поисковые

системы, узнавая новости в социальных медиа и с помощью обмена сообщениями в мобильных приложениях.

Отчет о социальном трафике Shareaholic показывает, какой объем трафика принесла каждая из восьми самых популярных социальных сетей на сайты издателей по всему Интернету. Данные показывают «долю визитов» в процентах от общего трафика – прямого трафика, переходов из социальных сетей, органического и платного поиска и т. д. для Facebook, Pinterest, Twitter, StumbleUpon, Reddit, Google Plus, YouTube и LinkedIn.

Отчет за IV квартал агрегирует данные из сети сайтов Shareaholic и содержит три основные части:

Раздел I: Переходы из социальных сетей в IV квартале 2014 г. (сентябрь – декабрь 2014) – краткий обзор данных за четыре месяца, полученных от более чем 300 тыс. сайтов с общей аудиторией более 400 млн уникальных посетителей в месяц.

Раздел II: Переходы из социальных сетей год к году (декабрь 2013–2014).

Раздел III: Переходы из социальных сетей в течение трех лет для понимания исторических тенденций (декабрь 2011–2014) – углубленный анализ 37 месяцев данных, полученных от более чем 150 тыс. сайтов с общей аудиторией более 200 млн уникальных посетителей в месяц.

Раздел I: Переходы из социальных сетей в IV квартале 2014 г.

В IV квартале только две платформы – Facebook и StumbleUpon – увеличили свою долю трафика. Доля остальных шести социальных сетей сократилась в течение этого времени на 0,46 – 0,01 процентного пункта.

Facebook продолжает занимать лидирующую позицию с 24,63 % долей трафика. Pinterest приносит сайтам 5,06 % трафика. Третье место занимает Twitter с 0,82 %. Однако этот показатель больше, чем совокупный трафик пяти остальных социальных сетей.

Раздел II: Переходы из социальных сетей в 2014 финансовом году

В течение последних 13 месяцев Facebook и Pinterest продемонстрировали потенциал своих платформ специалистам по маркетингу, издателям и владельцам сайтов. Год за годом они остаются единственными социальными сетями, чья доля трафика растет. При этом доля Facebook возросла на 59,58 % (9,20 процентных пункта) с максимумом 25,06 % в октябре 2014 г. Рост доли Pinterest гораздо более скромный – 5,82 % по сравнению с годом ранее (0,28 процентных пункта). Максимум роста – 7,10 % – наблюдался в марте 2014 г., после чего наблюдается стабильный спад.

Остальные шесть социальных сетей (Twitter, StumbleUpon, Reddit, Google Plus, LinkedIn и YouTube) за год утратили 25 % доли. Доля YouTube снизилась на 93,24 % (0,18 процентных пункта). В настоящее время видеохостинг приносит 0,01 % общего трафика.

Раздел III: Переходы из социальных сетей с 2011 по 2014 г.

Ниже приведены три ключевых вывода из этих данных:

1) Facebook приносит четверть общего трафика.

Платформа, которая знает о пользователях все, – Facebook – диктует пользователям, что им читать, позволяя брендам продвигать таргетированные сообщения и предложения, и является источником переходов из социальных сетей №1 на сайты по всему Интернету.

2) Pinterest достиг своего плато.

Одна из наиболее быстро растущих социальных сетей в истории и любимая платформа американских женщин, возможно, утратила свою силу.

3) Остальные шесть платформ приносят менее 2 % от общего интернет-трафика.

Более ранние исследования Shareaholic также свидетельствовали о том, что поисковый трафик постепенно уступает место социальному ***(Shareaholic: социальные медиа в Q4 2014 принесли треть трафика на сайты // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/shareaholic_sotsialnye_media_v_q4_2014_prinesli_tret_trafika_na_sayty). – 2015. – 6.02).***

***

Социальная сеть Facebook анонсировала новую функцию, которая должна упростить пользователям торговлю на сайте.

В настоящее время в социальной сети есть возможность создания специальных групп для торговли (For Sale Groups). Этот вид групп предназначен для покупки и продажи определённых товаров, например, сувениров или изготовленных вручную подарков. Теперь при добавлении товара на продажу пользователь сможет добавить к нему фотографии, цену и место, откуда можно забрать покупку.

Такая возможность может стать большим подспорьем для малого бизнеса, она позволит увеличить продажи без затрат на интернет-маркетинг. Данная функция может представить достойную альтернативу популярному сайту объявлений Craigslist.

Это не первая попытка Facebook выйти на рынок электронной коммерции. В 2007 г. компания представила платформу Facebook Marketplace для продажи товаров и аренды жилья, но два года спустя компания отказалась от развития проекта.

Добавление подобных функций может помочь Facebook ещё крепче привязать к себе пользователей мобильных устройств – главный источник дохода компании.

Новая функция станет доступна пользователям всех платформ в ближайшие месяцы, заявляют в компании ***(Следующая цель Facebook – электронная торговля // InternetUA (http://internetua.com/sleduuasxaya-cel-Facebook---elektronnaya-torgovlya). – 2015. – 14.02).***

***

Десять топ-прогнозов для социальных медиа в 2015 г.

Как вы знаете, социальным медиа свойственны быстрые и частые изменения, за которыми иногда достаточно сложно поспеть. Цель этой статьи – обозначить нынешние тренды социальных медиа и кратко изложить прогнозы на начавшийся 2015 г., пишет ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/10_top_prognozov_dlya_sotsialnyh_media_v_2015).

1. Facebook видео заставит YouTube «попотеть».

Ежедневно мы убеждаемся в том, что популярность видео достигла апогея.

В связи с тем, что Facebook, Twitter и LinkedIn значительно расширяют видеоконтент, можно предположить масштабное включение видео в маркетинг-микс различных компаний и маркетологов.

Хотя вероятность того, что Facebook полностью обойдёт YouTube в «видеошэринге» крайне мала, мы не могли не заметить того, что они заставляют YouTube нервничать. Ведь теперь пользователи постепенно отказываются от привычного алгоритма действий: загрузка видео на YouTube – «шэринг» его на Facebook. Сегодня маркетологи загружают видео прямо на Facebook, используя его собственный функционал. К слову, недавние исследования показали, что самые популярные по «шэрам» видео загружаются прямо на Facebook, а не через YouTube. Такие дела.

2. Pay to play станет нормой.

Поскольку компании получают всё меньше и меньше результатов от их основной маркетинговой деятельности в сфере социальных медиа, они будут вынуждены всё больше и больше следовать принципу pay to play, воплощая его посредством увеличения оплаты в различных социальных сетях. У нас уже была возможность убедиться в том, что в течение прошлого года Facebook и Twitter запускали новые рекламные опции и инструменты с завидной регулярностью и, скорее всего, обороты будут только увеличиваться.

Вы уже знаете, что охват целевой аудитории Facebook-постов значительно снизился за последние несколько лет. По последним сообщениям Facebook, они будут безжалостно ограничивать посты, которые посчитают «чересчур рекламными». Компании же полагают, что эти платные рекламные объявления и рекламные посты должны стать частью их маркетингового микса, если они, конечно, хотят охватить свою аудиторию.

3. Контент всё ещё важен, но «контент ради контента» получает весомое НЕТ в 2015 г.

Всем известно, что без чётко проработанной контент-стратегии компания практически не имеет шансов преуспеть онлайн. Тем не менее, мы видим, что компании могут инвестировать тонны денежных средств и уйму времени в создание контента, даже не представляя конечную цель.

Актуальность, ориентированность на клиента и потребительский опыт – вот ключи к успеху вашего контента в 2015 г.

Как просвещать, вдохновлять и развлекать вашу аудиторию? Направлен ли контент на потребности и интересы целевого рынка? Есть ли у вас готовый план не только относительно создания контента, но и относительно того, каким именно способом вы собираетесь его размещать и продвигать? Ответы на эти вопросы станут ключевыми моментами в создании успешной контент-стратегии в текущем году.

4. ROI (Return Of Investment) переходят от сбора данных к реальным маркетинговым стратегиям.

В 2015 г. мы станем свидетелями того, как цифровой маркетинг и социальные продажи станут неразрывно связаны между собой. Владельцам бизнеса придётся искать пути предоставления своим читателям ценной информации и ознакамливающего со своим продуктом и услугами контента; учитывая количество компаний, конкурирующих за внимание потенциального покупателя, только те из них, кто предложит самый лучший целевой контент – победит.

Компаниям нужно продолжать подбирать методы, с помощью которых они будут снабжать ценной информацией своих почитателей и фолловеров, что, соответственно, существенно ускорит и облегчит потребление и реализацию.

5. Инструменты социальных продаж появятся на крупных платформах.

Как нам известно, Twitter и Facebook уже тестировали кнопку «Купить» в 2014 г. Эта функция, пока ещё не представленная широкой публике, будет иметь немаловажное значение для социальной торговли. Так как каждый дополнительный шаг в процессе покупки является ещё одним шансом потери клиента, возможность покупки в один клик по кнопке «Купить» обещает увеличение коэффициента обращаемости посетителей и покупателей.

Ещё один наблюдаемый тренд – комментирование покупки. Это стратегия, по которой почитатели и фолловеры отвечают на ваше предложение комментарием (например: «продано») или их письма, для того, чтобы осуществить покупку. Затем, компании могут связываться с этими лицами чтобы завершить продажу, высылая счёт на оплату.

6. Подлинные Be You бренды станут настоящим трендом в 2015 г.

Аутентичный маркетинг станет одним из основных аспектов стимулирования больших продаж в 2015 г.

Покупателям надоели безымянные и безликие бренды, которые воспринимаются, как сделанные по шаблону и несозвучные с их потребностями и интересами.

Бренды, сосредоточенные на создании сообщества и предоставлении высококлассного контента посредством социальных медиа, станут беспрецедентными лидерами.

7. Instagram совсем вырос!

В течение последних нескольких лет мы с вами были свидетелями впечатляющего своей масштабностью роста Instagram – платформы для обмена фото и видео. В декабре Instagram насчитывал 300 млн пользователей, которые «шэрят» больше 70 млн фото каждый день.

Очень вероятно, что в этом году компании и маркетологи будут использовать эту платформу, как основную составляющую их маркетинговой стратегии, как это уже происходит с Facebook и Twitter. По версии 2014 Social Media Marketing Industry Report, 28 % маркетологов использовали эту платформу в 2013 г., что на 10 % больше по сравнению с 2012 г. (18 %).

И что самое впечатляюще: уже 42 % маркетологов планируют увеличить «эксплуатацию» Instagram в 2015 г. Этот феномен обещает быть весьма интересным и вызывает желание за ним понаблюдать.

8. Будь mobile-friendly или отправляйся восвояси.

Mobile-friendly – модное словосочетание, которым разбрасываются направо и налево. Однако, некоторые компании до сих пор полагают, что для того, чтобы ему соответствовать, достаточно иметь мобильно-оптимизированный сайт или блог. И если наличие собственного сайта или мобильного приложения – насущная необходимость в 2015 г., то умение быть mobile-friendly намного важнее.

Весь ваш контент – посты блога и в социальных медиа, emails – должны создаваться, в первую очередь, с ориентированием на мобильные устройства.

Большинство фолловеров и подписчиков, вероятнее всего, будут знакомиться с контентом с мобильных устройств. Тем не менее, многие компании до сих пор создают и продвигают свой контент, не учитывая этих пользователей.

Обдумывание того, как и где ваши мобильные пользователи будут читать emails и посты в социальных медиа – и есть ключ к успеху. Направляются ли фолловеры по ссылкам социальных медиа непосредственно на оптимизированную для мобильных устройств страницу? Используете ли вы много разных изображений, способных привлечь внимание фолловеров?

9. Визуальный контент всё ещё задаёт тон.

Иногда это звучит, как испорченная пластинка, но визуальный контент социальных медиа снова и снова выигрывает. В 2015 г. мы всё ещё будем видеть бренды, которые делают упор на изображениях, графической и видео-составляющей социальных медиа.

10. Поддержка клиентов станет лакмусовой бумажкой для потенциальных победителей и проигравших.

Несмотря на невероятный рост социальных медиа за последние пару лет, можно увидеть, что некоторые компании застряли на создании основных элементов контента и последующем его распространении, вместо того, чтобы заниматься обслуживанием и поддержкой клиентов.

Социальное обслуживание клиентов – уже давно не просто модное выражение: покупатели полностью рассчитывают на оперативный сервис для

покупателей через социальные медиа. Как показывает инфографик на Convince and Convert, 42 % пользователей социальных медиа надеются получить ответ от компании в течение 60 минут. Вероятно, через 2–3 года этот процент станет больше.

Бренды, которые не воспринимают сициальное обслуживание клиентов серьёзно, сперва столкнутся с лояльностью клиентов, их расположением, но в конечном счёте продажи значительно снизятся.

Бонусное предсказание: Twitter станет ещё мощнее в 2015 г.

Twitter – отличная платформа для бизнеса. Он ориентирован на контент (что привлекает траффик), кроме того, там существенно улучшили рекламные предложения и модернизировали рекламную платформу. Ходили слухи, что Twitter внедрит filtered feed (схожий с аналогичным на Facebook), так что внимательно следите за изменениями на Twitter в 2015 г.

Все 10 «предсказаний» основаны на сегодняшних реалиях социальных медиа. В них нет невероятных цифр и конечных дат, так как несмотря на быстрые и регулярные изменения в социальных медиа, что-то многообещающее может так и остаться в бета-версии. Поэтому, каждый сможет сделать свои выводы к концу 2015 г. ***(10 топ-прогнозов для социальных медиа в 2015 // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/10_top_prognozov_dlya_sotsialnyh_media_v_2015). – 2015. – 11.02).***

***

Найти работу в кризис непросто, но киевляне не отчаиваются и создают в соцсетях альтернативные «биржи труда», пишет Сегодня.ua (http://kiev.segodnya.ua/kpeople/kievlyane-v-socsetyah-sozdayut-svoi-birzhi-truda-i-uchat-pereselencev-vesti-biznes-591985.html).

«Я МОГУ». В нескольких новых сообществах в Интернете жителям столицы предлагают рассказывать об услугах, которые они могут предоставлять другим. Главное правило – начинать свое объявление словами «Я могу».

Одна из недавно созданных групп – vk.com/ican_kiev. Администраторы группы считают, что такой соцсервис будет очень полезным: учитывая, что многие в настоящее время без работы, некоторые умеют мастерить симпатичные безделушки и полезности, но не знают, как об этом рассказать.

«Такой сервис уже работает в Кременчуге. Люди активно им пользуются. Теперь мы решили организовать такой же в Киеве. Многие предлагают хендмейд вещи. Кто-то умеет делать симпатичные подарки для новорожденных, кто-то мастерит своими руками украшения, кто-то умеет печь красивые тортики. Есть люди, которые увлекаются реставрацией фотографий или могут организовать различные фотосессии. С помощью сервиса обо всем этом могут узнать остальные и заказать себе необходимое», – говорит администратор сообщества М. Кокойло.

Пока на киевской страничке немного объявлений: предлагают услуги по починке компьютеров, обещают научить танцевать, продают украшения из глины. Но создатели думают, что со временем она станет популярной.

В похожей группе vk.com/club_ican люди также рассказывают о своих талантах. Здесь участники предлагают проводить частные тренировки, предоставляют услуги косметолога и шьют текстильные игрушки на заказ. Здесь также могут размещать объявления те, кто нуждается в какой-то услуге ***(Киевляне в соцсетях создают свои «биржи труда» и учат переселенцев вести бизнес // Сегодня.ua (http://kiev.segodnya.ua/kpeople/kievlyane-v-socsetyah-sozdayut-svoi-birzhi-truda-i-uchat-pereselencev-vesti-biznes-591985.html). – 2015. – 12.02).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Психологи Миссурийского университета, США, отмечают, что завистливым людям лучше не заводить себе профили в социальной сети Facebook во избежание депрессии.

Исследователи отмечают, что использование Facebook может в ряде случаев вызвать у людей, склонных к зависти, симптомы депрессии. Данный факт удалось установить команде учёных под руководством М. Даффи.

Для эксперимента специалисты разделили пользователей на две группы: первая использовала социальную сеть по прямому назначению – для общения с друзьями и родственниками. Вторая группа пользовалась Facebook для «слежки» за своими «друзьями».

Когда участники второй группы посредством Facebook узнавали о финансовом, карьерном и семейном положении своих друзей и знакомых и сравнивали эти данные со своими, то значительно чаще демонстрировали признаки депрессии.

Учёные поясняют, что пользователи впадают в депрессию из-за того, что находятся практически в непрерывном потоке информации об успехах и достижениях своих «друзей».

Начиная сравнивать свою жизнь с жизнью других, у них порой возникает чувство недовольства, что порождает симптомы депрессии.

Исследователи рекомендуют не расстраиваться из-за подобного рода заметок – в социальных сетях большинство людей склонно выставлять напоказ только положительные аспекты своей жизни, стараясь скрыть отрицательные ***(Американские психологи доказали, что Facebook***

вызывает депрессию // InternetUA (http://internetua.com/amerikanskie-psihologi-dokazali--csto-Facebook-vizivaet-depressiua). – 2015. – 8.02).

***

10 лютого, з нагоди Міжнародного дня безпечнішого Інтернету, у Києві відбулася прес-конференція, на якій обговорювалися найбільші небезпеки для дітей у мережі.

Захід провели Інтернет Асоціація України (ІнАУ) та спільна програма Європейського Союзу та Ради Європи «Зміцнення інформаційного суспільства в Україні».

Учасники прес-конференції зазначили, що сьогодні тези про важливість безпеки дітей в Інтернеті набувають нового значення. Оскільки останнім часом в українському медіапросторі зросла кількість мови ворожнечі, закликів до тероризму, а також показ сцен насилля.

У цьому контексті науковці Інституту соціальної та політичної психології провели дослідження «Нові небезпеки Інтернету під час воєнних дій очима дітей». У рамках дослідження були проведені фокус-групові інтерв'ю з дітьми 12–15 років. Мета дослідження – з'ясувати, чи воєнні дії та їх висвітлення, зокрема в Інтернеті, створюють нові небезпеки для дітей.

«Дуже акцентованим сьогодні є ризик психологічного болю – наслідки показу контенту з елементами насильства, застосування зброї, показом постраждалих та наляканих людей, – пояснила Л. Найдьонова, завідувач лабораторії психології масової комунікації та медіаосвіти. – Діти говорять, що дуже страшно, коли "падають будинки, коли вбивають людей, бо відчуття таке, що завтра це може статись з тобою"».

Значний негативний вплив, за словами Л. Найдьонової, мають фейкові факти у свідомості дітей – наприклад, почувши неправдиву новину про розстріл дітей біля школи, діти сприймають її як істину і запам'ятовують.

Іншим ризиком є те, що діти не довіряють джерелам інформації в Інтернеті – хоча раніше ситуація була протилежна: Інтернету вірили більше, ніж новинам на телебаченні. Тепер же діти кажуть, що матеріали в мережі надто суб'єктивні і важко розібратись, де в них правда.

Крім того, як показали результати досліджень у фокус-групах, нинішня ситуація вплинула на спілкування дітей у соціальних мережах: почалися сварки на політичні теми, з багатьма «друзями» діти припинили спілкування. Також респонденти зазначали, що часто бояться щось писати в соціальних мережах і прямо висловлювати свою думку.

Е. Шнурко-Табакова, голова Комітету ІнАУ з питань захисту прав людини і свободи слова, наголосила, що сьогодні інтернет-середовище багато в чому не відповідає вимогам часу, у тому числі для дітей. Наприклад, він мав би давати адекватні відповіді на такі питання, як поводити себе в різноманітних небезпечних ситуаціях, містити більші рекомендацій для дітей. Крім того, в Україні не організована система дистанційного навчання, що гостро відчувають жителі з Донбасу.

Нарівні з новими ризиками, залишаються старі – віруси, шахрайство, дитяча порнографія. Т. Попова, голова правління ІнАУ радить встановлювати програми батьківського контролю, однак найголовніше – спілкуватися з дітьми про їх онлайн-досвід, обговорювати всі можливі ризики інтренте-середовища, разом встановлювати антивірус та «дружити» в соціальних мережах. Оскільки просто заборони, як правило, можуть дати зворотний ефект.

Про боротьбу з дитячою порнографією в Інтернеті говорила К. Турк, експерт Ради Європи: «Заборона певного контенту в онлайні завжди має ризик цензури інформації, і тут проявляється певний конфлікт із правами людини». Учасникам було представлено Посібник з прав людини для інтернет-користувачів, який був прийнятий Радою Європи у 2014 р. Він ознайомлює користувачів з їхніми правами в Інтернеті і можливими їх обмеженнями. Окрема увага в ньому приділена правам дітей, зокрема зазначено, що дітям має надаватися спеціальний захист від втурчання у їх фізичне, психічне та моральне благополуччя, у тому числі захист від сексуальної експлуатації.

Під час заходу було також презентовано онлайн-гру для дітей «Дикий Інтернет Ліс» (Through the Wild Web Woods), створену Радою Європи для того, щоб навчити дітей користуватися Інтернетом безпечно. Гра перекладена українською.

Ідея запровадити День безпечнішого Інтернету (англ. Safer Internet Day) ініційована Європейською комісією в січні 2004 р. Відзначається в другий вівторок лютого (цього року – 10 лютого) з метою підвищення культури користування Інтернетом, запобігання поширенню через інформаційні ресурси проявів дитячої порнографії, расової нетерпимості, тероризму. В Україні відзначається з 2009 р. Заходи до Дня безпечнішого Інтернету допомагають досягти об’єднання зусиль зацікавлених сторін – як державного, так і приватного секторів – задля підвищення рівня обізнаності етики поведінки при використанні інформаційних технологій, зокрема Інтернету, дітьми та молоддю ***(Діти в інтернеті стикаються з новими «воєнними ризиками» – дослідження // Телекритика (http://osvita.mediasapiens.ua/mediaprosvita/kids/diti_v_interneti_stikayutsya_z_novimi_voennimi_rizikami_doslidzhennya/). – 2015. – 10.02).***

***

Ученым из Великобритании удалось выяснить, что размер головного мозга человека зависит от количества друзей в соцсетях. Чем больше у пользователей социальных сетей друзей, тем больше объем серого вещества в отдельных участках мозга, пишет 24СМИ (http://24smi.org/news/22271-uchenye-razmer-mozga-zavisit-ot-kolichestva_newsya.html).

Такое заявление ученые сделали после первого этапа исследований с участием 200 человек. Все участники являются пользователями соцсетей. Первым делом учеными определялся объем серого вещества в мозге при

помощи магнитно-резонансного томографа. После этого исследователи проводили у испытуемых опрос о количестве друзей в сетях.

Сопоставив полученные данные, специалисты выяснили, что у участников опроса с большим количеством друзей (более 1000) отвечающая за эмоции височная часть мозга больше, чем у пользователей с малым количеством «френдов» (меньше 30). Однако это нельзя считать доказательством того, что эти люди умнее остальных, поскольку в некоторых случаях большой мозг не является залогом концентрированности на решениях определенных задач, заявили исследователи.

После первого этапа ученые желают провести ряд исследований, чтобы выяснить связь между объемом головного мозга и наличием друзей ***(Ученые: размер мозга зависит от количества друзей в соцсетях // 24СМИ (http://24smi.org/news/22271-uchenye-razmer-mozga-zavisit-ot-kolichestva_newsya.html). – 2015. – 2.02).***

Маніпулятивні технології

Гендиректор Twitter Д. Костоло признался, что его сервис проиграл войну с троллями и постоянно теряет из-за этого пользователей. Об этом стало известно из служебной записки его авторства, опубликованной изданием The Verge.

В своём внутреннем письме для сотрудников Д. Костоло не стеснял себя в выражениях, чтобы описать плачевное положение компании в борьбе с грубиянами.

«Мы проигрываем в вопросах борьбы с оскорблениями и троллингом уже несколько лет. Ни для кого не секрет, что весь остальной мир говорит об этом каждый день. Мы теряем активных пользователей одного за другим, будучи не в состоянии оперативно разбираться с оскорблениями, с которыми они сталкиваются ежедневно», – написал генеральный директор Twitter.

Д. Костоло назвал сложившуюся ситуацию абсурдной и возложил вину за неё на себя, признав, что за время своего руководства не сделал почти ничего для разрешения серьёзной проблемы. Чтобы избежать недопонимания, он даже прислал сотрудникам второе письмо, в котором подчеркнул, что снимает с них всю ответственность за поражение в борьбе с троллингом. «Давайте проясним вопрос о степени моей вины. Я беру ЛИЧНУЮ ответственность за то, что наша компания не справляется с этой задачей», – говорится в письме.

Гендиректор Twitter добавил, что признание – это первый шаг к разрешению проблемы, и пообещал обеспечить сотрудников, реагирующих на жалобы пользователей, всеми необходимыми ресурсами для того, чтобы сделать борьбу с троллингом более эффективной.

Поводом для писем Д. Костоло стала резонансная история женщины по имени Л. Уэст: крупные СМИ вроде The Guardian рассказали о том, как один из пользователей Twitter создал издевательский микроблог от имени её недавно ушедшего из жизни отца. На новостной сюжет обратили внимание сотрудники Twitter и обратились к гендиректору с вопросом о том, возможно ли как-то избежать похожих ситуаций в будущем.

Проблема борьбы с оскорблениями в сети стала особенно актуальной в связи с движением Gamergate, в рамках которого, в частности, домогательствам в Twitter и других соцсетях за свои высказывания в адрес геймеров подвергается известная феминистка А. Саркисян.

В декабре Twitter ускорил процесс приёма жалоб на грубое поведение пользователей, однако эти меры не принесли заметных плодов ***(Twitter признался в неспособности справиться с троллями // InternetUA (http://internetua.com/Twitter-priznalsya-v-nesposobnosti-spravitsya-s-trollyami). – 2015. – 6.02).***

***

У Швеції викрили мережу проросійських інтернет-тролів, які намагаються порушувати потрібні Росії питання та показують країну в потрібному руслі.

Незвичну активність помітила газета «Дагенс Нюхетер», повідомляє Шведське радіо. Журналісти помітили у шведських ЗМІ чималу кількість коментарів та повідомлень, проплачених російською владою.

Дослідник російської пропагандистської війни в Держінституті досліджень оборони FOI У. Франке вважає, що ці тролі ведуть активну роботу з поданням російської політики в кращому світлі. «Схоже, що певні типи новин і дискусій привертають до себе цих людей, які висловлюються у відповідності з лінією російської сторони. З великою часткою ймовірності, частина з них – російські мережеві тролі», – розповів він.

У. Франке уточнив, що не можна з упевненістю сказати, що ці люди фізично перебувають на території Швеції.

За його словами, як тролі можуть виступати й «корисні ідіоти» – люди, які поширюють інформацію російської пропаганди, не піддаючи її сумніву ***(У Швеції викрили мережу проросійських інтернет-тролів // Watcher (http://watcher.com.ua/2015/02/06/u-shvetsiyi-vykryly-merezhu-prorosiyskyh-internet-troliv/). – 2015. – 6.02).***

***

Російські інтернет-боти почали 6 лютого дуже активно поширювати цитату голови МЗС Німеччини, у якій той погрожує Україні санкціями в разі, якщо не буде знайдено політичного рішення української кризи:

«Мы введем санкции против Украины, если не будет найдено политическое решение».

«Накануне министр иностранных дел ФРГ Ф. Штайнмайер заявил, что если на Украине не будет найдено политическое решение, то правительство ФРГ оставляет за собой право “решительно выступить против украинского руководства, вплоть до принятия санкций”».

Ми вас здивуємо, але новина реальна, вийшла 4 лютого. Правда, є нюанс. Це 4 лютого 2014 р., а не 2015 р. Рік тому німці у відверто жорсткій формі спілкувались із представниками режиму В. Януковича.

Поширення новин річної давнини під видом цьогорічних – один з методів, який використовують російські пропагандисти.

Але нас зацікавила активність не лише ботів, а й спеціально створених сайтів в українських доменних зонах, які намагаються бути схожими на реальні новинарні сайти, але їх мета – легалізація російської пропаганди. Наприклад, на новині про МЗС «спалилися» сайти alfanews.com.ua, 1news.com.ua. Але таких сайтів існує десятки в українському сегменті Інтернету ***(Дмитренко О. В Уанеті існує мережа сайтів, які займаються легалізацією російської пропаганди // Watcher (http://watcher.com.ua/2015/02/06/v-uaneti-isnuye-merezha-saytiv-yaki-zaymayutsya-lehalizatsiyeyu-rosiyskoyi-propahandy/). – 2015. – 6.02).***

***

Немецкая международная радиостанция и телеканал Deutsche Welle планирует в апреле запустить мультимедийный англоязычный сервис DWNews, пишет Marketing Media Review (http://mmr.ua/news/id/germanija-zapustit-mezhdunarodnyj-novostnoj-servis-dlja-protivodejstvija-rossijskoj-propagande-43050/).

Как сообщает The Wall Street Journal, президент DW П. Лимбург видит цель нового медиа в «противостоянии пропаганде Путина» в Европе.

Как отмечает The Wall Street Journal, Россия через международный телеканал RT распространяет свое влияние за рубежом, создает все больше немецкоязычных и англоязычных программ.

Правительство канцлера Германии А. Меркель увеличило годовой бюджет Deutsche Welle более чем на 2 %.

Вместе с тем, некоторые работники DW, оппозиционные политики и другие критики негативно высказываются относительно такой инициативы. «Я не хочу видеть, как Deutsche Welle превращается в рупор немецкого Министерства иностранных дел», – говорит Х. Петцольд, член парламента от оппозиционной левой партии Die Linke.

Зато министр культуры и медиа М. Грютерс считает, что Deutsche Welle является маяком немецкой демократии в мире. Для некоторых, по ее словам, это единственная связь со свободным миром.

Deutsche Welle в настоящее время говорит на более 30 языках, его аудитория насчитывает 100 млн зрителей еженедельно по всему миру ***(Германия запустит международный новостной сервис для противодействия российской пропаганде // Marketing Media Review***

(http://mmr.ua/news/id/germanija-zapustit-mezhdunarodnyj-novostnoj-servis-dlja-protivodejstvija-rossijskoj-propagande-43050/). – 2015. – 30.01).

***

Олександрійський міський голова С. Цапюк на особистій сторінці у Facebook поширює інформацію із сайту «Новости Донецкой Республики».

Сайт є одним із джерел інформації про терористичну організацію «ДНР» та постійно розповідає про діяльність «ДНР» та її очільників, цитує керівників терористів, розміщує відео- та аудіозаписи терористів.

Також С. Цапюк є прихильником таких груп Facebook, як «Стоп-майдан» та каналу «112», які популяризують відверто антиукраїнські погляди.

Цікаво, що серед тих, кому ця публікація С. Цапюка сподобалась, фігурує В. Кукуруза – колишній Пантаївський селищний голова, який був засуджений за організацію замовного вбивства та за отримання хабара. В. Кукуруза неодноразово схвально оцінював діяльність мера та став депутатом міської ради і Пантаївським селищним головою саме за попереднього мерства С. Цапюка. Тоді ж, при попередньому керуванні С. Цапюком Олександрією, В. Кукурузу задокументували правоохоронці і запроторили за грати за скоєні тяжкі злочини.

Висловлювання тих, хто є прихильниками поширюваних мером Олександрії новин, досить прикметні. Наприклад, В. Кукуруза прямо вказує на своє ставлення до України: «Буду краток, – мы с Тобой не идиоты и прекрасно понимаем, что это та же инфраструктура, что и на нашем Майдане – Америке все неймется и она нагло лезет к богатствам Сибири. Развал России приведет к полному краху Империи, чего в принципе и добиваются США, и тут надо принимать решительные действия – утопить в крови, чтобы не повадно было американским прихвостням…»

Нещодавно на Кіровоградському обласному телебаченні обговорювалося питання антидержавницьких поглядів представників влади і керівників комунальних закладів, де підкреслювалось, що поширення сепаратистської інформації через соціальні мережі є неприпустимим вчинком для тих, хто працює на державу і територіальні громади. Такі чиновники не мають права працювати в органах влади та очолювати заклади, що фінансуються з бюджету. Після викриття у поширенні антиукраїнської інформації, під тиском громадськості звільнився з займаної посади директор комунального закладу «Кіровоградський обласний центр туризму, краєзнавства та екскурсій учнівської молоді» А. Михайлюк.

Потім з цього ж питання надав коментар голова Кіровоградської обласної держадміністрації С. Кузьменко. Він, зокрема, заявив, що державний службовець повинен мати проукраїнські погляди, а посадовець з антиукраїнською позицією – «це не логічно». С. Кузьменко наголосив, що відстежувати такі антиукраїнські погляди держслужбовців мають громадські активісти та небайдужі громадяни, а також правоохоронні органи

(Олександрійський міський голова поширює новини терористичної організації «ДНР» // Олександрійські новини (http://alnews.com.ua/news/11857-oleksandrijjskijj-miskijj-golova-poshiryue-novini-teroristichnoyi-organizaciyi-dnr). – 2015. – 2.02).

Зарубіжні спецслужби і технології «соціального контролю»

Сервіс мікроблогів Twitter опублікував новий піврічний звіт зі статистикою про запити влади різних країн світу про розкриття інформації користувачів і видалення інформації.

Судячи зі звіту, можна зробити висновок, що частота запитів особистих даних користувачів продовжує зростати. За друге півріччя 2014 р. їх кількість збільшилася на 40 % – до 2871.

«На наше переконання, публікація цієї статистики відповідає інтересам суспільства, особливо в наш час зростаючого занепокоєння про стеження з боку держав», – заявив керівник правової політики Twitter Д. Кессель.

Найбільша кількість запитів про видалення інформації (477) в липні – грудні 2014 р. надійшла з Туреччини, де перед президентськими виборами прогримів корупційний скандал навколо нинішнього президента країни Р. Ердогана. Задоволені були 50 % запитів. Але з 356 турецьких запитів на деанонімізацію користувачів не був задоволений жоден. Торік Twitter був деякий час заблокований у Туреччині, перш ніж Конституційний суд країни не скасував це рішення.

На другому місці опинилася Росія з 91 запитом про видалення інформації, з яких задоволено 13 %, заблоковано три акаунта. У порівнянні з першим півріччям 2014 р. їх загальна кількість більш ніж подвоїлася. Усі окрім одного запити надійшли від Роскомнадзора, причому вони включають застосування закону № 398-ФЗ у частині блокування екстремістських сайтів.

«Ми відмовилися виконувати декілька запитів про блокування популярних противників російського уряду та інші вимоги обмежити свободу слова стосовно до масових ненасильницьких виступів в Україні», – повідомив сервіс мікроблогів.

За запитами про розкриття особистих даних беззастережно лідирують США, на які довелося більше половини їх світової кількості (1622). Задоволено було 80 % запитів. З Росії надійшло 108 подібних запитів, не задоволено жодного.

На 81 % за півроку збільшилася кількість запитів на видалення матеріалів, захищених авторським правом, – до 16 648 випадків. У 66 % випадків запити було задоволено ***(Twitter відмовився блокувати інформацію про Україну на запит Росії // Watcher***

(http://watcher.com.ua/2015/02/10/twitter-vidmovyvsya-blokuvaty-informatsiyu-pro-ukrayinu-na-zapyt-rosiyi/). – 2015. – 10.02).

***

Британська армія створює спеціальний підрозділ воїнів Facebook, що володіють навичками проведення психологічних операцій і використання соціальних медіа для ведення нетрадиційних бойових дій, характерних для інформаційного століття, пише The Guardian. На таке рішення вплинули, зокрема, дії Росії в Україні, пише Корреспондент.net (http://ua.korrespondent.net/world/3474575-brytanska-armiia-stvoruiie-komandu-voiniv-Facebook-Guardian).

77-ма бригада базуватиметься в Хермітіджі, поблизу Ньюбері в Беркширі, і до її складу буде включено близько 1500 осіб, які будуть переведені туди з частин, розташованих у різних місцях країни. Формально цю бригаду буде створено у квітні.

Вона відповідатиме за те, що називається нелетальними бойовими діями. І ізраїльська, і американська армії вже активно займаються проведенням психологічних операцій. На основі 24-годинної інформації, смартфонів і соціальних медіа, включаючи Facebook і Twitter, цей підрозділ буде намагатися контролювати наратив.

Особлива перевага при підборі кадрів буде віддаватися солдатам, які мають журналістську підготовку і знайомим із соціальними медіа.

«77-а бригада створюється для того, щоб об'єднати численні існуючі та розроблювані можливості, які є виключно важливими для того, щоб відповісти на виклики сучасних конфліктів і військових дій. Її створення означає визнання того, що на дії противника в сучасних умовах ведення війни можна вплинути такими методами, які не обов'язково є насильницькими», – сказав офіційний представник армії.

Цей крок частково є наслідком проведення операцій проти повстанців в Афганістані. Його також можна розглядати як відповідь на події останнього року, у тому числі на дії Росії в Україні, особливо в Криму, і на захоплення Ісламською державою значних територій Сирії та Іраку.

НАТО поки не змогло знайти противаги тому, що, на думку американських і британських фахівців, «робить Росія, коли вона, створюючи конфліктну ситуацію, спрямовує свої регулярні війська під виглядом місцевих ополченців, що дозволяє президенту В. Путіну уникати відповідальності».

Ісламська держава продемонструвала свою здатність ефективно використовувати соціальні медіа для залучення у свої лави бойовиків з усього світу.

Армія оборони Ізраїлю стала піонером у використанні збройними силами держави соціальних медіа, і її спеціальні підрозділи займаються подібною роботою з часу проведення операції Литий свинець (Cast Lead), тобто з часу війни в Газі у 2008–2009 рр.

Армія оборони Ізраїлю діє на 30 платформах, включаючи Twitter, Facebook, YouTube і Instagram, і проводить цю роботу шістьма мовами. «Це дозволяє працювати з аудиторією, яка в іншому випадку була б для нас недоступною», – зазначив офіційний представник ізраїльської армії.

До Армії оборони Ізраїлю звернулися вже представники кількох західних країн, які хотіли б познайомитися з накопиченим ізраїльськими фахівцями досвідом.

Під час війни в Газі влітку минулого року і проведення операції Рубіж оборони (Protective Edge) Армія оборони Ізраїлю і військове крило ХАМАСу Бригада аль-Кассам активно використовували Twitter, а іноді вони вступали в безпосередній бойовий контакт один з одним у цьому сервісі.

Створення 77-ї бригади відбувається в той момент, коли командувач штабу спеціальних операцій НАТО генерал-лейтенант М. Вебб у своєму виступі у Вашингтоні цього тижня висловив занепокоєння щодо дій Росії та Ісламської держави. «Штаб з проведення спеціальних операцій – це унікальне місце для того, щоб займатися цими проблемами, – сказав він. – Ми воліємо непрямий підхід. Ми можемо діяти без ескалації і агресивності. Ми схильні розглядати речі не під прямим кутом і повністю визнаємо, що довіра, обмін інформацією та міжвідомче співробітництво відіграють ключову роль» ***(Британська армія створює команду воїнів Facebook – Guardian // Корреспондент.net (http://ua.korrespondent.net/world/3474575-brytanska-armiia-stvoruiie-komandu-voiniv-Facebook-Guardian). – 2015. – 3.02).***

***

В СБУ Полтавской области открыли уголовное производство против пользователя соцсети, у которого на странице в Facebook следователи увидели призывы к совершению действий, целью которых является изменение границ территории или государственной границы Украины.

Уголовное производство открыто по ч. 1 ст. 110 УК Украины (умышленные действия, совершенные с целью изменения границ территории или государственной границы Украины, а также публичные призывы или распространение материалов с призывами к совершению таких действий).

Как сообщил корреспонденту «Полтава, Комментарии» руководитель пресс-группы СБУ в Полтавской области А. Скрыльник, пользователь – житель Киева. Все необходимые материалы сотрудники полтавского СБУ передали своим столичным коллегам.

Пользователю грозит заключение до трех лет ***(В СБУ открыли производство против пользователя соцсети // InternetUA (http://internetua.com/v-sbu-otkrili-proizvodstvo-protiv-polzovatelya-socseti). – 2015. – 11.02).***

***

В Верховной Раде зарегистрирован проект внесения изменений в Закон Украины «Об информации» (относительно распространения массовой информации в сети Интернет). Документ разработал и подал внефракционный народный депутат В. Петевка, член Комитета ВР по вопросам аграрной политики.

В своем проекте автор дает определение слову «блогер». По его мнению, блогерами являются владельцы сайтов, а также владельцы страниц сайтов, на которых размещается массовая информация. Именно так называемым блогерам и посвящен весь документ. В частности, В. Петевка предлагает на законодательном уровне утвердить правила их поведения в Интернете.

«Целью законопроекта является урегулирование прав и обязанностей блогера, а также запрета использования сайта или его страницы в целях сокрытия или фальсификации общественно значимых сведений, распространения заведомо недостоверной информации под видом достоверных сообщений», – сказано в пояснительной записке к документу.

Согласно проекту закона, блогер не должен использовать свой сайт или свою страницу в сети для совершения уголовно наказуемых дел, для разглашения государственных тайн, для распространения материалов, содержащих публичные призывы к террористической деятельности или публично оправдывающих терроризм, а также других экстремистских материалов.

Помимо этого, пользователи Интернета не должны распространять материалы, которые пропагандируют порнографию, культ насилия, и материалы, содержащие нецензурную брань. Пользователи сети обязаны проверять достоверность размещенной информации, а также не нарушать права и законные интересы граждан и организаций, в том числе их честь, достоинство и деловую репутацию.

В то же время в своем документе В. Петевка разъясняет и то, что украинским блогерам можно делать на своих страницах. Так, они могут размещать рекламу, свободно искать, получать, и распространять законную информацию. А также высказывать в блогах свое мнение, но при этом обязательно указывать свою фамилию или псевдоним под этим суждением.

По словам управляющего партнера адвокатского объединения «Юскутум» А. Афяна, на первый взгляд законопроект может показаться таким, который несет положительный смысл, но если в него вчитаться, видно, что все его нормы абсурдны. «Во-первых в украинском законодательстве нет такого определения как блогер. Это все равно, что определение “хипстера” и подобных ему слов. По логике депутата, блогерами являются все пользователи Интернета и своим законопроектом он их загоняет в жесткие цензурные рамки», – отметил А. Афян, добавив, что законопроект В. Петевки напоминает ему закон Российской Федерации о

блогерах. «Но там хоть было оговорено количество подписчиков», – резюмирует собеседник «Капитала».

Напомним, в России с 1 августа прошлого года вступил в силу так называемый закон о блогерах. Согласно ему блогеры, чьи страницы посещают 3 тыс. и более пользователей в сутки, должны регистрировать свой ресурс в специальном реестре Роскомнадзора. От таких блогеров также требуется сообщать свои контактные данные и соблюдать практически все основные требования, относящиеся к средствам массовой информации ***(Верховная Рада намерена взять под контроль блогеров // InternetUA (http://internetua.com/verhovnaya-rada-namerena-vzyat-pod-kontrol-blogerov). – 2015. – 14.02).***

***

Китайское правительство ужесточило контроль за Интернетом, сделав умнее интернет-фильтр, отделяющий китайских пользователей от всемирной сети. Об этом сообщает The Wall Street Journal (WSJ).

Последняя модернизация системы веб-фильтров Китая, называемых «Великим файерволом», затруднила для китайцев использование виртуальных частных сетей (virtual private networks, VPN), которые обычно применяются, чтобы обойти блокировку и подключиться к американским сервисам, таким как Facebook и Twitter.

Пользователи отмечают, что государство перешло на автоматическое блокирование VPN. Если раньше прекращался доступ только к известным серверам с поддержкой этого сервиса, то теперь прерывается трафик, напоминающий связь через виртуальную частную сеть.

Китайские власти официально подтвердили блокирование VPN-сервисов, объяснив, что для развития Интернета были необходимы такие меры. Неработоспособность своих сервисов зафиксировала компания Astrill, крупнейшая из предоставляющих доступ через виртуальные частные сети.

Введение новых мер показывает дальнейшую работу Китая по созданию собственного Интернета, который будет находиться под полным государственным контролем. Такой подход позволяет правительству блокировать доступ к контенту, критикующему государственный строй, а также обеспечивает преимущество китайских интернет-компаний на внутреннем рынке.

VPN позволяет шифровать данные, передаваемые между пользователем и сервером сервиса. Затем сервис может делать запрос к сайтам, запрещенным в месте расположения пользователя (задавать ключевое слово в поиске Google, оставлять пост в Facebook), а потом передавать пользователю полученную информацию. Работа сервиса VPN протекает для пользователя незаметно, однако оператор не может контролировать, к каким ресурсам и с какими запросами обращается абонент. Таким образом, через VPN китайские пользователи обходили «Великий файервол» ***(Китай усложнил преодоление «Великого файервола»***

интернет-пользователям // InternetUA (http://internetua.com/kitai-uslojnil-preodolenie--velikogo-faiervola--internet-polzovatelyam). – 2015. – 1.02).

***

Власти КНР потребовали от всех пользователей сети использовать только своё реальное имя и дать провайдерам письменное соглашение не критиковать в Интернете политику коммунизма. Об этом сообщает АР.

Указ использовать настоящее имя относится в первую очередь к социальным сетям и блог-платформам, а также к комментариям на сайтах. Подобное правило уже существует с 2012 г., но относилось оно лишь к некоторым пользователям китайского Интернета ***(Китайские власти запретили анонимность в Сети // InternetUA (http://internetua.com/kitaiskie-vlasti-zapretili-anonimnost-v-seti). – 2015. – 4.02).***

***

Служба безпеки України затримала громадянку України, яка адмініструвала кілька груп сепаратистської спрямованості в соціальних мережах, де поширювала заклики до створення на Харківщині так званої «народної республіки», схвалювала діяльність терористів, викривляла інформацію про хід антитерористичної операції. Про це повідомляє прес-центр СБУ.

Як встановлено слідчими, 24-річна мешканка Харківської області через організовані нею спільноти в соцмережах збирала кошти для бойовиків терористичних угруповань, організовувала придбання для них технічних засобів та камуфляжного одягу, вербувала людей до незаконних збройних формувань. Вона поширювала інформацію про диверсії та теракти, скоєні терористичною групою так званих «харківських партизан», закликала наслідувати їхньому прикладу.

СБУ повідомляє, що крім того затримана видавала себе за волонтерку і під прикриттям здійснювала протиправну діяльність на підтримку терористичних організацій «ДНР» та «ЛНР».

«24-річна мешканка Харківської області, підтримуючи тісні зв’язки з терористами, вела подвійне життя. Вона підступно проникла у волонтерські кола. За завданням бойовиків зловмисниця відвідувала місця дислокації підрозділів Збройних сил України, де робила приховану фото- та відеозйомку української військової техніки, позицій особового складу, об’єктів життєзабезпечення. Зібрану інформацію спільниця терористів передавала ватажкам бандформувань, які використовували відомості для обстрілів сил АТО, організації диверсій у мирних містах», – повідомляє Служба безпеки України.

СБУ також зазначає, що підозрювана була затримана на гарячому під час зйомки на мобільний телефон місця тимчасової дислокації військової

бронетехніки. У пам'яті телефону виявлені електронні адреси, на які спільниця терористів відправляла відзняті кадри.

Під час обшуку в помешканні затриманої вилучено бойову гранату, матеріали прихованої відеозйомки, мікрофон дальньої дії, агітаційні матеріали антиукраїнського змісту.

Затриманій оголошено про підозру у скоєнніі злочину за ч. 2 ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України. Слідство триває ***(На Харківщині СБУ затримала особу, що адмініструвала сепаратистські групи у соцмережах // Телекритика (http://www.telekritika.ua/pravo/2015-02-04/103292). – 2015. – 4.02).***

***

Офіційні особи в Пакистані заявляють, що заборона YouTube в країні продовжуватиметься «на невизначений термін». Про це пише radiosvoboda.org

Агентство AFP цитує чиновника, який побажав залишитись неназваним, як підтвердження новини 7 лютого після заяви міністра інформаційних технологій і телекомунікацій Пакистану А. Рехман про те, що заборона залишатиметься в силі.

Пакистан заблокував сайт для обміну відеоматеріалами у вересні 2012 р. після того, як на ресурсі розмістили фільм «Невинність мусульман», який викликав хвилю протестів у всьому світі як антиісламський фільм.

Відтоді пакистанські чиновники кажуть, що вони не знайшли іншого способу відфільтровувати богохульні відеофайли, ніж повністю блокувати YouTube.

Прихильники свободи слова кажуть, що Ісламабад використовує релігію як привід для того, щоб запроваджувати цензуру ***(Заборона YouTube в Пакистані продовжуватиметься – чиновники // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42357/118/lang,ru/). – 2015. – 9.02).***

***

Евросоюз добивается права шпионить за пользователями интернет-сервисов Skype и Viber, пишут Новости ИТ.

О необходимости разработки законного способа перехвата данных в Skype и Viber заявило агентство Евроюст. Согласно данным, такие меры необходимы в целях наблюдения за деятельностью радикально настроенных граждан, вернувшихся в Европу из стран Ближнего Востока.

Агентство выпустило доклад, в котором отмечается, что экстремисты все чаще используют различные интернет-сервисы для пропаганды и вербовки новых сторонников среди европейских граждан.

В свою очередь передача данных посредством глобальной сети препятствует расследованию дел о терроризме, как с технической, так и с юридической точки зрения.

Таким образом, необходимо разработать правовые основы перехвата личных данных пользователей для выявления возможных террористов ***(Евросоюз будет шпионить за пользователями Skype и Viber // Новости ИТ (http://www.novostiit.net/evrosoyuz-budet-shpionit-za-polzovatelyami-skype-i-viber-00015626). – 2015. – 8.02).***

***

У Росії заблокують понад 60 сайтів за порушення законодавства. Причиною блокування Роскомнагляд називає порушення законодавства про захист персональних даних.

Як повідомляє сайт наглядового органу, блокування відбудеться відповідно до рішення Симоновського районного суду м. Москви від 29 січня 2015 р.

На сайтах, що будуть заблоковані, переважно розміщувалися різноманітні бази даних та довідники з персональними даними росіян.

Рішення суду набере чинності 1 березня 2015 р. Після цього зазначені в ньому ресурси буде занесено до єдиного реєстру забороненої інформації та заблоковано операторами зв'язку ***(У Росії заблокують понад 60 сайтів за порушення законодавства // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/media_law/government/u_rosii_zablokuyut_ponad_60_saytiv_za_porushennya_zakonodavstva/). – 2015. – 12.02).***

***

В новом номере британской версии журнала Wired вышла колонка «гендиректора крупнейшей российской группы электронной коммерции» (цитата по журналу) М. Гавэ под названием «Данные говорят, что Google и Facebook нужно регулировать». Она пишет, что сегодня данными практически всего мира заправляет горстка технологических гигантов, и любая дискуссия между прогрессом и защитой частной жизни рассматривается как выбор между позициями «за данные, и, следовательно, за инновации» и «застрял в Средневековье».

М. Гавэ сетует, что в таких условиях сложно заявить «я против Big data». Big data – технологии анализа огромных объемов данных из разных источников. Почему транснациональные корпорации в работе с этими данными будут ставить интересы пользователей превыше собственных? М. Гавэ считает, что надежды на саморегуляцию в защите персональных данных наивны, но они могут привести к опасным последствиям. Она вспоминает, что компании энергосектора озаботились безопасностью на производстве только после громких аварий на нефтедобывающих вышках, показа в теленовостях сюжетов с птицами, испачканными нефтью, – и появлением законопроектов об охране природы.

Гендиректор «Озона» считает, что без госрегулирования не обойтись и в Интернете: иначе все закончится гигантскими утечками данных пользователей вместо утечек нефти. А непрозрачность в ценообразовании на рынке данных в Интернете напоминает М. Гавэ цены монополистов связи, которые во многих странах – например, в Евросоюзе – в итоге власти начали регулировать ***(Гендиректор Ozon.ru предложила регулировать работу Facebook и Google // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42394/118/lang,ru/). – 2015. – 11.02).***

Проблема захисту даних. DOS та вірусні атаки

Facebook обновил настройки приватности. Каждый пользователь, посетивший соцсеть после 30 января, автоматически считается принявшим новые условия.

Основное изменение в новой политике состоит в том, что Facebook теперь имеет право собирать данные пользователя от любого просмотренного им «партнерского сайта», а также в самой сети. Это может быть любой сайт, который использует рекламную платформу Atlas.

Использование данных для таргетирования рекламы не является новинкой в Facebook, но теперь пользователи будут подвергаться отслеживанию во всем Интернете, так как понятие «партнерские сайты и приложения» включает в себя большинство популярных приложений.

Facebook подчеркивает, что не передает персональную информацию – имя и адрес электронной почты – которая может быть использована для связи с пользователем или его идентификации.

При этом Facebook не позволяет отказаться от его сбора данных. Но пользователи, которые хотят знать, какие именно персональные данные хранит соцсеть, могут загрузить отчет об общих настройках аккаунта из меню настроек Facebook.

Новая рекламная политика Facebook означает, что если пользователь вошел в Facebook с мобильного устройства или десктопа, соцсеть будет автоматически отслеживать, какие сайты посещает пользователь, как он взаимодействует с ними (например, делает ли покупки) – и что он делает в мобильных приложениях. Facebook может использовать эту информацию для создания таргетированной рекламы.

Facebook позволяет пользователям жаловаться на конкретные таргетированные объявления в момент просмотра. Но предотвратить отслеживание с помощью функции браузера «Не отслеживать» невозможно.

Между тем исследователи обнаружили, что «лайки» в Facebook – даже если это всего лишь «лайки» Гарри Поттеру или Тейлор Свифт – могут быть использованы для создания подробного портрета личности пользователя.

Алгоритм, созданный исследователями Стэнфорда и Кембриджа, на основе «лайков» может создать более точный портрет личности, чем ближайшие друзья или семья пользователя. Можно предположить, что использовать персональную информацию для построения портрета личности могут не только компании, но и правоохранительные органы.

Представители Facebook в конце ноября 2014 г. официально уведомили пользователей о том, что социальная сеть обновила Политику управления данными и Правила в отношении файлов cookie. Все изменения вступили в силу с 1 января 2015 г. ***(Facebook обновил настройки приватности // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_obnovil_nastroyki_privatnosti). – 2015. – 12.02).***

***

Как сообщают исследователи безопасности из Websense, им удалось обнаружить новое вредоносное приложение, использующее весьма хитрые методы сокрытия своей вредоносной активности на системе. Вирус, получивший название F0xy, активно использует популярные легитимные веб-сайты и сервисы в целях маскировки вредоносной активности.

Первые версии программы появились в открытом доступе 13 января 2015 г., однако с тех пор функционал вируса неоднократно обновлялся. Так, изначально вредонос инфицировал только компьютеры на базе Windows Vista или более поздних версий ОС от Microsft, но теперь F0xy способен заражать и Windows XP.

При этом в ходе проверки сервисом VirusTotal распознать вредоносное ПО смогли лишь пять антивирусных решений. В настоящее время, по данным исследователей, этот показатель несколько увеличился.

При этом разработчики не стали прибегать к применению обфускации, чтобы не вызывать лишних подозрений ***(F0xy – вирус, использующий «умные» методы для сокрытия своего присутствия на системе // InternetUA (http://internetua.com/F0xy---virus--ispolzuuasxii--umnie--metodi-dlya-sokritiya-svoego-prisutstviya-na-sisteme). – 2015. – 1.02).***

***

Хакеры атакуют около 30 тыс. веб-сайтов предприятий в сутки

Прошлый год ознаменовался рядом громких краж финансовой информации у крупных компаний и банков, однако исследования показывают, что больше всего пострадали мелкие фирмы.

Среднестатистическая атака мошенников, как правило, стоит мелким и средним компаниям от 65 тыс. до 115 тыс. фунтов стерлингов. Об этом сообщается в исследовании PwC. Некоторые компании становятся жертвами кибермошенников до шести раз в год. Если крупные предприятия могут быстро справиться с потерями, то для мелких и средних затраты таких масштабов могут стать причиной краха.

Несмотря на это, многие небольшие компании, как правило, пренебрегают мерами безопасности, поскольку хотят сосредоточить свои усилия на основной коммерческой деятельности, говорят эксперты. Хуже того, компании быстро пытаются внедрять новейшие интернет-технологии и платежные решения, не задумываясь о соответственном уровне защиты.

Более 30 тыс. веб-сайтов небольших компаний становятся жертвами кибермошенников ежедневно. Около 250 тыс. новых вирусов появляются каждый день, а атаки становятся все серьезнее. Компаниям следует задуматься о надежной защите, чтобы не понести серьезных потерь от преступников в сети ***(Хакеры атакуют около 30 000 веб-сайтов предприятий в сутки // InternetUA (http://internetua.com/hakeri-atakuuat-okolo-30-000-veb-saitov-predpriyatii-v-sutki). – 2015. – 10.02).***

***

В 2015 г. ожидается всплеск активности банковских троянов. Ожидается, что в этом году злоумышленники продолжат развивать вредоносное ПО Dyreza и Dridex.

2014 г. ознаменовался устранением двух превалирующих семейств вредоносов – банковских троянов Gameover Zeus (GOZ) и Shylock. Однако, как сообщают специалисты ИБ-компании CrowdStrike, их место тут же заняло новое вредоносное ПО – Dyreza и Dridex (также известное как Bugat). Эксперты предсказывают, что в 2015 г. увеличится активность не только банковских троянов, но и программ-вымогателей.

Как отмечается в годовом отчете Global Threat Intel, Dyreza использует более упрощенный подход к банковскому мошенничеству, перехватывая логины и HTTP POST данные в банковской SSL сессии. В свою очередь Dridex представляет собой типичный банковский троян. Его главная функциональность – кража учетных данных для доступа к онлайн-банкингу, так что злоумышленники получают доступ к денежным средствам жертвы и могут перевести их на другой счет. По словам специалистов, для загрузки Dyreza на компьютер жертвы злоумышленники используют троян Upatre, который ранее применялся загрузки GOZ.

В 2015 г. эксперты CrowdStrike прогнозируют дальнейшее развитие банковских троянов, в том числе Dyreza и Dridex. К примеру, в ноябре прошлого года в арсенал Dridex был добавлен функционал peer-to-peer (P2P). Кроме того, не исключено появление новых угроз, следующих бизнес-модели, в которой фишинговые приманки распространяются спамботами, использующими первоклассные загрузчики для маскировки функциональной части трояна ***(В 2015 году ожидается всплеск активности банковских троянов // InternetUA (http://internetua.com/v-2015-godu-ojidaetsya-vsplesk-aktivnosti-bankovskih-troyanov). – 2015. – 15.02).***

***

Отчет по интернет-безопасности, представленный компанией Akamai Technology, показал, что за последний год число DDoS-атак увеличилось почти в два раза. Практически половина из них были мультивекторными. Количество DDoS-атак со скоростью 100 ГБ в секунду возросло на 200 %, а их длительность увеличилась на 28 %.

Самыми распространенными были атаки на базе UDP, а наиболее используемые протоколы для тактики отражения – NTP, CHARGEN и SSDP.

Наибольшее число DDoS-атак было осуществлено с территории США (31,54 %). На втором месте оказался Китай (17,61 %), далее следуют Германия (12 %), Мексика (11,69 %), Франция (7,64 %), Индия (4,61 %), Испания (4,12 %), Великобритания (3,8 %), Корея (3,65) и Россия (3,64 %).

Наиболее популярными для нападения хакеров в 2014 г. стали игровые сервисы. Рождественская кибератака на Microsoft Xbox Live и Sony PlayStation Network вынесли игровую индустрию на первое место по частоте и количеству кибернападений.

Д. Саммерс из компании Akamai рассказал в отчете, что все чаще злоумышленники начали прибегать к новой тенденции в кибернападении. В частности, они предлагают остановить DDoS-атаку за выкуп ***(Akamai Technology: Количество DDoS-атак за год увеличилось почти в два раза // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/02/03/Q4-2014-State-of-the-Internet--Security-Report-Released.html). – 2015. – 3.02).***

***

Сотрудники Trend Micro обнаружили две мобильные программы для iOS, используемые для прослушки коммуникаций в высших кругах власти. Успешному проникновению туда способствует новая тактика, избранная пока еще неизвестными инициаторами кампании шпионажа, получившей название Operation Pawn Storm. Она заключается в том, что атаки направлены не на главную цель, а на ее непосредственное окружение – «пешки» (pawn). Инфицировать пытаются устройства, принадлежащие людям, которые входят в круг общения высокопоставленных чиновников, военных и сотрудников масс-медиа.

Эти «пешки» часто находятся в одном помещении с крупными фигурами или могут обмениваться с ними сообщениями, содержащими желательную для хакеров информацию.

Атака начинается с фишинговой почты, обычно имеющей отношение к мероприятию, в котором реципиент может быть заинтересован принять участие. Ссылка внутри сообщения направляет жертвы на сайт с инструкциями по установке приложения. При нажатии на него происходит загрузка и запуск ПО, работающего на заднем плане, собирая текстовые сообщения, списки контактов, картинки и данные геолокации.

Фишинговое письмо и программный код написаны по-английски, т. е. ориентированы преимущественно на англоговорящих жертв.

Trend Micro обнаружила два типа приложений, XAgent и MadCap. На устройствах iOS 7 пиктограмма Xagent скрыта, а при попытке остановить программу, удаляя процесс, она сразу стартует снова. В iOS 8 ее иконка остается видимой на рабочем столе и автоматического рестарта не происходит. MadCap во всем аналогична Xagent, но устанавливается только на устройствах с модифицированным ядром (Jailbreak).

Trend Micro продолжает собирать информацию, которая в итоге должна позволить идентифицировать хакеров. Д. Клэй, старший менеджер Trend Micro по глобальным угрозам для коммуникаций, уверен, что злоумышленники не откажутся от продолжения этой кампании, которая, судя по всему, оказалась для них весьма эффективной.

До тех пор пока не найдено более радикальное решение проблемы, он рекомендует устанавливать на смартфоны защитные программы, способные выявлять работу скрытых приложений ***(Хакеры шпионят за жертвой, проникая в круг ее общения // InternetUA (http://internetua.com/hakeri-shpionyat-za-jertvoi--pronikaya-v-krug-ee-obsxeniya). – 2015. – 6.02).***

***

Злоумышленники отправляют пользователям Facebook поддельные уведомления о блокировке их учетной записи. Из сообщений следует, что учетные записи «заморожены», согласно обновлениям, внесенным в соглашение об условиях пользования социальной сети.

Уведомление, отправленное с электронной почты и якобы подписанное командой Facebook, просит пользователей перейти по ссылке TermsPolicies.pdf.exe, которая перенаправляет их на электронный адрес http://ladiezspoy[.]com/ с трояном-вымогателем CTB-Locker.

Зараженный файл был обнаружен с помощью антивирусных программ службы VirusTotal.

Напомним, что ранее компания Malwarebytes предупредила о подобной фишинговой компании, ориентированной на пользователей Google Chrome.

Судя по всему кибератаки совершались одними и теми же хакерами ***(Злоумышленники используют поддельную учетную запись Facebook для распространения вирусов // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-poddelnuua-ucsetnuua-zapis-Facebook-dlya-rasprostraneniya-virusov). – 2015. – 5.02).***

***

Facebook запускает социальную сеть ThreatExchange для профессионалов в области кибербезопасности, пишет The Financial Times. Пользователям платформы предложат обмениваться информацией об угрозах, которые могут привести к кибератакам.

Facebook усиливает свою работу в этой сфере, сотрудничая с другими технокомпаниями, среди которых Yahoo и Pinterest, отмечает издание.

Как рассказал М. Хэммел из Facebook, платформу ThreatExchange разработали на основе системы, которая уже используется внутри компании, чтобы упростить каталогизацию угроз сайту в режиме реального времени. По словам М. Хэммела, вместе с Yahoo и Pinterest «мы защищаем довольно внушительную долю Интернета».

Издание обращает внимание, что запуск нового проекта произошел в период, когда Facebook пытается расширить свою деятельность, выходя за пределы инструментов для социального общения пользователей с друзьями и родственникам. Ранее компания разработала приложение и сайт Facebook at Work для профессионалов ***(Facebook запускает соцсеть для экспертов по кибербезопасности // InternetUA (http://internetua.com/Facebook-zapuskaet-socset-dlya-ekspertov-po-kiberbezopasnosti). – 2015. – 12.02).***

***

51-летний гражданин Великобритании Й. Салливан сознался в осуществлении ряда DDoS-атак на сайты социальных служб государства, включая ресурсы по предотвращению преступности и предоставлению социального жилья. Об этом сообщает издание The Register.

Й. Салливан также сознался в осуществлении в 2013 г. атак на частные компании, включая межнациональные банки. В это время он сотрудничал с активистами Anonymous. Стоит отметить, что атаки на сайты социальных служб осуществлялись скорее по личным мотивам – обычно Anonymous не препятствует работе подобных ведомств.

Действия Й. Салливана привели к тому, что более 300 веб-сайтов были временно выведены из строя. Тысячи людей не могли получить доступ к нужным им сервисам. При этом Й. Салливан не пытался взломать серверы или похитить личные данные клиентов соцслужб.

Для того чтобы арестовать Й. Салливана, правоохранители осуществили специальную операцию при поддержке Отдела по борьбе с организованной преступностью Северо-западного округа Великобритании. Полицейским удалось связать DDoS-активность с одной учетной записью в Twitter, которая координировала атаки. Преступника задержали в июле 2013 г. Экспертиза показала, что используемое Й. Салливаном ПО было аналогично тому, которое применяли активисты Anonymous при атаках на другие сайты ***(51-летний активист Anonymous сознался в осуществлении DDoS-атак на сайты социальных служб // InternetUA (http://internetua.com/51-letnii-aktivist-Anonymous-soznalsya-v-osusxestvlenii-DDoS-atak-na-saiti-socialnih-slujb). – 2015. – 12.02).***

***

Немецкая автомобильная компания BMW исправила уязвимость, позволяющую злоумышленникам разблокировать двери более 2,2 млн машин

серии Rolls-Royce, Mini и BMW. Об этом сообщается в пресс-релизе концерна.

По словам представителей BMW, уязвимость обнаружили мотористы Всеобщего немецкого автомобильного клуба (ADAC). Брешь затрагивала машины, оснащенные ПО ConnectedDrive со встроенными SIM-картами. ConnectedDrive позволяет авторизованным водителям удаленно активировать механизмы блокировки дверей, получать информацию об обстановке на дороге, изменять настройки кондиционера и просматривать другую информацию, связанную с автомобилем.

Уязвимость существовала из-за ошибки при передаче данных. BMW заверяет, что брешь не позволяла злоумышленникам захватить контроль над критическими функциями автомобиля – управлением, разгоном и торможением. Более того, компания утверждает, что безопасность самих автомобилей не пострадала.

В последние годы эксперты неоднократно критиковали производителей автомобилей за недостаточное обеспечение безопасности автомобилей с функциями передачи данных через сеть. Специалисты опасаются, что, обойдя ограничения безопасности, злоумышленники смогут управлять бортовым компьютером автомобиля, который отвечает за нормальное функционирование всех компонентов машины. Они считают, что уже скоро хакеры смогут совершать гораздо более опасные преступления – например, подстраивать аварии или шантажировать водителей, угрожая им масштабным ДТП.

Исследователи ADAC смогли проэксплуатировать уязвимость, сымитировав поддельную мобильную сеть. Автомобили BMW пытались связаться с этой сетью, позволяя хакерам управлять функциями, активируемыми с помощью SIM-карты. BMW исправила брешь, добавив поддержку HTTPS в ПО ConnectedDrive ***(Уязвимость в ПО от BMW позволяла хакерам угонять автомобили // InternetUA (http://internetua.com/uyazvimost-v-po-ot-BMW-pozvolyala-hakeram-ugonyat-avtomobili). – 2015. – 2.02).***

***

Компания ESET, международный разработчик антивирусного ПО и решений в области компьютерной безопасности, предупредила о росте активности новой модификации банковского троянца Win32/Emotet. Среди пострадавших преобладают пользователи из Германии, есть жертвы из стран Восточной Европы и других регионов.

Как сообщает ITResearch, Win32/Emotet распространяется в спам-рассылке, имитирующей официальные уведомления от мобильных операторов, банков или платежной компании PayPal. В письмах содержится вредоносная ссылка или PDF-документ, при открытии которого загружается троянская программа. Такие письма сложно отфильтровать, поскольку они приходят с реально существующих адресов.

После загрузки Win32/Emotet устанавливает соединение с удаленным сервером, фиксирует сетевой трафик и перехватывает логины и пароли онлайн-банкинга жертвы. Троян способен подключаться к восьми сетевым API-интерфейсам, открывая злоумышленникам доступ к данным, которые передаются через защищенное HTTPS-соединение.

Троянцы семейства Win32/Emotet способны не только перехватывать данные интернет-банкинга, но и компрометировать аккаунты в почтовых сервисах и мессенджерах, в том числе Google Talk, Windows Live Messenger, различных версиях Outlook. Аутентификационные данные передаются на удаленный сервер, и взломанные аккаунты используются для дальнейшего распространения троянца.

Эксперты лаборатории ESET напомнили пользователям об основных мерах защиты, в первую очередь о недопустимости загрузки подозрительных вложений и перехода по ссылкам из спам-писем ***(Новый троян перехватывает пароли онлайн-банкинга // InternetUA (http://internetua.com/novii-troyan-perehvativaet-paroli-onlain-bankinga). – 2015. – 15.02).***

***

Исследователи зафиксировали атаку на подключенную к Интернету систему управления насосами топливного хранилища.

Как следует из сообщения в блоге исследователей безопасности из Trend Micro, неизвестные хакеры, возможно, связанные с движением Anonymous, атаковали как минимум одну заправочную станцию на территории США. Злоумышленникам удалось скомпрометировать подключенную к Интернету систему управления насосными механизмами, контролирующими работу топливного хранилища.

Осуществить нападение удалось благодаря наличию в цистернах специальных датчиков ATG, используемых для мониторинга уровня запасов бензина, отправления сигналов об опасности, поломке, аварии, а также тестирования герметичности контейнера для топлива и многого другого. Данная технология широко распространена в США и за ее пределами, однако в серьезных инцидентах безопасности она не фигурировала.

Запрограммировать ATG на те или иные задачи можно как при помощи последовательного порта, так и через модем, TCP/IP и т. п. При этом в целях обеспечения удаленного контроля многие администраторы таких систем оснащают их подключением к Интернету.

Вместе с тем обеспечению информационной безопасности в этих комплексах традиционно уделяется недостаточное количество внимания. По предварительным оценкам экспертов, в настоящее время в открытом доступе находятся не менее 5,8 тыс. ATG (90 % в США), не имеющих даже парольной защиты ***(Хакеры атакуют автозаправки // InternetUA (http://internetua.com/hakeri-atakuuat-avtozapravki). – 2015. – 14.02).***

***

Исследователи безопасности из Sucuri обнаружили ряд веб-сайтов с инъекцией вредоносного iframe.

Как следует из сообщения в блоге компании Sucuri, местным исследователям безопасности удалось обнаружить уязвимость нулевого дня в плагине Fancybox для популярной CMS WordPress. Общее количество загрузок Fancybox за все время составляет 550 тыс. раз.

Выявить брешь удалось после того, как ряд пользователей этого продукта обратились в компанию с жалобами о том, что они стали жертвами вредоносной кампании. В ходе анализа заявок выяснилось, что все пострадавшие веб-сайты содержат инъекцию вредоносного iframe «203koko».

Метод осуществления атаки, не соответствовал тем уязвимостям, информация о которых содержалась в открытом доступе. Потому исследователи провели собственный подробный осмотр имеющегося кода.

«После ряда тщательных проверок мы действительно обнаружили серьезную уязвимость в плагине, с помощью которой становиться возможным инфицировать веб-ресурс», – пояснили эксперты.

По их словам, большее количество информации о бреши будет предоставлено после того, как разработчики Fancybox выпустят исправление ***(Обнаружена уязвимость нулевого дня в плагине WordPress Fancybox // InternetUA (http://internetua.com/obnarujena-uyazvimost-nulevogo-dnya-v-plagine-WordPress-Fancybox). – 2015. – 6.02).***

***

Координатор хакерської групи «Українські кібервійська» Є. Докукін заявив, що завдяки зусиллям групи був закритий сайт харківської сепаратистської організації «Исход». Про це він 1 лютого написав на своїй сторінці у Facebook.

Ідеться про сайт лідера сепаратистської організації «Исход» О. Новікова novikov.org.ua.

«Нещодавно мій помічник написав скаргу, і сайт закрили. Цей сайт належить О. Новікову, засновнику харківської сепаратистської організації “Исход”, над блокування рахунків якої я працюю з грудня», – написав Є. Докукін.

Також 1 лютого «Українські кібервійська» заблокували ресурси без-вести.рф, mdsdnr.info, ungu.org, cik-lnr.info, pravdatoday.info, bne.su, lvs-global.ru, slemtt.myjino.ru, molotpravdu.com, новорус.рф, novorossia.co, nol.su, dnrepublic.info, ukrnovosti.info, donetsk-gov.su, k61.dn.ua, ntribunal.su та ntribunal.mcdir.ru, які вони називають такими, що належать терористам.

«Операція “Відплата” триває. Сьогодні лежали 70 сайтів терористів. DDoS атаки – це артилерія “Українських Кібер Військ”. Яка працює і в день, і в ночі», – написав координатор.

Як повідомяв сайт Media Sapiens, нещодавно хакери з групи «Українські кібервійська» заявили, що контролюють велику кількість мережевих пристроїв у Росії та Криму.

Нагадаємо, раніше «Українські кібервійська» передали Службі безпеки України дані 1025 проросійських бойовиків, виклали у відкритий доступ документи російського Міністерства внутрішніх справ, а також домоглися блокування веб-сайтів та банківських рахунків багатьох сепаратистів ***(«Українські кібервійська» домоглися закриття сайту харківських сепаратистів // Телекритика (http://www.telekritika.ua/kontekst/2015-02-02/103199). – 2015. – 2.02).***

***

Следователи Федерального бюро расследований обнаружили, что 90 % всех кибератак, платежного мошенничества и утечек данных можно было избежать. Для этого предпринимателям нужно было усилить меры для защиты конфиденциальной информации.

Агент ФБР, Д. Шульцел отметил, что около 90 % компаний подверглись хакерским атакам из-за слабых систем защиты либо полного игнорирования правил безопасности.

Д. Шульцел рекомендовал систему мероприятий, которые необходимо провести для предупреждения легкого взлома сетей предприятия. Агент отметил, что частные компании должны сотрудничать с государственными органами по всем вопросам, касающимся реализации защиты.

Среди предложенных методов защиты стоит отметить образовательные программы, направленные на повышение осведомленности о возможных способах кибератак. Также ФБР поощряет внедрение более сложных систем шифрования данных, сведение к минимуму объема информации, который хранится в компьютерах, а также своевременное уведомление властей о несанкционированном доступе к даннным компании ***(ФБР: 90 % кибератак можно было предотвратить // InternetUA (http://internetua.com/fbr--90--kiberatak-mojno-bilo-predotvratit). – 2015. – 7.02).***

***

2 февраля компания Adobe выпустила уведомление безопасности, в котором сообщается об очередной уязвимости нулевого дня в Adobe Flash Player. Это уже третья уязвимость нулевого дня в 2015 г. в популярном проигрывателе. Уязвимость получила идентификатор CVE-2015-0313, а эксплоит к уязвимости входит в состав Angler Exploit Kit.

О новой уязвимости в Adobe Flash сообщили специалисты компании Trend Micro. Согласно исследователям, злоумышленники разместили эксплоит на сайте dailymotion.com. Пользователи этого портала перенаправлялись на файл hxxp://www.retilio.com/skillt.swf, который и осуществлял компрометацию.

В настоящее время уязвимость присутствует в последней версии Adobe Flash 16.0.0.296. Производитель планирует выпустить экстренное исправление безопасности в течение этой недели. Пока исправление недоступно, SecurityLab рекомендует своим читателям временно отключить уязвимый плагин ***(Еще одна уязвимость нулевого дня в Adobe Flash Player // InternetUA (http://internetua.com/esxe-odna-uyazvimost-nulevogo-dnya-v-Adobe-Flash-Player). – 2015. – 3.02).***

***

Свыше 60 % популярных Android-приложений для знакомств могут быть легко взломаны хакерами. Об этом свидетельствует исследование подразделения компании IBM, отвечающее за кибербезопасность.

По данным исследования IBM, многие мобильные приложения для знакомств имеют доступ к расширенному набору функций и данных на мобильном устройстве, включая камеру, микрофон, встроенную память, GPS-геолокацию и платежную информацию. В сочетании с уязвимостями в самих программах, они становятся легкой мишенью для хакеров.

«Многие пользователи доверяют информацию на своих смартфонах разнообразным приложениям. Именно это доверие дает хаверам возможность эксплуатировать уязимости, подобные тем, что были обнаружены в приложениях для знакомств. Пользователям стоит быть осмотрительнее и не раскрывать слишком много личной информации в попытке построить отношения», – говорит представитель IBM К. Барлоу.

Исследование выявило, что 26 из 41 Android-приложения для знакомств имели серьезные уязвимости. Они теоретически позволяли хакерам получать доступ к личной информации пользователей, загружать вирусы на их смартфоны, узнавать местонахождение пользователя, устанавливать контроль над устройством либо взламывать аккаунт на используемом сервисе.

Помимо личной информации, под угрозой могут оказаться и корпоративные данные. В половине из изученных IBM организаций на мобильных устройствах сотрудников было выявлено как минимум одно приложение для знакомства, которое имело доступ к бизнес-информации.

По данным исследовательского центра Pew Research, каждый десятый американец или примерно 31 млн человек хотя бы раз использовали сайт или приложение для знакомств в Сети.

Эксперты IBM рекомендовали пользователям не раскрывать подробные данные о себе на подобных сервисах, проверять, к каким данным приложение запрашивает доступ при запуске, создавать отдельные пароли для разных онлайн-аккаунтов, вовремя устанавливать обновления и не подключаться к непроверенным сетям связи ***(Эксперты выявили уязвимость приложений для знакомств перед хакерами // InternetUA (http://internetua.com/eksperti-viyavili-uyazvimost-prilojenii-dlya-znakomstv-pered-hakerami). – 2015. – 13.02).***

***

Специалисты ИБ-компании Symantec провели исследование рынка наборов инструментов для осуществления фишинга и выяснили, что стоимость таких наборов варьируется от 2 до 10 дол. Стоит отметить, что такие наборы довольно просты в использовании и не требуют от мошенников обладания особыми техническими навыками и умениями. Как пишет специалист Symantec Р. Спончиони в своем блоге, злоумышленник может модифицировать фишинговые страницы набора по своему усмотрению.

По словам Р. Спончиони, некоторые наборы являются вполне базовыми и содержат всего две веб-страницы, однако другие более профессиональны и убедительны. Такие наборы включают более 25 исходных PHP-файлов и 14 различных языковых файлов, которые выбираются и загружаются в зависимости от местонахождения жертвы.

Профессиональные пакеты инструментов для фишинга могут быть использованы не только для похищения паролей и имен пользователя, но и персональных данных, таких как имена, фамилии, даты рождения, номера кредитных карт и т. д. С помощью таких наборов мошенники могут имитировать популярные веб-сайты, принадлежащие операторам облачных хранилищ, банковским организациям, поставщикам услуг электронной почты и многим другим компаниям.

Нередко мошенники предпринимают попытки компрометации легитимных систем управления контентом (legitimate content management systems,CMS) или блогов с целью установки набора на серверы, поясняет Р. Споничони. Атакующие часто используют автоматизированные скрипты для эксплуатации уязвимостей в целевых системах, пытаясь скомпрометировать как можно большее количество серверов ***(Наборы инструментов для фишинга помогают мошенникам осуществлять фишинг-атаки // InternetUA (http://internetua.com/nabori-instrumentov-dlya-fishinga-pomogauat-moshennikam-osusxestvlyat-fishing-ataki). – 2015. – 15.02).***

***

Нужен ли смартфону антивирус? Этот вопрос не раз поднимали многие пользователи Android, однако в действительности ни к какому выводу они не приходили. Одни считают, что антивирус является незаменимой вещью, которая защитит их от вредоносного контента, другие, напротив, не считают нужным защитить себя. Так кто же из них прав? Сегодня мы попытаемся разобраться, так ли нужны антивирусы или же это пиар-акция их создателей.

Вопрос не такой простой, на первый взгляд, однако всё очень просто. В первую очередь всё зависит от пользователя, и эта формула работает не только для Android, но и для других платформ: если вы не открываете подозрительные ссылки, если вы знаете, что есть реклама, а что есть правда – вам не страшны вирусы, соответственно, вы не нуждаетесь в антивирусе. К примеру, в моём компьютере и в телефоне нет антивирусов. Всё почему?

Потому что я знаю, что скрывается под ссылкой – и пусть это не выглядит хвастовством, – всё зависит от опыта: если вы опытный пользователь, вы с легкостью сможете отсортировать контент.

Однако, если взглянуть с другой стороны, давайте зададим себе вопрос: «Что такое антивирус?» Антивирус – это в первую очередь средство, которое продлит вашу работу с устройством, и неважно, компьютер это либо ваш Android-девайс. Каким бы вы ни были гиком, как бы вы ни были уверены в своих возможностях, вирус рано или поздно попадёт на ваше устройство, другими словами, установив антивирус, вы продлите вашу работу с девайсом.

Конечно, есть и нюансы, касаемые только Android. Google изначально встроила в Android свой защитный механизм, который включен в сервисы Google Play, эта система сканирования защитит вас от вредоносного контента, и работает она, отметим, ничуть не хуже сторонних антивирусов, поэтому устанавливать Norton смысла нет, но всегда есть «но». Согласно коллегам из androidcentral, на рынке очень много девайсов, не имеющих встроенных сервисов Google, которые используют сторонние магазины приложений, например, Nokia N1 или Nokia X, в таком случае, вам просто необходимо обезопасить себя, установив антивирус. Впрочем, установить антивирус не помешает и в случае, если у вас есть Root-доступ или же если вы часто устанавливаете контент от неизвестных источников.

Возникает вопрос: почему же тогда все не могут поставить антивирусы и на всякий случай защитить себя? Могут, но какие последствия? При выборе чего-либо вы должны чем-то жертвовать, и в данном случае это: место в постоянной памяти девайса, не менее 50 МБ занимаемого места в оперативной памяти, более медленная работа в играх и в целом в интерфейсе. Минусов действительно много, поэтому, если у вас всего 1 ГБ оперативной памяти, подумайте, так ли вам нужен антивирус? ***(Нужны ли Android антивирусы? // InternetUA (http://internetua.com/nujni-li-Android-antivirusi). – 2015. – 3.02).***

***

Специалист ИБ-компании PricewaterhouseCoopers М. Фагани предупредил об атаке, осуществляемой в настоящее время на пользователей социальной сети Facebook. По словам М. Фагани, злоумышленники распространяют вредоносное ПО под видом фальшивого плагина Flash Player.

Распространение вредоноса происходит довольно обычным способом: пользователь Facebook получает видеосообщение, предположительно содержащее контент для «взрослых». Для того чтобы просмотреть видеоролик, жертве предлагается загрузить обновление плагина Flash, которое на самом деле является вредоносным ПО.

После инфицирования ПК пользователя, вредонос рассылает свои копии контактам из списка друзей жертвы и инсталлирует кейлоггер для

сбора конфиденциальной информации, такой как адреса электронной почты и пароли банковских счетов. Затем троян устанавливает связь с удаленным сервером злоумышленников и ожидает дальнейших указаний.

Данный вредонос, известный как Chromium.exe и Google Chromium, является универсальным дроппером, который помимо кейлоггера может устанавливать и другие вредоносные программы. Он использует системный реестр Windows для запуска каждый раз, когда пользователь осуществляет вход в систему ***(Злоумышленники распространяют вредоносное ПО на Facebook // InternetUA (http://internetua.com/zloumishlenniki-rasprostranyauat-vredonosnoe-po-na-Facebook). – 2015. – 2.02).***

***

4 февраля появилась информация в публичном доступе о ранее неизвестной уязвимости в Microsoft Internet Explorer. Обнаруженная уязвимость позволяет злоумышленнику обойти политику единства происхождения и выполнить произвольный JavaScript сценарий в браузере жертвы в контексте безопасности произвольного сайта. Для этого жертва должна зайти на страницу, содержащую XSS-эксплоит.

PoC-код эксплоита доступен на сайте deusen.co.uk. Для демонстрации уязвимости исследователи выбрали сайт www.dailymail.co.uk. При нажатии на специально сформированную ссылку пользователь перенаправляется на сайт dailymail.co.uk, после чего ему выводится сообщение Hacked by Deusen ***(Обнаружена XSS уязвимость в Microsoft Internet Explorer // InternetUA (http://internetua.com/obnarujena-XSS-uyazvimost-v-Microsoft-Internet-Explorer). – 2015. – 4.02).***

***

Исследования «Доктор Веб» показали, что появился новый вирус, который отличается от других троянов для ОС Linux своей особой многофункциональностью. Бэкдор обладает возможностью выполнять различные команды, поступающие от злоумышленников, организовывать DDoS-атаки и реализует обширный ряд других функциональных задач.

По команде злоумышленников, бэкдор может назначить зараженной машине уникальный идентификатор, начать DDoS-атаки, такие как SYN Flood, UDP Flood, HTTP Flood и NTP Amplification на удаленный узел с заданным адресом, прекратить начатую ранее атаку, обновить исполняемый файл, записать информацию в файл или удалить себя.

Троян также способен выполнять отдельный блок задач с различными файловыми объектами. Получив соответствующую команду, бэкдор отсылает злоумышленникам информацию о файловой системе инфицированного компьютера (общее количество блоков, данных в файловой системе, количество свободных блоков).

После этого вирус в силе запустить, переименовать, принять, удалить файл, отправить файл на C&C-сервер, отправить ему сигнал о готовности

принять файл, создать файл, в котором можно будет сохранить принимаемые данные, перечислить файлы и каталоги внутри указанного каталога, отослать на сервер сведения о размере файла, создать и удалить каталог. Кроме этого, он способен запустить на зараженном компьютере SOCKS proxy или собственную реализацию сервера portmap ***(Новый бэкдор для ОС Linux позволяет осуществить DDoS-атаку // InternetUA (http://internetua.com/novii-bekdor-dlya-os-Linux-pozvolyaet-osusxestvit-DDoS-ataku). – 2015. – 7.02).***

***

Кількість смартфонів на ОС Android, уражених специфічним смс-вірусом, перевищила 85 тис. Про це повідомили в центрі інформаційної безпеки CERT-UA.

За даними центру, загальна кількість скомпроментованих смартфонів у світі становить близько 200 тис., і найбільша кількість жертв зловмисників – в Україні. У вересні 2014 р. власники багатьох смартфонів на Android отримали смс-повідомлення такого змісту “Привет :) Тебе фото!” з посиланням на веб-ресурс, при переході на який телефон зазнавав ураження вірусом. УВсі пристрої, які підхопили цей вірус, з часом ставали учасниками бот-мережі.

Спеціалісти CERT-UA розробили сервіс, що дає можливість визначити, чи є ураженим ваш телефон. Для цього потрібно ввести IMEI-код смартфону на сторінці сервісу ***(Кількість уражених SMS-вірусом Android-смартфонів в Україні перевищила 85 000 // Watcher (http://watcher.com.ua/2015/02/05/kilkist-urazhenyh-sms-virusom-android-smartfoniv-v-ukrayini-perevyschyla-85-000/). – 2015. – 5.02).***

***

Министерство обороны США выложило в сеть программный комплекс для защиты от хакерских атак Dshell.

Программный комплекс уже пять лет используется Министерством обороны для анализа и исследования атак из сети. Теперь он стал доступен рядовым пользователям Интернета, пишет Imena.UA (http://www.imena.ua/blog/army-open-sources-cyber-defense/).

Архитектура Dshell представляет собой каркас, на базе которого любой пользователь может создавать собственные аналитические модули, используя в качестве основы атаки, с которым ему пришлось столкнуться.

Разработки на базе Dshell позволят создать принципиально новые системы защиты от хакерских атак, антивирусные программы и тому подобные утилиты.

Предполагается, что в ближайшие шесть месяцев вокруг системы Dshell сформируется сообщество программистов, хакеров и разработчиков, в которое войдут и представители правительств, научных кругов.

Программным комплексом уже заинтересовались аналитики и разработчики из 18 стран.

Ранее в Интернете появился сервис Hacker's List – фриланс-биржа для хакеров. Ресурс позволяет подобрать компетентных исполнителей в сфере IT. Главная особенность ресурса – с его помощью заказывают не веб-сайты или программы, а услуги хакеров.

Создатели Hacker's List считают, что найм хакеров не должен быть сложным процессом, вызывающим беспокойство или проблемы ***(Армия США опубликовала свою систему защиты от хакеров // Imena.UA (http://www.imena.ua/blog/army-open-sources-cyber-defense/). – 2015. – 5.02).***

***

Роутеры D-Link уязвимы к перехватам DNS-запросов. Об этом сообщил член исследовательской группы Ethical Hacker Т. Донев. Он обнаружил брешь в прошивке ZyNOS в маршрутизаторе D-Link DSL-2740R ADSL.

«Сомнительная прошивка устройства используется производителями сетевого оборудования, компаниями D-Link, TP-Link Technologies и ZTE, и может вызвать проблемы у их клиентов», – рассказал Т. Донев изданию Computerworld.

Уязвимость позволяет злоумышленнику без аутентификации получить доступ в веб-администрации интерфейса устройства, изменять настройки DNS и перенаправлять пользователей на фишинговые сайты с вредоносным ПО. Т. Донев не уведомил D-Link об этой бреши, а выпустил код эксплойта для устранения ошибки ***(Роутеры D-Link уязвимы к перехватам DNS-запросов // InternetUA (http://internetua.com/routeri-D-Link-uyazvimi-k-perehvatam-DNS-zaprosov). – 2015. – 1.02).***

***

Новый вариант вируса Zeus нацелился на системы нескольких банков Канады. В их число могут войти Национальный банк Канады, Royal Банк и Банк Монреаля.

Новый вирус инфицирует веб-систему с целью похищения паролей и имен пользователей, номеров кредитных карт, социального страхования и водительских прав. Этот вид информации может быть использован для совершения банковского online-мошенничества, мошенничества в системе здравоохранения, для открытия кредитных счетов на имена жертв или для фишинг-атак на индивидуальные лица.

Генеральный директор SentinelOne Т. Вайнгартен заявил, что данный троян распространяется через социальную инженерию и эксплойты.

Троян не обнаруживается антивирусными программами и обходит SSL сертификаты. Только технология интеллектуального прогнозирования, которая контролирует активность на конечном устройстве, сможет выявлять и блокировать такой вид кибератаки.

«Жертва может даже не подозревать, что возникли какие-то проблемы», – добавил Т. Вайнгартен.

Модули платформы вредоносного ПО можно с легкостью использовать для атак на множество различных компаний. Это значит, что под угрозой находятся и банки США ***(Банки могут стать мишенью для нового варианта трояна Zeus // InternetUA (http://internetua.com/banki-mogut-stat-mishenua-dlya-novogo-varianta-troyana-Zeus). – 2015. – 1.02).***

***

У минулому році Чернівецька область була лідером із зараження комп'ютерів шкідливими програмними забезпеченнями. Про це йдеться у результатах дослідження вірусної активності в Україні за 2014 р. вітчизняної антивірусної лабораторії Zillya!

Так, кількість атакованих ПК, на яких встановлено український антивірус, у Чернівецькій області становила 35,47 % від числа всіх комп'ютерів. Друге місце посідає Закарпатська область – 32,74 %. Це означає, що кожен третій комп'ютер регіону піддавався атакам шкідливого ПЗ. Також до трійки лідерів увійшла і Тернопільська область з показником у 32,44 % зараження ПК.

Найбезпечнішим регіоном країни стала Миколаївська область. Рівень зараження комп'ютерів шкідливими програмами становить найнижчий по країні результат – 18,19 %. У Києві зараженими виявилися 23,33 % комп'ютерів.

Лідером зараження за сімействами стало програмне забезпечення Adware. Його специфіка у тому, що в процесі свого використання воно показує користувачеві рекламу. За підрахунками Zillya!, атаки цього шкідливого програмного забезпечення на комп'ютери українців становлять 36,1 %. «Це можна пояснити заглибленістю українців в глобальну мережу, адже ми стали значно більше купувати в Інтернеті, шукати цікаві продукти, більше користуємось соціальними мережами тощо. Рекламний бізнес у мережі – це мільярдні прибутки», – пояснює О. Сич.

Друге місце за активністю 2014 р. зайняли програми троянського типу – у 25,64 % випадків. Решта – 38,26 % – програми сімейства Downloader, Backdoor, Worm, Rootkit та ін.

Найпоширенішими вірусами минулого року стали програми типу Adware – зайняли шість пунктів у ТОП-10. «Певну активність показали і небезпечні шкідливі програми сімейства Backdoor, за допомогою яких зловмисники можуть узяти під контроль ПК користувача», – ідеться у звіті антивірусної лабораторії.

Водночас експерти антивірусної лабораторії Zillya! прогнозують, що популярність шкідливого ПЗ, спрямованого на маніпуляції з рекламою та пошуковою видачею, буде невпинно зростати. «Цей сегмент чорного, а часом і сірого ринку невпинно зростає і буде зростати надалі, поки Інтернет не

почне в черговий раз змінювати свою структуру», – прогнозує технічний директор Zillya! Антивірус.

Щоб протидіяти популяризації шкідливого ПЗ, спрямованого на маніпуляції з рекламою та пошуковою видачею, О. Сич рекомендує, по-перше, встановлювати сучасні антивірусні програми, а також користуватися ліцензійним програмним забезпеченням. «Дуже обережно ставтесь до завантаження програмного забезпечення з невідомих або підозрілих ресурсів. Навіть якщо встановлюєте безкоштовну програму – під прикриттям "чистої" програми можуть пропонуватися додаткові інсталяції. Уважно дивіться на активовані галочки навпроти запропонованих додаткових установок, перед тим як натиснути "ОК"», – говорить він.

По-друге, варто уважно стежити за надходженнями нових листів на електронну пошту. «Не відкривайте підозрілі листи від невідомих адресатів, особливо якщо вони мають у своїй темі заклики це зробити. Це ж правило працює для вкладень», – пояснює О. Сич.

Не менш пильну увагу слід приділити постам, повідомленням та позначкам на фото в соцмережах. Адже, за словами технічного директора Zillya! Антивірус, акаунти друзів можуть бути зламані і від них може надходити шкідливе ПЗ. Воно може зламати та викрасти дані вашого акаунту і встановити на ПК рекламні модулі.

«Також періодично варто перевіряти в налаштуваннях браузерів встановлені раніше додатки. Інколи шкідливе ПЗ встановлює рекламні модулі зовсім непомітно. Видалення непотрібних додатків, дозволить позбутися набридливої реклами», – додає О. Сич ***(Буковинці взяли «лідерство» по зараженню комп'ютерів вірусами // Газета "Молодий буковинець" (http://molbuk.ua/chernovtsy_news/85768-bukovynci-vzyaly-liderstvo-po-zarazhennyu-kompyuteriv-virusamy.html). – 2015. – 1.02).***

***

Не так давно разработчики мессенджера WhatsApp представили новый сервис под названием WhatsApp Web, при помощи которого пользователи могут синхронизировать историю сообщений в мобильной и настольной версиях программы. Несмотря на то что после появления новых опций прошло менее двух недель, исследователи безопасности уже обнаружили брешь, влияющую на конфиденциальность пользовательских данных.

Как сообщает издание Naked Security со ссылкой на IT-эксперта И. Бхуяна, в некоторых случаях пользователи WhatsApp Web способны получить доступ к фотографиям других пользователей, несмотря на препятствующие этому настройки приватности. При этом в мобильной версии мессенджера подобные ошибки не проявляются.

Речь идет о случаях, когда пользователь сервиса отправляет одному из своих контактов изображение, а затем удаляет ее. В мобильной версии, получатель больше не сможет посмотреть фотографию, однако все еще будет

видеть ее «размытую» миниатюру. Тем не менее, при просмотре снимка через WhatsApp Web, эффект размытия не накладывается.

Более того, по данным И. Бхуяна, настольная версия сервиса позволяет сторонним пользователям просматривать фотографию и данные профиля даже если они были скрыты ***(Брешь в web-версии WhatsApp ставит под угрозу конфиденциальность пользователей // InternetUA (http://internetua.com/bresh-v-web-versii-WhatsApp-stavit-pod-ugrozu-konfidencialnost-polzovatelei). – 2015. – 3.02).***

***

По мнению разработчиков из стартапа Power Fingerprinting Cybersecurity (PFP), есть потенциальная возможность определять наличие уязвимостей и заражённых устройств по изменению в их потреблении энергии.

Идея вполне здравая, ведь вредоносный код создаёт дополнительную нагрузку на процессор. Соответственно, энергопотребление тоже увеличивается. Это особенно актуально в связи с распространением «интернета вещей», где мониторинг энергопотребления может быть особенно актуальным, ведь на персональных компьютерах этот показатель не даёт такой ясной картины.

Руководители Power Fingerprinting Cybersecurity утверждают, что во время теста им удалось успешно определить наличие Stuxnet на оборудовании в отсутствии антивируса.

Стартап создан при финансировании научно-исследовательского подразделения американской армии DARPA, а также при участии Министерства внутренней безопасности США. По идее авторов, эту технологию планируется внедрить в АСУ и системах SCADA, а именно, в программируемых логических контроллерах и других устройствах ***(Вычисление уязвимостей по потреблению энергии // InternetUA (http://internetua.com/vicsislenie-uyazvimostei-po-potrebleniua-energii). – 2015. – 7.02).***

***

Украинские патриотически настроенные веб-специалисты, объединенные в инициативу «Украинские кибервойска» (УКВ), захватили уже 6810 частную веб-камеру, почти половина из которых находятся во временно оккупированном Крыму и на территории России, пишет «Обозреватель» (http://tech.obozrevatel.com/news/01438-myi-sledim-za-vami-ukrainskie-kibervojska-zahvatili-okolo-7-tyisyach-vebkamer-protivnika.htm).

Об этом сообщил на своей странице в Facebook «главнокомандующий» УКВ Е. Докукин.

«На сегодня это следующее количество веб-камер. Всего: 681 хост с камерами. Из них в Украине – 414, в Крыму – 19 и в России – 248 хостов. На каждом из них в панели управления могут быть несколько веб-камер (обычно

количество камер от 1 до 16, но мне попадались и 32 камеры). В среднем по 10 камер. Таким образом? общее количество отдельных частных камер 6810», – говорится в сообщении.

Как утверждает Е. Докукин, враг, как на временно оккупированных территориях в Крыму и Донбассе, так и на территории Российской Федерации, должен понимать, что за его действиями всегда следят ***(Мы следим за вами: украинские «кибервойска» захватили около 7 тысяч веб-камер противника // Обозреватель (http://tech.obozrevatel.com/news/01438-myi-sledim-za-vami-ukrainskie-kibervojska-zahvatili-okolo-7-tyisyach-vebkamer-protivnika.htm). – 2015. – 9.02).***

***

Исправление уязвимостей стало более зависимым от внимания прессы и раздуваемой СМИ паники. Об этом сообщает компания Secunia в интервью изданию The Register.

Уязвимость в OpenSSL, более известная как Heartbleed, вынудила разработчиков ПО в течение 40 дней выпустить исправления безопасности для более чем 600 продуктов. Еще одна брешь, обнаруженная в июне 2014 г., привела к исправлению более 800 единиц ПО. Тем не менее, следующая уязвимость, найденная в августе, была исправлена лишь в 75 продуктах.

Как сообщил руководитель отдела исследований и безопасности Secunia К. Линдгаард в интервью The Register, августовская уязвимость и брешь Heartbleed были во многом похожи. Тем не менее, в течение месяца после обнаружения бреши в августе быи выпущены исправления лишь для 75 из более чем 200 продуктов, подверженных этой уязвимости. К. Линдгаард считает, что «неторопливость» разработчиков была вызвана тем, что СМИ не приделили последней бреши столько же внимания, чем в случае с Heartbleed.

Обнаруженная в апреле 2014 г. уязвимость Heartbleed была довольно легка в эксплуатации, но с ее помощью злоумышленники могли лишь раскрыть некоторые данные. Более поздние бреши были гораздо более опасными, позволяя хакерам полностью скомпрометировать целевую систему.

К. Линдгаард сказал, что Heartbleed стала самой обсуждаемой в СМИ, и, как следствие, самой популярной уязвимостью в ПО. Тем не менее, отделам безопасности производителей ПО следует работать над исправлением всех брешей, а не только над теми, которые привлекли внимание журналистов.

Также отмечается, что в мире кибербезопасности появился своеобразный тренд – специалисты все чаще присваивают разным уязвимостям логотипы. Вскоре после Heartbleed была обнаружена уязвимость ShellShock, которую также снабдили собственным логотипом. Аналогично поступили в случае с брешами POODLE и Ghost ***(СМИ напрямую влияют на скорость исправления уязвимостей // InternetUA***

(http://internetua.com/smi-napryamuua-vliyauat-na-skorost-ispravleniya-uyazvimostei). – 2015. – 9.02).

***

Торгпредство США включило Россию в список стран, в которых нарушаются права на интеллектуальную собственность. РФ оказалась на первых местах в так называемом «списке 301» вместе с Китаем, Индией, Индонезией, Таиландом, Вьетнамом и Чили.

Торгпредство включило в свой список социальную сеть «ВКонтакте», назвав ее крупнейшим распространителем пиратской музыки, фильмов и сериалов. «ВКонтакте» удаляет пиратский контент по требованию правообладателей, отметили в ведомстве. Но этого недостаточно для борьбы с пиратством, считают они. Также в социальной сети «Одноклассники» тоже есть сервис нелицензионной музыки, пишет издание «Ведомости».

Несмотря на то что, вступив во Всемирную торговую организацию, Россия обязалась защищать права авторов и правообладателей, онлайн-пиратство остается серьезной проблемой в этой стране, сказано в документе, который составили совместно Торгпредство США и Международный альянс интеллектуальной собственности, IIPA.

Авторы документа рекомендуют российскому правительству отказаться от идеи авторского налога и сфокусироваться на правовой защите интеллектуальной собственности. В частности, они советуют принять эффективные меры против интернет-пиратов – нелицензионных стриминговых музыкальных сервисов, сайтов с пиратскими играми, сайтов с киберлокерами, торрент-трекером и т. п.

Также в «список 301» американские власти включили ряд крупных торрент-трекеров, таких как rutracker.org, rutor.org, torrent-games.net, rapidator.net и др. ***(США признали «ВКонтакте» и «Одноклассники» пиратскими сайтами // InternetUA (http://internetua.com/ssha-priznali--vkontakte--i--odnoklassniki--piratskimi-saitami). – 2015. – 10.02).***

***

Специалисты компании Hewlett-Packard провели исследование, в котором протестировали ряд домашних систем безопасности и выяснили, что каждая из них содержала ряд брешей, в том числе уязвимость пароля, слабое шифрование и проблемы с аутентификацией.

Команда службы безопасности HP Fortify on Demand провела анализ 10 популярных устройств безопасности дома (такие как видеокамеры и детекторы движения), а также их облачные компоненты и мобильные приложения. Как оказалось, уязвимости присутствовали во всех системах: ни в одной из них не была реализована двухфакторная аутентификация, а вход производился при помощи довольно слабого пароля.

Все системы, проверенные специалистами, в том числе облачные веб- и мобильные интерфейсы, не требовали установки пароля достаточной длины

и сложности. При этом для входа в большинство из них требовалось ввести обыкновенный буквенно-цифровой шестизначный пароль. Более того, оказалось, что во всех системах не реализовано ограничение количества попыток входа, что делает их уязвимыми к брутфорс-атакам.

Также, отмечают специалисты, в 7 из 10 проанализированных систем присутствовал ряд проблем в программном обеспечении, отвечающем за обновления. В число проблем входили использование незашифрованных протоколов для идентификации загрузочного сервера, отсутствие шифрования при передаче файлов обновления, а также неспособность определения новых модификаций пакета обновления ***(Все домашние системы безопасности содержат уязвимости // InternetUA (http://internetua.com/vse-domashnie-sistemi-bezopasnosti-soderjat-uyazvimosti). – 2015. – 13.02).***

***

10 февраля этого года исследователи из Rapid7 обнаружили серьезную уязвимость в Google Play, которая позволяет злоумышленникам устанавливать приложения на смартфон под управлением Android без ведома владельца. Как вы сами можете понимать, приложения бывают разные, от полностью бесполезных до вредоносных. Впрочем, раз уязвимость распространяется только на Google Play, никаких действительно вредоносных приложений установить не удастся, однако стоит все же обезопасить себя, и ниже мы расскажем – как.

Для того чтобы установить приложение на ваш смартфон без вашего ведома и согласия, злоумышленнику потребуется использовать сразу две бреши в безопасности. Одна из них находится в браузере смартфона, а другая – в веб-приложении Google Play. При этом некоторые сторонние браузеры и старые версии браузеров, особенно на Android 4.3 и старше, являются менее безопасными, чем обновленные версии. Браузеры старых версий Android с открытым исходным кодом имеют уязвимость UXSS, и вместе с уязвимостью в веб-интерфейсе Google Play злоумышленник может выполнить функцию удаленной установки приложения, даже не показывая вам интерфейс магазина.

Для защиты от подобных злодеяний вам перво-наперво рекомендуется обновиться до самой последней версии Android. Далее рекомендуется использовать браузеры, невосприимчивые к UXSS-уязвимостям, такие как Google Chrome, Dolphin Browser и Mozilla Firefox. Следите за тем, чтобы браузеры своевременно получали обновления и, разумеется, постарайтесь заметить неожиданно появившееся на вашем смартфоне новое приложение. Если вы хотите полностью обезопасить себя, осуществите выход из учетной записи Google в своем браузере при посещении веб-страниц. Это может быть не совсем удобно, но для старых браузеров это единственный метод полностью исключить риск нежелательной установки приложений ***(Уязвимость Google Play позволяет устанавливать приложения на***

смартфон без ведома владельца // InternetUA (http://internetua.com/uyazvimost-Google-Play-pozvolyaet-ustanavlivat-prilojeniya-na-smartfon-bez-vedoma-vladelca). – 2015. – 13.02).

***

Международная хакерская организация Anonymous сообщила о взломе более 800 аккаунтов в социальных сетях и электронной почте сторонников «Исламского государства» (ИГ).

Свое заявление группировка разместила на сервисе Pastebin, который используется ею для публикации своих новостей. Anonymous объявили войну «Исламскому государству» в феврале 2015 г., после теракта на издание Charlie Hebdo.

Хакерами были взломаны 800 аккаунтов Twitter, 12 страниц Facebook и более 50 адресов электронной почты. По данным группы, владельцы этих страниц имели отношение к террористической группировке. Большинство указанных аккаунтов недоступны или временно отключены. Руководство Facebook удалило 11 из 12 страниц, перечисленных хакерами в листе причастных к ИГ, так как записи на них противоречили правилам сети.

«Мы будем охотиться на вас, выводить из строя ваши сайты, аккаунты, электронную почту. С этого момента в сети нет для вас безопасного места. К вам будут относиться, как к вирусу, а мы – лекарство», – заявили они в своем видеообращении.

В своем видеообращении к «Аль-Каиде», «Исламскому государству» и другим группировкам Anonymous пообещали выследить и закрыть все учетные записи в социальных сетях, связанные с террористами ***(Anonymous взломали более 800 аккаунтов участников ИГ // iLenta.com (http://ilenta.com/news/internet/news_5797.html). – 2015. – 12.02).***

***

Корпорация Microsoft выпустила ежемесячную порцию патчей для своих программных продуктов.

На этот раз опубликовано девять бюллетеней безопасности, содержащих описание 56 различных уязвимостей. Причём 41 из устранённых «дыр» присутствуют в браузере Internet Explorer, который признан самым ненадёжным с точки зрения безопасности компонентом Windows.

Кумулятивный патч для IE затрагивает версии веб-обозревателя с 6-й по 11-ю на всех поддерживаемых платформах Windows. Обнаруженные уязвимости позволяют злоумышленникам получить несанкционированный доступ к удалённому компьютеру и выполнить на нём произвольный программный код. Кроме того, некоторые «дыры» дают возможность обойти средства защиты. В целом, кумулятивное обновление для IE получило статус критического.

Ещё два критически важных апдейта закрывают бреши в различных версиях операционных систем Windows. «Дыры» могут использоваться для выполнения произвольных операций на атакуемом ПК или сервере.

Оставшиеся шесть бюллетеней безопасности охарактеризованы важными. Уязвимости выявлены в различных компонентах Windows и офисных приложениях ***(Microsoft устранила четыре десятка уязвимостей в Internet Explorer // InternetUA (http://internetua.com/Microsoft-ustranila-csetire-desyatka-uyazvimostei-v-Internet-Explorer). – 2015. – 11.02).***