СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(4–17.11)

2013 № 21

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(4–17.11)
№ 21

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 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ 4

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА 12

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ 14

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ 26

Інформаційно-психологічний вплив мережевого спілкування на особистість 26

Маніпулятивні технології 30

Зарубіжні спецслужби і технології «соціального контролю» 35

Проблема захисту даних. DOS та вірусні атаки 47

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Социальная сеть Facebook обновила дизайн кнопок Like («Нравится») и Share («Поделиться»), используемых на сторонних сайтах. Сообщение об этом 7 ноября появилось в официальном блоге разработчиков соцсети.

Основной фон лайка стал темно-синим (вместо светло-синего, использовавшегося ранее), а место руки с поднятым вверх большим пальцем занял логотип Facebook. Большой палец теперь отображается только в квадратном «окне» над кнопкой, в котором может увидеть общее количество лайков, собранное той или иной записью. Похожие изменения коснутся и кнопки Share, с помощью которой можно поделиться ссылкой на контент в личном сообщении или в группе.

Как говорится в посте, внедрение новых кнопок будет происходить постепенно в течение нескольких недель. При этом кнопки на сайтах, использующих старые версии Like и Share, будут обновлены автоматически.

Кнопка Like впервые была представлена Facebook в 2009 г. Возможность встраивать кнопку на сторонние сайты появилась в 2010 г. С тех пор дизайн лайка не менялся ни разу. По данным социальной сети, Like и Share размещены в общей сложности на более чем 7 млн сайтах. Каждый день подобные кнопки пользователи сети видят в общей сложности около 22 млрд раз ***(Facebook убрал большой палец с кнопки лайк // Marketing Media Review (http://mmr.ua/news/id/facebook-ubral-bolshoj-palec-s-knopki-lajk-36945/). – 2013. – 7.11).***

***

Дж. Бібер інвестував у нову соціальну мережу для тінейджерів Shots of Me 1,1 млн дол.

Суть сервісу тримають у таємниці, але, якщо судити з егоцентричної назви, нас чекає чергове гетто для підліткових селфі (соціальних мереж без дорослих), пише Fortune.

Відомо, що музикант Дж. Бібер очолив фінансовий раунд у Shots of Me, вклавши в стартап 1,1 млн дол. Раніше творці Shots of Me – компанія RockLive – випускали мобільні ігри під брендами зірок на зразок М. Тайсона чи К. Роналду.

Дж. Бібера називають лід-інвестором у проект, що вже стало приводом для жартів з боку технологічних блогів. Залишається невідомим, чи дійсно співак узяв на себе функції з організації та структурування угоди.

Додаток Shots of Me повинен дебютувати на IOS найближчим часом. Можна не сумніватися, що десятки мільйонів фоловерів Дж. Бібера у Twitter і Facebook швидко виведуть сервіс на перші місця чартів App Store ***(В Інтернеті з'явиться нова соціальна мережа для підлітків // iPress.ua (http://ipress.ua/news/v_interneti_zyavytsya_nova_sotsialna_merezha_dlya_pidlitkiv_32399.html). – 2013. – 5.11).***

***

Социальная сеть «Одноклассники» обновила приложение для устройств на платформе Android, значительно изменив интерфейс, сообщила компания Mail.Ru Group.

В обновленном приложении, по сообщению компании, появилось боковое меню, в котором сосредоточены все разделы приложения. Там же находится новый музыкальный мини-плеер, который позволяет управлять музыкой параллельно с другими развлечениями. Другое дополнение приложения – раздел с собственной новостной лентой, на которой доступны все записи, опубликованные пользователем.

Галерея фотографий в обновленном приложении изменила дизайн, фото в открытых альбомах теперь расположены в виде плитки ***(Соцсеть «Одноклассники» изменила интерфейс в приложении для Android // InternetUA (http://internetua.com/socset--odnoklassniki--izmenila-interfeis-v-prilojenii-dlya-Android). – 2013. – 5.11).***

***

У соціальній мережі «Однокласники» з'явилася кнопка для негативної оцінки невдалих, на думку користувачів, фотографій. Про це повідомив прес-секретар соцмережі І. Грабовський.

Нова кнопка – це синій квадрат з намальованим на ньому великим пальцем, що вказує вниз. Передбачається, що з її допомогою користувачі соцмережі зможуть висловити своє критичне ставлення до контенту, який їм не подобається.

Крім того, на зміну традиційній п'ятибальній шкалі оцінок прийшли ще чотири кнопки – червона кнопка з серцем (як пояснив І. Грабовський це означає: «мені дуже подобаються твої фотки»), помаранчева кнопка з кошеням (фотографія є «еталоном мімімішності»), фіолетова кнопка з піднятою вгору рукою, що показує козу («для найкрутіших фотографій») та зелена – із чоловічком, який зіває («для відверто нудних фото»).

Соціальна мережа «Однокласники» була запущена у 2006 р. На сьогодні сайт є одним з найбільш відвідуваних ресурсів у Рунеті. За даними comScore, щоденна аудиторія соцмережі в липні 2013 р. становила понад 30 млн осіб ***(В «Однокласниках» з'явилася кнопка «не подобається» // ВГОЛОС (http://vgolos.com.ua/news/v_odnoklasnykah_zyavylasya_knopka_ne_podobaietsya_foto_123355.html). – 2013. – 11.11).***

***

Відеохостинг YouTube розкритикували за нову систему коментарів на сервісі, яка дає змогу коментувати відео лише тим користувачам, які мають акаунти в соцмережі Google+. Про це повідомляє Digit.ru

Ще наприкінці вересня YouTube почав запроваджувати зміни в систему коментарів, послідовно розміщуючи їх за релевантністю, а також вимагаючи пов'язати свій YouTube-аккаунт з обліковим записом у Google+ для можливості

коментування відео. Крім того, автори відео отримали нові інструменти для модерації коментарів до їхньої публікації.

Майже 87 тис. користувачів підписали петицію на сайті Change.org з вимогою до Google повернути колишню систему коментарів, зазначає CNN. «Google змушує нас створювати акаунти в Google+ і втручається у наше приватне життя, намагаючись відібрати право на анонімні коментарі», – ідеться в петиції.

Один із співзасновників YouTube Д. Карім, якому належить найперший відеоролик, розміщений на YouTube, через вісім років опублікував друге повідомлення у своєму акаунті, і воно також стосується нової системи коментарів. «Навіщо мені потрібен акаунт у Google+, щоб коментувати відео?» – дивується він.

Урешті, одна з популярних відеоблогерів Е. Блекері написала, виконала та виклала на YouTube пісню з різкою критикою інтеграції YouTube і Google+. Суть не дуже цензурного тексту пісні полягає у тому, що, на думку користувачів YouTube, вимога акаунта в Google+ для використання YouTube є поганим рішенням компанії. За три дні після публікації відеоролик Е. Блекері набрав понад 675 тис. переглядів на YouTube ***(Користувачі протестують проти нової системи коментарів на YouTube // ZIK (http://zik.ua/ua/news/2013/11/12/korystuvachi_protestuyut_proty_novoi_systemy_komentariv_na_youtube_439350). – 2013. – 12.11).***

***

Сервис микроблогов Twitter позволит пользователям составлять подборки твитов, посвященных определенной теме. Сообщение об этом 12 ноября появилось в официальном блоге соцсети. Новая функция в ближайшее время станет доступа через бесплатный клиент Tweetdeck.

Пользователи Tweetdeck смогут добавлять в подборку любые твиты, которые будут автоматически располагаться в хронологическом порядке. Каждая такая подборка будет иметь свое уникальное название, адрес и будет публичной (подписаться на ее обновления смогут все зарегистрированные в Twitter пользователи). При этом над одной подборкой смогут работать сразу несколько человек, а делиться ей можно будет не только через соцсеть, но и путем встраивания ее на внешние сайты.

В Twitter уже существует похожая функция, позволяющая формировать подборки твитов в зависимости от их авторства – пользователи соцсети могут объединять в единую ленту твиты из других выбранных ими аккаунтов. Однако в таких списках отображаются все твиты и возможности найти сообщение, посвященное какой-то определенной теме, нет ***(Twitter позволит пользователям составлять из твитов сборники // Минфин.com.ua (http://minfin.com.ua/2013/11/13/834759/). – 2013. – 13.11).***

***

Социальная сеть Facebook присоединилась к ассоциации GSMA, которая на сегодняшний день объединяет более 750 операторов мобильной связи в 218 странах мира. Об этом сообщает IT Expert со ссылкой на «РБК-Украина».

Вот уже долгое время руководство Facebook сосредотачивает усилия на мобильном рынке, который дает существенный прирост пользовательской базы и рекламных средств. Поэтому неудивительно, что в Facebook хотят укрепить сотрудничество и сформировать более тесные взаимоотношения с операторами сотовой связи.

Участники ассоциации GSMA предоставляют свои услуги в стандартах GSMA и 3G более чем 3 млрд клиентов, что составляет более 86 % всех мировых пользователей мобильного Интернета.

Своими главными целями GSMA видит: обеспечение возможности использования услуг мобильной связи в любой точке земного шара; предоставление людям легкого доступа к данному виду услуг; повышение ценности этих услуг для индивидуальных клиентов и для экономики в целом, а также предоставление новых коммерческих возможностей операторам связи и их поставщикам.

Facebook стала первой соцсетью, которая примкнула к GSMA. В компании сообщают, что будут стараться максимально активно участвовать в делах ассоциации.

«Присоединение к GSMA отражает нашу сосредоточенность на мобильном сегменте, а также свидетельствует о нашем остром желании работать в тесном сотрудничестве с представителями данной отрасли. Мы надеемся, что наше участие в ассоциации будет активным», – комментирует решение руководства Facebook вице-президент компании по развитию бизнеса Д. Роуз.

В свою очередь присоединение к GSMA позволит социальной сети существенно продвинуться в развитии проекта Internet.org, участники которого, обмениваясь разнообразными ресурсами, передовым опытом и разнообразными инструментами, ищут решения для основополагающих областей развития мобильного Интернета.

«Вовлечение в дела и проблемы, с которыми сталкиваются операторы и индустрия в целом, не является единственно важной целью для Facebook, рассчитывающей также и на развитие инициативы Internet.org», – сообщил представитель Facebook Д. Майнс ***(Facebook вступила в ассоциацию сотовых операторов GSMA // IT Expert (http://itexpert.in.ua/rubrikator/item/31739-facebook-vstupila-v-assotsiatsiyu-sotovykh-operatorov-gsma.html). – 2013. – 13.11).***

***

Жизнь после Facebook: куда мигрируют подростки из главной мировой соцсети.

В ноябре финансовый директор Facebook Д. Эберсман впервые признал долгосрочный тренд, о котором эксперты говорили все последние месяцы: крупнейшая мировая социальная сеть фиксирует снижение активности аудитории подросткового возраста, самой перспективной демографической группы.

«Мы наблюдаем сокращение в динамике ежедневного посещения сайта, особенно среди тинейджеров», – так Д. Эберсман описал статистику II–III кв. 2013 г. Во вторник ее подкрепили результаты исследования аналитической группы GlobalWebIndex, исследующей интернет-пользователей на 32 рынках.

Эксперты провели опрос среди подростков в 30 странах. Выяснилось, что число респондентов в возрастной категории 16–19 лет, активно пользующихся Facebook (т. е. не только молчаливо «лайкающих» чужие посты, но и производящих контент), в III квартале снизилось до 56 % с 76 в I квартале. Самый низкий показатель зафиксирован в Голландии – 52 %. В США за полгода 16 % подростков перестали быть активными пользователями Facebook.

Что приходит на смену соцсети № 1? Это давно уже не секрет: главными бенефициарами подростковой миграции с Facebook становятся мобильные мессенджеры, включая лидера – WeChat, и фотоприложения, такие как Instagram и Snapchat. Удивление вызывает лишь скорость, с которой растет аудитория этих социальных платформ.

Итоги исследования GlobalWebIndex были опубликованы во вторник. Статистика свидетельствует, что китайский мессенджер WeChat местного интернет-гиганта Tencent в отчетный период продемонстрировал невероятные темпы наращивания аудитории 16–19 лет по всему миру – свыше 1000 %.

Другими лидерами по этому показателю оказались видеоприложение Vine, принадлежащее Twitter, и мобильное приложение фотохостинга Flickr, которым владеет Yahoo! Показатели роста активности пользователей-подростков у сервисов с начала года составляют 639 и 254 % соответственно.

Быстро растет и сверхпопулярное у молодой аудитории приложение «самоуничтожающихся» фотосообщений Snapchat, которое в конце октября инвесторы оценили в 4 млрд дол. В списке GlobalWebIndex сервис не представлен, так как эксперты всего несколько месяцев как замеряют его рейтинг, но результат уже впечатляет: не менее 10 % подростков по всему миру активно пользуются «эфемерным» фотоприложением – в абсолютных цифрах это больше, чем у Pinterest, Vine, WeChat, Line и LinkedIn в том же демографическом срезе.

Мобильная миграция

«Тенденция абсолютно очевидна: от снижения популярности Facebook выигрывают, в первую очередь, мессенджеры, а также фото- и видеоприложения, – говорит гендиректор GlobalWebIndex Т. Смит. – И это особенно болезненная история для соцсети М. Цукерберга, которая всегда декларировала возможность обмена сообщениями, фото- и видеоконтентом как свои фундаментальные ценности, позиционировала ее как сильную сторону горизонтальных социальных связей между пользователями».

Подростки больше интересуются не «всей» Facebook, а ее собственным мессенджером Facebook Messenger (прирост подростковой аудитории с начала года – около 90 %). У стандартной версии соцсети за тот же период стало на 17 % меньше активных пользователей в возрастной категории 16–19 лет. Instagram прибавил 85 %, мессенджер WhatsApp – 81 %. Менее интенсивно (30 %) росла аудитория блог-платформы Tumblr, в мае купленной Yahoo! за 1,1 млрд дол.

«Вся аудитория неуклонно перемещается в мобильные устройства, – продолжает Т. Смит. – Приложение Facebook для смартфонов и планшетов тоже набирает популярность у подростков, у него на 69 % больше активных пользователей с начала года. Так что меняется сам принцип коммуникации людей с Интернетом».

По словам эксперта, для Twitter уход молодой аудитории на новые социальные платформы представляет меньшую угрозу. Сервис микроблогов остается незаменимой площадкой для трансляции новостей в режиме реального времени, имеет хорошие перспективы наращивания коммуникации с ТВ и активно рекрутирует в ряды своих пользователей звезд, а вслед за ними – и многомиллионные армии их поклонников. Даже Google лучше готов к отстаиванию своих конкурентных преимуществ, поскольку ассоциируется у пользователей с многими видами услуг и контента, заключает глава GlobalWebIndex.

Китайская экспансия

Несмотря на стремительные темпы роста WeChat, американские и европейские подростки пока не слишком активно пользуются этим мессенджером (хотя экспансия на Запад происходит посредством распространения в зарубежных китайских коммьюнити). Зато приложение невероятно популярно на родине и в странах Юго-Восточной Азии. Ежемесячная аудитория сервиса в 250 млн пользователей пока не догнала «настольный» мессенджер материнской компании Tencent, который в Поднебесной аккумулировал уже 800 млн пользователей. WeChat – англоязычная реинкарнация китайского оригинала WeiShin.

«Мы запустили продукт под другим брендом, расположенный на других внутренних серверах», – говорил президент Tencent М. Ло на октябрьской конференции GMIC в Сан-Франциско. Национальные версии «экспортной» WeChat тоже отличаются в зависимости от спецификаций аудитории в каждой стране, отмечал топ-менеджер. М. Ло, в 2004 г. курировавший IPO Tencent в статусе топ-менеджера Goldman Sachs, также назвал первые иностранные рынки, выбранные для активной экспансии сервиса, – Италия, Мексика и Бразилия.

США глава интернет-корпорации назвал «рискованным рынком». «Хотя у нас есть здесь офис и команда, которая думает, как бы мы могли правильно позиционировать себя в Америке», – отметил М. Ло.

Как WeChat планирует монетизировать свою популярность в подростковой среде? Сервис применяет механизмы, которые в перспективе

превратят приложение в платежный механизм. Партнер Tencent – сеть Ubox – недавно установил в пекинской подземке 300 автоматов по продаже газировки под брендом WeiShin. Оплатить товар можно через мессенджер, причем с большой скидкой к обычной цене напитка. Таким образом, происходит синергия офлайн-торговли и онлайн-платежей.

«Пока все это эксперименты, – признавал М. Ло. – Но по мере того, как мобильный Интернет проникает в повседневную жизнь людей, такие рыночные модели будут давать нам все больше возможностей».

Глава Tencent не согласен с тем, что сервисы, подобные WeChat, со временем могут «съесть» социальные сети так же, как в свое время Facebook отодвинула на обочину сервисы мгновенного обмена сообщениями. По мнению М. Ло, мобильные мессенджеры, как правило, привязаны к номерам телефонов, а потому изначально предполагают коммуникацию внутри узких групп, обычно между знакомыми в реальной жизни людьми.

«И Facebook, и WeChat – социальные сервисы, но они адресованы разным моделям поведения пользователей, – подытожил М. Ло. – Так что эти платформы могут сосуществовать» ***(Жизнь после Facebook: куда мигрируют подростки из главной мировой соцсети // InternetUA (http://internetua.com/jizn-posle-Facebook--kuda-migriruuat-podrostki-iz-glavnoi-mirovoi-socseti). – 2013. – 14.11).***

***

Похоже, в Twitter оценили положительно идею программы бета- и альфа-тестирования Android-приложений Facebook, потому что сеть микроблогов тоже запустила собственную программу тестирования предварительных версий мобильных приложений для людей, желающих проверить последние новшества до официального запуска.

TechCrunch сообщает, что инициатива Twitter называется Android Alpha Program. В отличие от аналогичной программы у Facebook, в которой могут участвовать все желающие, у Twitter она рассчитана только на предварительно приглашённых посредством email-рассылки пользователей. Программа позволяет получить доступ к предварительным и экспериментальным функциям и к особому форуму Google Group, на котором можно делиться отзывами и сообщениями об ошибках.

Twitter, как сообщается, запустила указанную программу по причине заинтересованности в создании более привлекательного для конечных пользователей мобильного приложения для платформы Android. В конце концов, Twitter теперь открытая компания и ей приходится больше внимания уделять прибыльности и показателям роста числа пользователей. Хорошо работающее Android-приложение – лишь один из многих факторов, на которые компании придётся обращать внимания для удовлетворения инвесторов и поддержания курса акций на бирже ***(Twitter запустила программу альфа-тестирования для Android // InternetUA (http://internetua.com/Twitter-zapustila-programmu-alfa-testirovaniya-dlya-Android). – 2013. – 13.11).***

***

В новой версии Facebook Messenger пользователи получили возможность обмениваться мгновенными сообщениями по номеру телефона вне зависимости от того, входят ли они в список друзей на Facebook или нет. Благодаря новой функциональности Messenger стал сильным полноценным конкурентом WhatsApp и других подобных сервисов.

Соцсеть Facebook выпустила новую версию приложения Facebook Messenger для Android и iOS. Самым важным ее нововведением стала возможность обмена мгновенными сообщениями по номеру телефона. Кроме того, в версии Messenger для iOS был обновлен дизайн – он был адаптирован под плоский вид iOS 7.

В конце декабря новая версия стала доступна для тестирования определенному кругу владельцев Android-смартфонов. Теперь ее может скачать любой владелец устройства на Android и iOS.

После установки Messenger автоматически распознает аккаунт владельца, если на смартфон установлено приложение Facebook. Если пользователь не зарегистрирован в Facebook, ему будет предложено перейти на сайт и пройти процедуру регистрации.

На следующем этапе необходимо указать номер мобильного телефона и ввести код подтверждения, который придет по SMS.

В программе отображается список друзей из Facebook, у которых тоже установлен Messenger. Кроме того, в новой версии есть список всех людей из адресной книги, которые пользуются Messenger, но при этом не входят в число друзей в Facebook. Всем им теперь тоже можно отправлять сообщения, которые будут доставлены мгновенно.

Чтобы добавить новый контакт, достаточно ввести номер мобильного телефона этого человека. Чтобы начать переписку с ним, необходимо, чтобы он тоже пользовался Messenger, при этом искать его аккаунт в соцсети и добавлять его в друзья не нужно.

Таким образом, новый Facebook Messenger стал прямым конкурентом популярным бесплатным сервисам обмена мгновенными сообщениями, таким как WhatsApp и Viber. При этом конкурентом достаточно серьезным, учитывая, что в Facebook зарегистрировано более 1 млрд пользователей. Для сравнения, аудитория мобильного приложения WhatsApp составляет более 300 млн активных пользователей в месяц.

Добавив возможность обмена сообщениями по номеру телефона, Facebook сможет расширить пользовательскую базу, так как для использования Messenger необходима регистрация в социальной сети.

Приложение Facebook Messenger является бесплатным, и в нем не отображается реклама. В WhatsApp реклама тоже не отображается, однако до некоторых пор его разработчики просили символическую плату за приложение. А в начале 2013 г. они объявил о намерении брать ежегодную плату в размере 1 дол. за пользование приложением.

Выпуск новой версии Facebook Messenger является результатом выбранного основателем и главой Facebook М. Цукербергом курсом на мобильные технологии. Ранее совместно с HTC был выпущен смартфон HTC First, с предустановленной оболочкой Facebook Home, но устройство не обрело популярности.

Наблюдатели отмечают исключительность этого события – дело в том, что Facebook впервые предложила свои возможности тем, кому сама по себе соцсеть не нужна ***(Facebook в одночасье сделал бессмысленными все мобильные мессенджеры // InternetUA (http://internetua.com/Facebook-v-odnocsase-sdelal-bessmislennimi-vse-mobilnie-messendjeri). – 2013. – 15.11).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Кількість читачів мікроблогу Папи Римського Франциска в Twitter перевищила 10 млн. «Дорогі фоловери, я дізнався, що вас уже більше як 10 млн. Сердечно дякую вам, і прошу продовжувати молитися за мене», – написав понтифік.

Мікроблог @Pontifex ведеться на дев'яти мовах: англійській, арабській, іспанській, італійській, латинській, німецькій, польській, португальській та французькій. Найбільше читачів іспаномовної версії – понад чотири мільйони.

За даними експертів Папської ради із соціальної комунікації, загальна аудиторія твітів Папи Франциска з урахуванням ретвітів (пересилання повідомлень понтифіка друзям і знайомим) може досягати 60 млн осіб.

Акаунт понтифіка у Twitter було створено в грудні 2012 р. Перший запис у ньому зробив колишній Папа Бенедикт XVI 12 грудня. Папа Франциск, обраний на апостольський престол 13 березня, помістив своє перше повідомлення в папському мікроблозі вже 17 березня, повідомляє РИА Новости ***(На Twitter у Папи уже понад 10 млн читачів // ZIK (http://zik.ua/ua/news/2013/11/04/na_twitter_u_papy_uzhe_ponad_10_mln_chytachiv_438027). – 2013. – 4.11).***

***

Корабли ВМС Украины фрегат «Гетман Сагайдачный» и корвет «Тернополь», которые в настоящее время выполняют задачи в дальних морских походах, отныне представлены в социальной сети Facebook.

В командовании украинского флота убеждены, что благодаря появлению страниц кораблей в популярной соцсети, граждане Украины узнают больше о жизнедеятельности экипажей и национальных ВМС в целом.

Флагманский корабль украинского флота фрегат «Гетман Сагайдачный» с вертолетом Ка-27 и группой специального назначения 12 октября в составе

многонационального корабельного соединения приступил к выполнению задач операции «Океанский щит» в Аденском заливе.

Противолодочный корвет «Тернополь» с 8 октября по 17 ноября выполняет задачи в рамках антитеррористической операции НАТО «Активные усилия» в определенных районах Средиземного моря ***(«Гетман Сагайдачный» и «Тернополь» представлены в социальной сети Facebook // Флот – 2017 (http://flot2017.com/posts/new/getman_sagajdachnyj_i_ternopol_predstavleny_v_socialnoj_seti_facebook). – 2013. – 5.11).***

***

Здавати гроші на те, чим повинна забезпечувати держава, набридло батькам нововолинських школярів. Батьки школярів і дошкільнят заявляють, що здають кошти під психологічним тиском. Перша спроба протистояння таким поборам з'явилася у мережі Інтернет, – повідомляє «Нововолинськ Діловий».

Група для тих, кому «набридло здавати гроші на те, чим повинна забезпечувати держава» була створена в соціальній мережі «Одноклассники» нещодавно. Нині вона налічує близько сотні активних учасників.

Адміністратором групи виступила молода мама двох малюків О. Шесталюк. Вона вважає, що державна та міська влада повинна забезпечити дітям безкоштовну освіту. Адже саме такою її декларує кожен український уряд. Проте на ділі батькам доводиться брати на себе чималу частку фінансових зобов'язань. З міського ж бюджету кошти, хоч і виділяються, проте незначні. До того ж їхнє освоєння часто викликає небезпідставні підозри про завищені ціни та нічим неприкриту безгосподарність заслужених чиновників.

«Багато батьків вважають добровільні внески примусовими, – розповідає О. Шесталюк. – Більшість здає їх з однієї причини – усі так роблять. Не бажаєш бути "білою вороною", хочеш, аби твою дитину не гнобили – теж здавай. Щоб зламати цей стадний інстинкт ми створили групу в соціальній мережі "Одноклассники". Вона називається "Ми проти поборів у навчальних закладах!".

Це перший крок до того, щоб батьки, які не хочуть здавати добровільні внески, об'єдналися між собою. Коли в групі чи класі не платитимуть цих коштів п'ятеро чи десятеро мам, тоді й інші перестануть. І що буде далі? Влада просто муситиме звернути на це увагу та знайти якесь рішення, а не звалювати все на плечі батьків».

Що ж, ідея насправді проста. Є група в соціальній мережі. У ній створено теми із номерами шкіл і дитячих садків. Кожна мама і тато може відмітити себе у тій темі, навчальний заклад якої відвідує їхня дитина. Таким чином зберуться групи однодумців і вже тоді разом зможуть вирішувати, як саме їм протистояти добровільно-примусовій підтримці освітнього бюджету.

До ідеї організованого спротиву поборам у навчальних закладах нововолинці дійшли вперше ***(На Волині вперше батьки об'єдналися проти поборів у школах // Волинські Новини***

(http://www.volynnews.com/news/analytic/na_volyni_vpershe_batky_obyednalysya_proty_poboriv_u_shkolakh_foto/). – 2013. – 14.11).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

С 5 ноября многие сообщества сети «ВКонтакте» получают доступ к рекламной бирже сети, которую анонсировали в конце октября (тогда к тестированию биржи получили доступ только избранные крупные сообщества). В настоящее время биржа работает в открытом бета-тесте, пишет AIN.UA (http://ain.ua/2013/11/05/500714).

Для начала работы с биржей у сообщества должен быть дневной охват не менее 100 тыс. пользователей, к концу года доступ к бирже появится у всех. Заявки на участие в бирже можно слать на почту exchange@corp.vk.com.

«Новая рекламная платформа предоставляет рекламодателям простой и прозрачный доступ к тысячам сообществ “ВКонтакте” для размещения рекламных записей. Цены на размещение формируются рынком и устанавливаются администраторами групп или публичных страниц», – говорится в сообщении компании. Помимо инструментов управления записями и подбора сообществ, рекламодателю предоставляется расширенная статистика для расчета эффективности рекламных кампаний.

Как AIN.UA рассказали в компании, фактически это означает, что у администраторов крупных сообществ появилась отдельная вкладка в разделе «Управление сообществом», с рекламными постами. Нажав на нее, администратор увидит все предложения с рекламными постами и ценами от рекламодателей, которые ему доступны. Он может выбирать посты, которые разместит у себя в сообществе. Эти предложения присылают рекламодатели, и как правило, содержание поста не меняется. Информацию о новых предложениях можно получать по почте или SMS. Администратор может анонимно обсудить с рекламодателем изменения в содержании поста. Для каждого поста есть статистика по переходам, охвату подписчиков, обратной связи.

Комиссия площадки составит около 45 %, куда будут включены все затраты на содержание и развитие сервиса, премии и бонусы рекламным агентствам, скидки крупным рекламодателям. «С введением прогрессивной шкалы, комиссия для небольших сообществ будет существенно снижена. При этом администраторам будет перечисляться вся сумма, указанная в заявке на размещение. “ВКонтакте” также берет на себя обязательства по уплате НДС», – сообщают в компании. Информацию о бирже можно найти на странице о рекламе «ВКонтакте», в разделе «Рекламные записи в сообществах» ***(«ВКонтакте» официально открывает биржу рекламных постов // AIN.UA (http://ain.ua/2013/11/05/500714). – 2013. – 5.11).***

***

Социальные сети очень популярны среди тех, кто ищет работу или расширяет сеть своих контактов, но когда речь идет о конкретных вакансиях, прибегать к помощи социальных сетей бессмысленно, выяснили специалисты рекрутинговой компании Hyphen. Кандидаты не верят в то, что социальные медиа могут быть правильным способом поиска работы, и поэтому до сих пор предпочитают традиционные методы трудоустройства. Примерно четверть профессионалов, опрошенных Hyphen, сказали, что даже если они размещали в соцсетях резюме с целью поиска работы, то не ожидали, что их информация будет воспринята всерьез, пишут Vedomosti.ru.

«Многие компании в последнее время создают свои рекрутинговые страницы и страницы поиска талантов в социальных сетях. И, к счастью, большинству работодателей все чаще удается найти кандидатов через эти источники», – говорит З. Вэди, управляющий директор Hyphen. Однако, добавляет он, «в соцсетях до сих пор мало вывешивается объявлений о поиске работы. Кандидаты предпочитают искать работу традиционными методами, так как боятся, что к ним не отнесутся серьезно». По мнению З. Вэди, «создание рекрутинговых каналов и каналов по поиску талантов в социальных сетях не должно рассматриваться просто как предоставление интернет-площадки талантливым соискателям, где размещается информация о рекрутинговых схемах и новых вакансиях». «Эффективное использование социальных медиа в рекрутинге напрямую связано с привлечением внимания к бренду работодателя и адаптации этих сайтов к нуждам целевой аудитории», – заявляет З. Вэди ***(Активность соискателей в LinkedIn или Twitter не сильно повышает шансы найти работу // IT Expert (http://itexpert.in.ua/rubrikator/item/31488-aktivnost-soiskatelej-v-linkedin-ili-twitter-ne-silno-povyshaet-shansy-najti-rabotu-issledovanie.html). – 2013. – 6.11).***

***

По данным отчета Simply Measured, 71 % самых крупных мировых брендов создали свой профиль в сети Instagram, которая в настоящее время составляет конкуренцию Google+ и Pinterest и является самой быстрорастущей социальной медиа в мире. Отчет включал мониторинг хэштегов брендов, мульти-контроль за текущими записями, мониторинг конкурентов и фотографий социальных медиа.

Н. Смита, специалист по маркетингу Simply Measured, отметил, что это был всеобъемлющий обзор брендов по всем социальным каналам, рассматриваемый в контексте других активностей в социальных медиа. «Instagram – это канал, который мы будем отслеживать какое-то время. Это отличный источник для брендов в целях распространения маркетинг-контента», – заявил эксперт. В этом случае, создание профилей брендов крайне важно, особенно для привлечения новых пользователей.

Топ-бренд в Instagram – Mercedes-Benz, у которого более чем 425 тыс. подписчиков и примерно 9 млн вовлеченных пользователей. Возможно, это

удивительно, учитывая, что Instagram предназначен в основном для молодежи. Но Н. Смита отметил, что Mercedes проделали отличную работу по визуализации своей истории, что и сделало его одним из лучших брендов.

Как и многие другие бренды, Mercedes-Benz получили больше всего вовлечения пользователей благодаря фото. Видео используются не так активно, Н. Смита допускает, что фото будут в преимуществе перед видеоконтентом. Означает ли это, что видео в Instagram не сработают?

Возможно, нет, заявляет Н. Смита, но добавляет, что слишком рано говорить про влияние рекламы на вовлечение пользователей. Она будет органично интегрирована, как спонсорские истории в Facebook. Первым брендом, который опубликовал свою рекламу в Instagram, стал Michael Kors.

Другие выводы исследования.

При увеличении количества активностей, растет число фолловеров. 57 % маркетологов топ-брендов публикуют хотя бы один пост в неделю, в 2012 г. эта цифра равнялась 38 %. В результате, примерно 1/3 брендов имеют по 10 тыс. подписчиков, а 19 % насчитывают до 100 тыс. подписчиков.

Вовлечение подписчиков быстро растет. Вовлечение в бренд возрастает примерно на 350 % каждый год, частично благодаря увеличению на 70 % публикаций в сетях.

Бренды автомобилей, медиа и бренды класса люкс в преимуществе. Mercedes-Benz, BMW и Audi топ-3 самых вовлеченных бренда в мире.

Фото получают больше комментариев и лайков, чем видео. Как и большинство новых функций, видеоконтент не настолько быстро получит популярность, как фото (только 6 % всех постов). Фото вызывают на 26 % больше вовлечения, чем видео.

Хэштеги стали нормой. 83 % постов Instagram включают хотя бы один хэштег, 63 из 65 активных брендов в Instagram используют эти функции. Что характерно, топ-бренды используют хэштеги более активно, чем другие бренды ***(Исследование: Instagram – самая быстрорастущая социальная сеть среди брендов // Marketing Media Review (http://mmr.ua/news/id/issledovanie-instagram-samaja-bystrorastuschaja-socialnaja-set-sredi-brendov-36932/). – 2013. – 6.11).***

***

Правообладатели проиграли в арбитраже Петербурга два дела о взыскании с соцсети «ВКонтакте» компенсации за нарушение авторских прав на песни, размещенные на страницах пользователей. Эксперты расходятся в оценках того, останется ли соцсеть неуязвимой для претензий, сообщает newsoboz.org. со ссылкой на digit.ru.

Арбитражный суд Петербурга и Ленинградской области в начале ноября отказал ООО «Никитин Медиа Диджитал Контент» (Никитин ЭмДиСи, Москва) в иске о взыскании с ООО «ВКонтакте», владельца одноименной социальной сети, 750 тыс. р. Судебное разбирательство было связано с размещением в соцсети десяти фонограмм Г. Лепса, в то время как компания

«Никитин» является обладателем исключительных смежных прав на его произведения, включая их доведение до всеобщего сведения.

Арбитраж Петербурга в октябре отказал в удовлетворении иска российского рекорд-лейбла «Студия СОЮЗ» о взыскании с ООО «ВКонтакте» 4,575 млн р. за нарушение авторских прав. Претензии к соцсети касались размещения 61 фонограммы, в том числе песен с альбома «Феникс» группы «Ария», а также композиций с альбома «TODD. Акт 2. На краю» группы «Король и Шут» (последний студийный альбом, изданный при жизни лидера коллектива М. Горшенева).

«За последний месяц выиграли два иска против музыкальных правообладателей: “Никитин” и “Союз”. Не удается бабок срубить им таким образом. Бедняги», – написал на своей странице заместитель генерального директора «ВКонтакте» И. Перекопский.

Эксперты расходятся во мнениях по поводу того, будет ли социальная сеть и в дальнейшем выигрывать аналогичные судебные процессы. «Я согласен с позицией суда», – сказал РИА Новости представитель Фонографической ассоциации Петербурга. По его оценке, одним из основных аргументов в пользу «ВКонтакте» является то, что ни сама соцсеть, ни ее пользователи не получают вознаграждения за размещение спорных музыкальных произведений.

«Если правообладателями в суде будет доказано, что сеть “ВКонтакте” имеет заинтересованность в размещении данного контента на сайте, решение (суда. – Ред.) может быть другим», – отметил собеседник агентства.

Он добавил, что проигрыш правообладателей в суде первой инстанции отчасти может быть обусловлен и тем, что соцсеть удаляет те фонограммы, которые размещены с нарушением авторских прав, после того, как правообладатели подтвердят свои полномочия и обратятся к администрации «ВКонтакте» с соответствующими требованиями. «Эта процедура должна быть соблюдена, и “ВКонтакте” от нее не отказывается. Поэтому мы и имеем такой результат судебных заседаний», – сказал представитель фонографической ассоциации.

Генеральный директор Северо-Западного центра по защите авторских прав Т. Бичев считает, в свою очередь, что судебные споры с соцсетью по поводу размещения музыки будут продолжаться, и по мере усиления борьбы с пиратством можно ожидать решений в пользу правообладателей. «Я думаю, что иски будут продолжаться», – сообщил он РИА Новости, добавив, что в случае с исками компании «Никитин» и студии «СОЮЗ» суды «не совсем учли», что спорные песни находятся на сервере «ВКонтакте», а не на жестких дисках частных компьютеров пользователей соцсети.

По словам певицы Т. Булановой, за скачивание музыкальных произведений из социальных сетей можно было бы брать «символические деньги» в пользу правообладателей, в том числе и самих артистов. «Конечно, это (размещение песен “ВКонтакте”. – Ред.) удобно – я и сама пользуюсь. <...> Но если за скачивание возьмут 10 или даже 100 р., то для меня это не будет существенной тратой, а артисту пойдет в плюс», – сказала она, отметив, что

размещение песен и видео-клипов в соцсети способствует популяризации творчества ***(«ВКонтакте» побеждает правообладателей музики // NewsOboz (http://newsoboz.org/it_tehnologii/-vkontakte-pobezhdaet-pravoobladateley-muzyki-10112013233000). – 2013. – 10.11).***

***

Facebook тестирует возможность пятибалльной оценки брендов. Рейтинги из пяти «звездочек» на страницах компаний и сервисов стали доступны некоторым пользователям.

До сих пор система оценки использовалась только в мобильной версии Facebook: первый рейтинг появился в начале 2012 г. в приложении Nearby. Видимо, теперь социальная сеть готова распространить возможность выставления рейтингов и на экраны персональных компьютеров, сообщаетTechcrunch.com.

«Звездочки» будут отображаться на страницах, посвященных различным местам и брендам – как наверху хроники, так и в сообщениях ленты новостей. В компании надеются, что введение публичной оценки позволит потребителям больше узнать о доступных продуктах и сервисах, а брендам – повысить осведомленность и привлечь новую аудиторию.

Безусловно, такой рейтинг даст больше информации об отношении пользователей к бренду: это уже не простая констатация наличия/отсутствия «лайка». Система «лайков» двусмысленна по своей сути: посетители ставят их, чтобы выразить симпатию, сочувствие, солидарность, интерес, а в некоторых случаях – неприятие и недовольство. Количество оценок «мне нравится» говорит о том, насколько сильно пост или страница привлекают внимание аудитории, однако не позволяет сделать выводов о том, как пользователи относятся к контенту. Некоторое представление об этом можно получить из комментариев, однако не все пользователи активны в таком общении, что делает оценку весьма субъективной.

Пока остается неясным, будет ли рейтинг обязательным для всех брендовых страниц. Если Facebook видит своей задачей отыграть у Foursquare и других аналогов нишу, связанную с рекомендацией локальных сервисов, такая опция будет предусмотрена по умолчанию. Это заставит компании изменить концепцию продвижения в социальной сети: им придется предложить нечто большее, чем просто активное информационное присутствие. Получить «лайк» относительно просто. Однако для того, чтобы пользователь выставил высокую оценку, придется приложить гораздо больше усилий ***(Facebook тестирует возможность пятибалльной оценки брендов // Marketing Media Review (http://mmr.ua/news/id/facebook-testiruet-vozmozhnost-pjatiballnoj-ocenki-brendov-36974/). – 2013. – 8.11).***

***

Рекламные посты, появившиеся на фотосервисе Instagram, вызвали большой энтузиазм у пользователей. Как объявил глава компании К. Систром

на конференции Gigaom Roadmap, около 5 % человек, увидевших продвигаемую фотографию, поставили ей «лайк». «Это довольно огромная цифра, с учетом того, что мы игнорируем большую часть рекламы в Интернете», – сказал он.

Кроме того, сказал К. Систром, в комментариях к снимку, рекламирующему часы бренда Michael Kors, многие пользователи спрашивали, где они могут купить такой же аксессуар. Слова гендиректора Instagram недалеки от истины. Аналитики из компании Nitrogram подсчитали, что эту фотографию увидело около 6,15 млн человек, а получила она 218 тыс. «лайков» (в процентах к просмотрам – 3,57 %).

К. Систром подчеркнул, что реклама – это еще один шаг Instagram на пути к лидерству. «У нас свыше 150 млн активных пользователей. Мы превратились из крутого стартапа в нечто, что влияет на мейнстрим», – сказал он, добавив, что на сервис ежедневно загружается более 55 млн фотографий.

По поводу конкурирующих продуктов, а также Facebook (компании-владельца Instagram) К. Систром сказал: «Я не думаю, что появится замена Facebook, Twitter или Instagram». По его словам, владельцы смартфонов, скорее, начнут уделять больше или меньше времени другим приложениям, но эти сервисы вряд ли вымрут в обозримом будущем.

К. Систром добавил, что поиск по хештегам (словам, начинающимся со знака решетки) сейчас не пользуется большой популярностью в Instagram. В будущем, намекнул он, на сервисе может появиться система поиска фотографии, схожая с Graph Search, как в Facebook ***(Реклама в Instagram понравилась одному из 20 пользователей // Marketing Media Review (http://mmr.ua/news/id/reklama-v-instagram-ponravilas-odnomu-iz-20-polzovatelej-36971/). – 2013. – 8.11).***

***

Одна из крупнейших продовольственных сетей Украины «Велика Кишеня» решила «двигаться в ногу со временем» и развивать направление digital в рекламе. Начали с запуска онлайн-игры «Купить за 60 секунд». Как утверждают в компании, это первая в Украине онлайн-игра о продовольственном супермаркете – с ее помощью люди научатся быстро скупаться в преддверии праздников. А заодно игра поможет ритейлеру собрать их персональные данные из соцсетей, пишет AIN.UA (http://ain.ua/2013/11/07/501159).

Для того, чтобы сыграть в игру, необходимо сначала пройти авторизацию через Facebook или «ВКонтакте». Приложение запрашивает доступ к личным данным пользователя, на основании анализа которых, вероятно, будет таргетироваться реклама «Великой Кишени» в процессе дальнейшей реализации вышеупомянутой digital-стратегии.

Суть игры в том, чтобы собрать продукты из предложенного списка разных категорий за 60 секунд, развивая при этом внимательность, реакцию и интуицию. Игра оформлена в фирменных цветах ритейл-сети, содержит

логотип и символ – «Кишеньку». Как пояснили в компании, общая концепция игры задумана таким образом, чтобы у пользователя создавалось ощущение, будто он отоваривается в одном из супермаркетов сети. Авторы идеи с помощью новой игры надеются установить связь между положительными эмоциями, которые вызывает игра, и брендом «Велика Кишеня».

Активным игрокам обещают подарки – в конце каждой недели будут определять случайных победителей, которые получат в подарок продуктовую корзину ***(«Велика Кишеня» запустила online-игру, которая собирает данные пользователей в соцсетях // AIN.UA (http://ain.ua/2013/11/07/501159). – 2013. – 7.11).***

***

Стартовая эйфория, которой сопровождалось размещение акций Twitter на бирже, завершилась. Во второй день после IPO котировки сервиса микроблогов упали, сообщает 3dnews.ru.

В пятницу, 8 ноября, торги акциями Twitter завершились падением их стоимости на 7,2 % – до 41,65 дол. По итогам первой сессии ценные бумаги подорожали до 44,9 дол., притом что цена размещения составила 26 дол. На своем IPO компания заработала 2,09 млрд дол.

Инвесторы оценивали Twitter в 14 млрд дол., однако за первый день торгов в Нью-Йорке рыночная капитализация соцсети достигла 24 млрд дол. Спустя день она снизилась до 19,68 млрд дол.

Таким образом, первичное размещение Twitter стало самым крупным на технологическом рынке после IPO Facebook в мае прошлого года. После выхода компании М. Цукерберга на биржу ее акции начали стремительно дешеветь, и за несколько месяцев они опустились ниже 19 дол.

Перед своим IPO Twitter озвучила показатели работы в III квартале. Выручка сервиса составила 168,6 млн дол. против 82,3 млн дол. годом ранее. За год чистый убыток компании возрос с 21,6 до 65,6 млн дол. Ежемесячная активная аудитория Twitter превышает 230 млн пользователей ***(Биржевая эйфория вокруг Twitter подошла к концу // IT Expert (http://itexpert.in.ua/rubrikator/item/31628-birzhevaya-ejforiya-vokrug-twitter-podoshla-k-kontsu.html). – 2013. – 10.11).***

***

Шесть причин, по которым биржа «ВКонтакте» не будет работать

1. Огромная комиссия.

Комиссия в 45 % – в полтора раза больше, чем позволяют себе такие компании, как Apple или Facebook.

Важно понимать, что «ВКонтакте» не работает бесплатно – система взимает конскую комиссию в 45 % + НДС.

4500 р. как стоимость рекламного поста «у себя», 9600 р. как стоимость «для всех».

Тут много непонятного. Впрочем, сам П. Дуров пишет: «Как было сказано, для абсолютного большинства сообществ цифра комиссии составит 20 %. Текущая цифра в интерфейсе для Вашего сообщества – временная». Похоже, что с размером комиссии еще до конца не определились даже внутри компании.

2. «Туман» с выводом денег.

Как с этим будут работать физлица? Юрлица? Граждане сопредельных государств? Будут ли бухгалтера соцсети подавать данные о заработках в налоговую? Вопросов больше, чем ответов.

3. Реклама не отличается от обычного контента.

Никаких маркеров «Реклама», выделения цветом или тегами не предусмотрено. Конечно, при невозможности поменять текст, рекламу можно будет легко распознать по клише, которые так любят все маркетологи, все эти «легендарные армии», «играй здесь», «нажимай сюда», «уникальная возможность», «осталось всего 5!» и прочим вовлекающим оборотам, которые, похоже, даются на первом уроке в любой школе маркетинга для старшеклассников.

Но ни Facebook, ни Instagram, ни Twitter себе такого не позволяет. Впрочем, «контент» на многих популярных страницах во «ВКонтакте» настолько неотличим от рекламы, что особого неудобства пользователям это, скорее всего, не доставит.

4. Сомнительная отдача.

Мы потратили 10 тыс. р. и получили 200 кликов – это 50 р. за переход. Привычным таргетом в том же «ВКонтакте» можно добиться на порядок более выгодных результатов. Правда, евангелист «ВКонтакте» говорит прямо, что биржа это то же самое, что и медийка.

Зачем тут тогда вообще CTR, клики и другие метрики?

Если это медийная реклама, то цены на нее на страницах с сомнительной аудиторией у опытного медиапланера вызовет еще больше вопросов.

Со стороны, возможно, не видно общей картины, ведь, по словам П. Дурова, «рекламодатели уже выстроились в очередь». Заставил всю редакцию подписаться на все популярные страницы, будем играть в игру «реклама или нет».

5. Неопределенность для сторонних игроков.

По словам «ВКонтакте»: «Ликвидировать доступ сторонним биржам пока что никто не собирается».

Ключевое здесь слово – «пока». Существует дюжина добротных сторонних решений по покупке рекламы, которые на сегодняшний день оказались не в самой понятной ситуации. С одной стороны, вроде бы им разрешили пока работать. С другой стороны, никто не даст гарантий того, что через месяц-другой, после того как внутренняя биржа будет отлажена и начнет работать на все 100 %, им не перекроют доступ и не выгонят на улицу (в Facebook, «Одноклассники»).

6. Нельзя измерить эффективность.

22 октября к нам пришло 200 человек по бирже. Как выяснить, кто эти люди, сколько статей они читали и стоило ли это 300 дол., совершенно непонятно. Почему переходы не маркируются соцсетью? Давно известно, что на ссылки через bit.ly или с UTM-метками люди нажимают куда менее охотно, чем на обычные.

Как и любое новое решение, биржа вызвала шквал критики и вопросов ***(6 причин, по которым биржа «ВКонтакте» не будет работать // InternetUA (http://internetua.com/6-pricsin--po-kotorim-birja-vkontakte-ne-budet-rabotat). – 2013. – 11.11).***

***

До какого предела растить аудиторию в Facebook? Aegis Media провело интересный эксперимент в социальной сети.

В рамках исследования в Facebook было создано несколько страниц несуществующего мебельного бренда Ashwood Furnishings, который якобы имел 150-летнюю историю и планировал экспансию на рынок США. Все, чем брендовые страницы отличались друг от друга – это количество лайков. Самая «непопулярная» из страниц содержала всего несколько отметок, самая «востребованная» – более 9 млн, пишет Thedrum.

Далее страницы бренда показывали группам респондентов и предлагали оценить по различным показателям. Результаты не оказались сюрпризом: чем больше лайков содержала страница, тем выше бренд котировался по всем показателям (интерес, доверие, готовность купить и рекомендовать, важность). Кроме того, по мере роста количества лайков росла и оценка того, сколько бренд предположительно будет стоить.

Однако, судя по полученным данным, после того как страница набирает 10 тыс. отметок, дальнейшие лайки уже не дают пропорциональный рост позитивного восприятия. При оценке бренда значение количества лайков стремительно растет до определенного предела, затем начинает снижать темп роста и постепенно переходит в «длинный хвост».

Исследование Aegis Media доказало, что пользователи Facebook могут придавать бизнесу косвенную ценность. По словам CEO компании Aegis Media в Великобритании Р. Хорнера, проведенный эксперимент явился лишь первым шагом в понимании механизма влияния социальной сети на поведение потребителей: «Это был пилотный проект. В ближайшем будущем мы планируем провести более широкое исследование, которое позволит более полно взглянуть на использование социальных сетей и других факторов, влияющих на потребительское поведение» ***(Ломская Т. Aegis Media: Насколько количество подписчиков в Facebook влияет на ценность бренда // Marketing Media Review (http://mmr.ua/news/id/aegis-media-naskolko-kolichestvo-podpischikov-v-facebook-vlijaet-na-cennost-brenda-37004/). – 2013. – 11.11).***

***

Испанский банк la Caixa запустил социальную сеть StockTactics для поддержки своего онлайн-брокера Bolsa Abierta. На сегодняшний день эта онлайн-компания обслуживает 1 млн пользователей, и социальная сеть станет для них площадкой, где они смогут поделиться своим опытом и обсудить инвестиционные стратегии.

Пользователи социальной сети смогут моделировать портфели акций и отслеживать их состояние в соответствии с реальными рыночными условиями. Инвесторам будут доступны для просмотра профили других участников сети, они смогут обмениваться друг с другом мнениями и комментариями.

В сообществе будет создаваться рэнкинг наиболее популярных акций, которыми торгуют участники, наиболее прибыльных портфелей и наиболее активных инвесторов. К сети можно будет подключиться и через мобильное приложение.

Клиентами банка в Испании является 9,4 млн человек, более трети из них пользуются мобильными банковскими сервисами. Создание сообществ по интересам, позволяющих участникам установить новые связи и деловые контакты, – часть стратегии la Caixa. Раньше банк создал клуб для своих пожилых клиентов, где они могут обмениваться информацией и мнениями о культурных мероприятиях ***(Испанский банк запустил социальную сеть для клиентов-инвесторов // IT Expert (http://itexpert.in.ua/rubrikator/item/31709-ispanskij-bank-zapustil-sotsialnuyu-set-dlya-klientov-investorov.html). – 2013. – 13.11).***

***

IBM тестирует технологию, которая позволит выявлять психологические особенности человека по его постам в Twitter. В случае успеха проекта рекламодатели смогут настраивать рекламные сообщения в соответствии с характером и темпераментом каждого пользователя.

В чем суть нового программного обеспечения? Для каждого пользователя создается персональный профиль, включающий в себя последние обновления его Twitter – от нескольких сотен до нескольких тысяч постов. Данные обрабатываются, после чего характер пользователя автоматически оценивается по пяти базовым психологическим категориям: открытость новым идеям и впечатлениям, добросовестность, экстраверсия, конформность, нейротизм, пишет Mashable.com.

Также выявляются руководящие человеком «ценности» (например, гедонизм или консерватизм) и «потребности» (например, любопытство или гармоничные отношения).

Программный код для обработки данных Twitter был создан на основе исследования содержимого микроблогов нескольких сотен респондентов. Испытуемые заполнили опросники с психометрическими тестами. Результаты были проанализированы специальным программным обеспечением, которое выявило высокую корреляцию – более 80 % – между ответами респондентов и

содержимым их Twitter-аккаунтов. Однако все зависит от цели ведения блога: когда он использовался для публикаций на профессиональные темы, зависимость твитов характера владельца аккаунта прослеживалась не столь явно.

Кроме того, исследование выявило, как различные речевые конструкции сочетаются с психологическими чертами личности. На основе этих данных были созданы языковые модели, позволяющие самостоятельно извлекать из микроблога пользователя его психологический портрет.

Технология уже тестируется некоторыми партнерами IBM. Сейчас необходимо определить, насколько «психологически настроенные» сообщения эффективнее стандартной рекламы. Разработчики ожидают очень высокого уровня конверсии – как минимум, выше обычного отклика в 0,34 % от e-mail и 13 % от холодных звонков. Если система окажется успешной, бренды смогут учитывать индивидуальный характер пользователя при настройке e-mail рассылки и рекламных сообщений в социальных сетях, а также определять, какой контент он увидит после авторизации в своем аккаунте.

Новинка также пригодится в call-центрах и центрах клиентского обслуживания. Она позволит на основе профиля пользователя понять, какое взаимодействие для него оптимально: желает ли он получать от компании исключительно информацию или же ждет эмоционального участия и поддержки ***(Twitter позволит рекламодателям проникнуть в психологию потребителя // Marketing Media Review (http://mmr.ua/news/id/twitter-pozvolit-reklamodateljam-proniknut-v-psihologiju-potrebitelja-37036/). – 2013. – 13.11).***

***

По результатам опроса компании ESET, только 29 % пользователей каким-либо образом редактируют содержание аккаунтов социальных сетей при поиске работы (удаляют фото и видео сомнительного содержания, вычищают список друзей, ставят более привлекательную аватарку и т. д.), в то время как 65 % потенциальных работодателей проявляют интерес к этой информации и просматривают ее при принятии решения относительно той или иной вакансии. Еще 15 % опрошенных используют настройки приватности сервисов, заранее предполагая, что их личные профили могут заинтересовать работодателей. Они скрывают от посторонних глаз персональную или компрометирующую информацию, ограничивая ее видимость «только для друзей», либо «для себя».

Сразу 56 % соискателей ничего не меняют в своих профилях – не корректируют содержание, не ограничивают видимость, не скрывают друзей и даже не удаляют комментарии или изображения с ненормативной лексикой. По мнению большинства пользователей, эта информация не интересна посторонним людям.

Однако работодатели так не думают – по данным опроса, проведенного компанией FutureToday по заказу компании ESET, 65 % работодателей просматривают социальные профили кандидатов, приславших им резюме. Подавляющее большинство из них учитывают собранную таким образом информацию, принимая решение относительно того или иного кандидата.

Что примечательно, пользователи разных социальных сервисов и сообщества ESET Club, в которых проходил опрос, проявили редкое единодушие в своей беспечности – от 55 % («Одноклассники») до 61 % (Facebook и ESET Club) опрошенных не задумываются о том, что их профили в соцсетях могут заинтересовать работодателя.

Осторожные соискатели по-разному готовятся к поиску работы – так, содержание своих аккаунтов меняют 30 % пользователей «ВКонтакте» и всего 14 % завсегдатаев Facebook. Зато продвинутые настройки приватности применяют лишь 14 % соискателей из «ВКонтакте», а из Facebook – 25 %. В «Одноклассниках» эти две группы пользователей разделились примерно поровну (22 % корректируют содержание и 23 % ограничивают доступ сторонним лицам).

«Важно понимать, что кандидаты зачастую пользуются не одной, а сразу несколькими социальными сетями, и профиль в каждой из них может служить для "разных" целей. По своему опыту скажу, что профиль "ВКонтакте" больше носит развлекательный характер и служит личным целям, Facebook – для неформального общения с более "формальными" друзьями и нетворкинга, а аккаунт в LinkedIn вообще может заменить официальное резюме, а при желании его можно "залинковать" со всеми другими своими страницами.

Также не могу не отметить и обратный процесс – при поиске работы кандидаты начинают интересоваться страничками компаний в социальных сетях, и порой они становятся более важным источником информации о карьерных возможностях компаний, чем их официальные сайты. Если HR компаний хотят выйти в социальные сети, они должны быть готовы к постоянной работе со своими страницами», – отметила С. Саори, бренд-менеджер компании FutureToday.

Стоит отметить, что интерес работодателей к социальным профилям кандидата на ту или иную позицию – это не только повод скрывать информацию, но и, напротив, возможность продемонстрировать свои сильные стороны, которые могут заинтересовать работодателя, делают вывод эксперты ***(Соцсети попали в поле зрения работодателей // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/23259-2013-11-15-07-10-07.html). – 2013. – 15.11).***

***

Сеть микроблоггинга Twitter заявила, что в ближайшем времени запустит сервис автоматизированного размещения рекламы для клиентов за пределами США. В Twitter говорят, что международная версия системы будет ориентирована на предприятия малого и среднего бизнеса. На первом этапе рекламная платформа заработает для коммерческих клиентов в Великобритании, Ирландии и Канаде, где клиенты смогут покупать услугу Promoted Tweets. Здесь запуск состоится на будущей неделе ***(Twitter запускает за пределами США систему размещения рекламы // InternetUA***

(http://internetua.com/Twitter-zapuskaet-za-predelami-ssha-sistemu-razmesxeniya-reklami). – 2013. – 17.11).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Социальные сети могут негативно влиять на работу иммунной системы организма, гормональный баланс, работу артерий и процессы мышления, пишет E-news.

Биолог из Великобритании А. Сигман опубликовал в журнале британского Института биологии Biologist результаты исследования влияния социальных сетей на здоровье человека, сообщает Русская служба «Би-Би-Си». Статья называется «Всегда на связи: биологическое влияние социальных сетей».

По мнению британского ученого, чрезмерное увлечение социальными сетями в Интернете может вредить здоровью из-за сокращения общения с реальными людьми. В частности, утверждает ученый, недостаток общения может негативно влиять на работу иммунной системы организма, гормональный баланс, работу артерий и процессы мышления, что в долгосрочной перспективе повышает риск появления и развития таких болезней, как рак, сердечно-сосудистые заболевания и слабоумие.

Это связано с тем, пишет в статье А. Сигман, что физиологические процессы в организме протекают по-разному в зависимости от того, находится человек в одиночестве, в чьем-то обществе или в виртуальной реальности, что сейчас происходит все чаще. «Многое из этого еще предстоит исследовать, но, похоже, существует разница между влиянием реального присутствия кого-то и виртуальным заменителем общения», – полагает биолог.

В среднем общение британцев с 1987 г. с шести часов сократилось почти до двух часов в 2007 г. Зато использование Интернета за это время возросло с четырех до почти восьми часов в день. При этом за два десятилетия, констатирует А. Сигман, количество людей, которым, по их же словам, не с кем обсудить важные вопросы, почти утроилось.

Также ученый отмечает, что родители все меньше времени проводят с детьми – меньше всего детей ужинают с родителями среди всех европейских стран именно в Великобритании.

В статье биолог также отвергает утверждение, будто социальные сети способствуют установлению контактов между людьми. По его мнению, они дают лишь иллюзию общения. «По идее, социальные сети должны способствовать нашей социальной активности, но в реальности мы наблюдаем

совсем другое. Хвост виляет собакой, вместо того чтобы интенсифицировать общение, социальные сети его подменяют», – считает А. Сигман.

Британские ученые не первый раз высказывают опасения касательно социальных сетей. Так, в прошлом году на собрании в британском Королевском колледже психиатров было высказано мнение, что социальные сети искажают восприятие реальности.

По мнению психиатров, у поколения 1990-х годов, которому неведом мир без Интернета, может развиться «потенциально опасный» взгляд на окружающий мир и собственную личность. Дети, которые с пеленок привыкли к социальным сетям, могут испытывать трудности в «реальных» взаимоотношениях с людьми, поскольку плохо разбираются в тонких оттенках выражений лица, тона голоса и языка тела.

К тому же социальные сети формируют у подростков ложное впечатление, что любовь и дружбу легко завоевать и столь же легко разрушить. «Это мир, где события происходят стремительно, где все постоянно меняется, где от близкого человека можно избавиться одним щелчком мыши, где в одно мгновение можно уничтожить свой профиль, если он не нравится, и заменить его на более приемлемый», – отметил доктор Х. Тяги.

Психиатр также отметил, что людям, привыкшим к быстрому течению интернет-жизни, реальность может показаться слишком скучной, и они могут попытаться «оживить» ее, совершая импульсивные поступки, в том числе попытки самоубийства, поскольку им свойственно занижать ценности реальной жизни ***(Ученые: общение в социальных сетях опасно // Индустриалка (http://iz.com.ua/mir/24090-uchenye-obschenie-v-socialnyh-setyah-opasno.html). – 2013. – 6.11).***

***

Одинокие женщины не должны просматривать профили своих успешных друзей в Facebook. По словам психологов, это может реально подорвать их здоровье, передает The Daily Mail.

Специалист З. Стримпель подчеркивает: социальные сети постоянно «бомбардируют» пользователей картинками идеальной жизни, идеальных свадеб, детей, что вызывает у людей зависть и способствует развитию интернет-вуайеризма. В итоге у человека может возникнуть ощущение того, будто его жизнь пуста.

З. Стримпель призывает одиноких женщин полностью отказаться от социальных сетей. Кстати, по словам З. Стримпель, слабый пол проводит больше времени в поисках потенциальных женихов в Интернете. А наличие персональных данных в профилях социальных сетей заставляет женщин чрезмерно анализировать кандидатов. Потом складывается впечатление, что эти люди уже присутствуют в жизни женщины ***(Социальные сети вредят психике одиноких женщин // Новости Mail.Ru (http://news.mail.ru/inworld/ukraina/global/112/society/15541654/). – 2013. – 7.11).***

***

Изучив более 8 млн изображений в Instagram, аналитики из фирмы Curalate выяснили, что фотографии с преобладанием синего цвета получают в среднем на 24 % больше лайков, чем другие снимки.

Кроме того, большой популярностью пользуются изображения с невысокой насыщенностью и цветовыми блоками. Так, на 29 % больше лайков получают изображения, на которых преобладает фон.

Популярностью пользуются картинки, на которых доминирует какой-то один цвет. В среднем, они популярнее других на 40 %, хотя таких изображений вообще мало – около 10 %. В основном преобладают разноцветные фотографии.

Среди других установленных тенденций: светлые фотографии популярнее тёмных на 24 %, а фотографии с наложенной текстурой получают на 80 % больше лайков. Меньше всего лайков собирают фотографии в красных и оранжевых тонах.

Отдельного изучения удостоились фильтры Instagram. Снимки, обработанные фильтрами Walden и Rise, которые специально снижают цветовую насыщенность фотографии, собирают на 18 % больше лайков, чем изображения после других фильтров.

Важным оказалось и соотношение деталей и фона. Если в кадре отчётливо выделяется задний план, который занимает около 90 % от всего снимка, то изображение оказывается на 30 % интереснее, чем фотографии без фона вообще ***(Аналитики вычислили секрет популярности фотографий в соцсетях // InternetUA (http://internetua.com/analitiki-vicsislili-sekret-populyarnosti-fotografii-v-socsetyah). – 2013. – 12.11).***

***

Группа психологов из Канады и США продемонстрировала важность социального взаимодействия для сохранения и совершенствования прикладных знаний и умений. Исследователи выяснили, что социальные сети способствуют передаче навыков, причем в работе ученых термин социальная сеть используется в своем первоначальном значении. Подробности приводятся в статье для журнала Proceedings of the Royal Society B: Biological Sciences.

Авторы, специалисты из университетов Британской Колумбии (Канада) и Калифорнии (США) ставили перед собой задачу проверить гипотезу о важности социальных сетей для накопления и сохранения знаний. Собрав две группы добровольцев, ученые поставили перед ними задачу передать «следующему поколению» (другим участникам опытов) знания о том, как правильно завязывать узлы или как рисовать сложную фигуру в графическом редакторе. В одной группе действовало правило: каждый участник получает знания от одного учителя и передает их одному ученику, а во второй группе можно было учиться у всех пяти учителей, представляющих прошлое «поколение».

Сопоставив навыки разных групп через десять поколений, экспериментаторы выяснили то, что одиночки в итоге утратили часть знаний и навыков или остались на уровне первого поколения. В группах, которые могли учиться друг у друга, картина была иной: навыки, напротив, стали заметно лучше. К примеру, сложная фигура из нескольких окружностей в участников совместно обучавшейся группы с восьмого поколения получалась практически неотличимой от оригинала (одна ошибка на пять попыток), в то время как одиночки в лучшем случае рисовали правильно в двух случаях из пяти. В случае с вязанием узлов ситуация была хуже, но и тогда последнее совместное поколение правильно выполняло две трети заданий, в то время как последнее одиночное делало две трети узлов с ошибками.

По мнению исследователей, эти опыты подтверждают важность социального взаимодействия для сохранения знаний. О важности общения и развития социальной сети представители различных гуманитарных отраслей говорили давно, однако большая часть аргументов в пользу необходимости социальных сетей следовала из исторических данных, а не из результатов экспериментов.

В последние годы под термином «социальная сеть» понимаются интернет-сервисы, которые позволяют пользователям переносить в сеть свои социальные связи, однако само понятие социальной сети было предложено задолго до создания персональных компьютеров. Принятое учеными определение гласит, что социальная сеть – это структура (математически – социальный граф), состоящая из группы узлов, которыми являются люди или организации, а также связей между узлами. Связи могут выражать те или иные отношения: например, родства, знакомства или совместной работы ***(Социальные сети сделали людей умнее // InternetUA (http://internetua.com/socialnie-seti-sdelali-luadei-umnee). – 2013. – 14.11).***

***

За допомогою соціальних медіа користувачі збирають інформацію про потенційного партнера та запрошують на побачення. Традиційно більшу увагу віртуальним знайомствам приділяє молодь.

Сьогоднішню роль Facebook, Twitter чи Instagram у романтичних стосунках американців досліджує компанія Pew Research Center.

Так, виявлено, що 30 % американців віком від 18 років використовують соціальні медіа для збору інформації про особу, з якою воліли би мати романтичні стосунки. Серед молоді (18–29 років) цей показник вище і становить 41 %.

12 % дорослого населення США заводять віртуальну дружбу чи відслідковують тих, хто був рекомендований їм знайомими як потенційна пара.

15 % використовують соціальні медіа, щоб запросити візаві на побачення. Частіше цією опцією користуються чоловіки, ніж жінки – 19 проти 11 %.

Соціальні мережі також стають місцем звітів успішних побачень, наприклад фотографій чи окремих інтимних подробиць. Серед користувачів від 18 і старше таких – 17 %. А у віковій групі 18–29 – це кожен третій, тобто 31 %.

В опитуванні, проведеному в квітні – травні 2013 р., взяло участь 2252 американців віком від 18 років. Інтерв'ю проводилися англійською та іспанською мовами. Цільовою групою для дослідників були самотні люди, які шукають пару або були у стосунках останні 10 років ***(Понад 40 % молоді використовують соцмедіа у надії на стосунки // Телекритика (http://osvita.mediasapiens.ua/material/24885). – 2013. – 14.11).***

Маніпулятивні технології

Социальные сети – отличный источник информации для киберпреступников, желающих войти в круг доверия потенциальной жертвы.

Специалисты компании Websense зафиксировали в сети атаку с применением методов социальной инженерии, нацеленную на то, чтобы популяризовать среди пользователей LinkedIn определенный сайт знакомств. Однако, по мнению экспертов, окончательная цель злоумышленников более опасна.

Мошенники создали поддельную учетную запись LinkedIn, которая в настоящее время имеет более 400 контактов и используется как для просмотра профилей потенциальных жертв, так и для их перенаправления на вышеуказанный сайт.

Для увеличения эффективности используется премиум-аккаунт LinkedIn – это позволяет выполнять поиск по рабочим функциям, размеру компании и уровню старшинства. Вся эта информация в дальнейшем используется для проведения атаки.

«Стоит отметить, что возможности премиум-аккаунта позволяют мошеннику просматривать, кто посещал его страницу в социальной сети. Злоумышленник также может связаться с любым участником LinkedIn и выполнять более эффективный поиск жертв», – говорят исследователи.

В Websense полагают, что мошенники используют сайт знакомств в качестве приманки. Специалисты отметили, что сайт в настоящее время не содержит вредоносного кода, но его IP-адрес, как и весь ASN, ранее был привязан к доменам, которые содержали списки ссылок на C&C серверы для нескольких наборов эксплоитов.

Судя по всему, в настоящее время мошенники проводят лишь «разведку» перед более крупной атакой. Так или иначе, исследователи уведомили администрацию LinkedIn об учетной записи злоумышленников ***(Мошенники используют поддельные профили LinkedIn для подготовки к целенаправленным атакам // InternetUA (http://internetua.com/moshenniki-ispolzuuat-poddelnie-profili-LinkedIn-dlya-podgotovki-k-celenapravlennim-atakam). – 2013. – 6.11).***

***

Пользователи Twitter обвинили британский таблоид Daily Express в национализме из-за рекламного твита с призывом подписать петицию за ужесточение миграционного законодательства ЕС. Сообщение об этом появилось в блоге Edinburgh Eye.

Большинство пользователей посчитали такую рекламу возмутительной. Газету обвинили в расизме, ксенофобии и национализме. «Вы говорите в точности, как нацисты. Вы – нацисты? Нацисты использовали мигрантов в качестве козлов отпущения», – написал в комментарии под твитом один из пользователей соцсети.

«Продвигаемый твит» (promoted tweet), содержащий ссылку на петицию Daily Express, появился в социальной сети 2 ноября. Позже его текст был продублирован и в официальном аккаунте издания (@Daily_Express).

«Скажите “НЕТ” неограниченной миграции. Скажите “НЕТ” новому наплыву мигрантов из Восточной Европы. Подпишите нашу петицию и ОСТАНОВИТЕ это», – говорилось в тексте сообщения, после чего читателям предлагалось пройти на страницу с обращением к премьер-министру Великобритании, призывающим его отказаться от поддержки планов Европейского Союза снять миграционные ограничения для жителей Румынии и Болгарии.

Так называемые «продвигаемые твиты» относятся к одному из видов рекламного размещения на сервисе микроблогов Twitter. Рекламные сообщения чаще всего отображаются в верхней части новостной ленты. Пользователи соцсети видят такие твиты, даже если они не подписаны на аккаунт соответствующей компании ***(Британский таблоид обвинили в национализме из-за рекламного твита // InternetUA (http://internetua.com/britanskii-tabloid-obvinili-v-nacionalizme-iz-za-reklamnogo-tvita). – 2013. – 5.11).***

***

Представители службы информационной безопасности создали в соцсетях поддельный аккаунт привлекательной девушки, познакомились с сотрудниками одного из правительственных агентств и получили через них доступ к секретным документам.

Эксперимент был проведен еще до разоблачений Э. Сноудена, но результаты его озвучены только сейчас на одной из конференций по современным компьютерным технологиям. Его провели спецслужбы США при помощи профессиональных программистов компании World Wide Technology, сообщает в своей статье The Daily Mail.

Они создали поддельные аккаунты в соцсетях Facebook и LinkedIn. В качестве профильной фотографии «белые хакеры» использовали снимки молодой привлекательной девушки. Именно это и помогло им втереться в доверие к сотрудникам правительственного агентства мужского пола. После непродолжительного общения «девушке» удалось выудить у мужчины секретную информацию.

Название агентства не раскрывается, известно лишь, что оно специализировалось на кибербезопасности и защите национальных тайн. Сотрудники организации были так увлечены новой знакомой, что не заметили явных несоответствий в ее анкете. Например, там было указано, что она обладает 10-летним опытом в IT-коммуникациях, при этом ей было всего 28 лет.

В качестве модели для создания ложных аккаунтов использовалась реальная девушка по имени Э. Уильямс. Она работала официанткой в кафе неподалеку от офиса правительственного агентства. При этом никто из сотрудников организации ее не узнал.

Интересно, что в течение первых 15 часов после регистрации в соцсетях у нее уже было 60 друзей на Facebook и 55 на LinkedIn. Все они были сотрудниками секретного агентства, в котором предполагалось произвести экспериментальный взлом. В течение трех дней ей поступило три предложения по работе из разных компаний.

Исследователи также рассказали, что подобный эксперимент проводился и с мужчиной в главной роли. Но он не дал таких потрясающих результатов ***(Хакеры, прикинувшись миловидной девушкой, получили доступ к данным спецслужб США // InternetUA (http://internetua.com/hakeri--prikinuvshis-milovidnoi-devushkoi--polucsili-dostup-k-dannim-specslujb-ssha). – 2013. – 5.11).***

***

У рейтингу українських Facebook-користувачів днями відбувся різкий стрибок кількості фоловерів у А. Яценюка та Ю. Луценка. Ще тиждень тому обидва політики мали по 13 тис. фоловерів, а сьогодні в А. Яценюка – 21 тис., а в Ю. Луценка – 22 тис.

Зрозуміло, що органічно отримати 8–9 тис. фоловерів за кілька днів – завдання нереалістичне. Отже, це боти. Єдине запитання: звідки вони взялись.

Ми проаналізували інформацію щодо Ю. Луценка та А. Яценюка та з'ясували, що обох політиків фоловили ті ж боти, за допомогою яких накручували кількість фоловерів у В. Медведчука, його дружини О. Марченко та близької до В. Медведчука журналістки О. Маркосян. Ну і ще кількох тайців та індонезійців.

Більшість ботів мають приблизно однаковий список тих, кого вони фоловлять. Схоже, люди, які наганяють ботів для В. Медведчука у Facebook, після того як погоріли кілька разів на не дуже якісній роботі, вирішили днями підставити і його політичних конкурентів. Мовляв, а чим вони кращі – у них теж боти.

З нетерпінням чекаємо в найближчі дні на деяких новинарних сайтах феєричні розкриття про те, як Ю. Луценко з А. Яценюком нібито купують ботів для своїх акаунтів у соцмережах ***(Про інтернет-PR в стилі чоловіка відомої української телеведучої // UkrainianWatcher (http://watcher.com.ua/2013/11/06/pro-internet-pr-v-styli-cholovika-vidomoyi-ukrayinskoyi-televeduchoyi/). – 2013. – 6.11).***

***

В соцсети активизировался пользователь, который зарегистрировался под именем обвиняемого в днепропетровских терактах В. Сукачева и стал добавлять в друзья журналистов, общественников и нардепов. Однако кто стоит за фотографией В. Сукачева на фоне Эльбруса – пока загадка, ведь сам он сейчас находится в СИЗО. Поскольку адвокат подсудимого ответ на этот вопрос не дал, а супруга не общается с прессой, «Комсомолка» обратилась за комментарием к эксперту.

На стене странички В. Сукачева пока лишь размещены гиперссылки на новости, где цитируются его заявления о давлении сотрудников СБУ, о непризнании вины в терактах и о голодовке в защиту Д. Ревы и Л. Просвирнина.

А также есть запись, что он женат, и о том, какие фильмы, телепередачи и музыку любит. Из изображений – только фото-аватар 2009 г., где он сидит с картой в руках, а на обложке – Эльбрус (подсудимый раньше увлекался альпинизмом).

Судя по этим подробностям, страничку, скорее всего, создал человек, хорошо знавший В. Сукачева, который решил поддержать его таким вот современным образом. Возможно, это жена последовала примеру Л. Ревы, супруги обвиняемого в пособничестве террористам Д. Ревы, а возможно друзья или «фанаты» политолога, к которым можно отнести его бывших студентов. А возможно, некто решил нажиться на популярности обвиняемого, создав фейковый профиль.

«Такие странички создаются, чтобы заработать легкие деньги, – пояснил корреспонденту “Комсомольской правды” в Украине” специалист из компании по продвижению и раскрутки сайтов А. Письменный. – Весьма распространенная схема, когда в соцсетях специально создаются “привлекательные” странички, от имени людей/компаний/событий, на которые могут подписаться (добавиться в друзья) много наивных пользователей. Названный “террористом № 1” В. Сукачев тоже достаточно весомая фигура, и вполне вероятно, что кто-то решил заработать на любопытных пользователях соцсети. А потом просто-напросто этот аккаунт перепродадут каким-либо коммерческим организациям, которые будут на нем постить свою рекламу всем подряд “друзьям” В. Сукачева. Либо же сами создатели странички, набрав большое количество подписчиков, начинают размещать на стене рекламные ссылки» ***(«Днепропетровский террорист» В. Сукачев вышел в сеть, чтобы заработать на любопытных пользователях? // «Комсомольская правда» в Украине (http://kp.ua/daily/111113/423177/). – 2013. – 11.11).***

***

Мошенники под именем актера К. Хабенского в сервисе микроблогов Twitter распространили информацию о сборе средств на благотворительность с

реквизитами, не имеющими отношения к благотворительному фонду К. Хабенского.

Российский актер является основателем благотворительного фонда для детей, больных раком, сообщают «Вести» со ссылкой на РИА «Новости».

Сам К. Хабенский подтвердил, что в настоящее время представители его фонда занимаются разрешением сложившейся ситуации. «Этим уже занимаются люди, которые лучше меня понимают, что нужно делать в таких случаях», – добавил актер.

Друзья артиста распространили в социальных сетях информацию о том, что аккаунт @k_habenski – фальшивый и указанные там номера счетов благотворительного фонда – поддельные.

В настоящее время аккаунта @k_habenski в Twitter не существует ***(Прикрываясь именем К. Хабенского, мошенники устроили беспредел в Twitter // From-UA (http://www.from-ua.com/news/796700913c339.html). – 2013. – 15.11).***

***

Фотографии наркокартелей появились на Facebook, причем как на их официальных страницах, так и в личных профилях ее членов…

Судя по фотографиям оружия, наркотиков, денег и странным автопортретам, у этих парней (и девиц) довольно оживленная и разнообразная жизнь. Куда катится мир, если даже наркодилеры могут выставлять себя напоказ? Эти фото регулярно удаляются администрацией сети Facebook, но они вновь и вновь появляются на других аккаунтах.

Как полагают аналитики, наркокартели начали использовать социальные сети, чтобы создать себе более положительный образ. Они «рекламируют» свою деятельность, проводят мероприятия по связям с общественностью и практически стали для самих себя собственной медиа-компанией. Аналитики также соглашаются с тем, что фотографии в социальных сетях помогают картелям привлекать новые силы извне. При этом они стараются показать свою светлую сторону, пытаясь заявить миру, что они не такие уж плохие, как заявляют власти.

Видео, на котором члены одной из картелей привозят еду, воду и другую гуманитарную помощь мексиканцам, пострадавшим от урагана Ингрид, собрало 500 тыс. просмотров. Августовская речь лидера картеля «Рыцари Тамплиеры» по кличке Ла Тута собрала миллион просмотров на YouTube. Для сравнения, видео с речью президента Мексики Э. Пенья Ньето собрало менее 16 тыс. просмотров. Ну и кто тут национальный герой?

Уже «забаненная» страница на Facebook, принадлежавшая К. Меплариосу, собрала 10 тыс. лайков, прежде чем ее закрыли. Вместо нее позже появился профиль некого Броли – миловидного члена картеля с ненасытным аппетитом к автопортретам. Броли любит позировать с оружием и пачками наличных. Он даже не чужд дакфейсам.

Помимо прочих картели используют архивные фотографии, которые демонстрируют их жизнь как более «драматичную». В итоге, в архивах оказались фотографии оружия, людей в масках, снайперов с винтовками и других членов наркомафии. Фотографии натренированных бойцов картеля используются для устрашения.

Многие аналитики утверждают, что, несмотря на всю эту «популярность», она же и погубит мафиози. В одно мгновение технологии, которые до этого помогали картелям заявить о себе миру, могут превратиться в их уязвимое место. И в первую очередь это произойдет в Мексике, если правительство найдет новый способ и законы, чтобы противостоять наркокартелям в киберпространстве. Ну, а пока образ жизни мексиканских наркокартелей выставлен напоказ для всех желающих ***(Жизнь мексиканской наркомафии на Facebook // From-UA (http://www.from-ua.com/crime/97de916baa39b.html). – 2013. – 13.11).***

Зарубіжні спецслужби і технології «соціального контролю»

Э. Сноуден и его разоблачение программы PRISM наделали немало шума. Большинство высокопоставленных лиц не замедлили высказать своё возмущение по поводу слежки за пользователями, а некоторые стали считать Э. Сноудена настоящим героем. В свою очередь, крупнейшие технологические корпорации забыли о конкуренции и объединились перед лицом «потенциального противника». Теперь же данная история получила продолжение.

Напомним, что группа компаний, в число которых вошли Apple, Facebook, Google, Microsoft, Yahoo и AOL, планировала написать письмо Б. Обаме с просьбой разъяснить ситуацию и чётко очертить полномочия спецслужб, в частности АНБ.

И вот, данное письмо наконец составлено и отправлено, однако адресовано оно не президенту, а Юридическому комитету сената США. В нём компании не придумали ничего лучше, как потребовать обеспечить условия для «существенного улучшения в области защиты частной информации и создания соответствующего механизма для контроля программ слежения».

Также в письме было отмечено, что «недавние разоблачения шпионской деятельности вызвали серьёзное беспокойство как внутри США, так и за их пределами. Объёмы и важность озвученной за последние месяцы информации вызвали серьёзное замешательство как внутри страны, так и по всему миру, из-за чего стало ещё трудней составить необходимые рекомендации по улучшению ситуации».

Подготовив таким образом оправдание своим нерешительным действиям (стоит только вспомнить, что с момента оглашения инициативы до непосредственной отправки письма прошло чуть менее полугода), IT-компании весьма скромно отмечают, что, «позволив компаниям публиковать

информацию о количестве и сути запросов со стороны разведки, можно существенно повысить уровень понимания граждан того факта, что органы государственной власти вынуждают технологические компании раскрывать пользовательскую информацию».

При этом IT-гиганты утверждают следующее: «Наши компании дают понять, что мы отвечаем только на надлежаще заявленные требования о раскрытии личной информации пользователей».

Судя по отрывкам письма, попавшим в СМИ, технологические гиганты, вместо ожидавшейся от них борьбы за неприкосновенность личной информации пользователей и требований прекращения незаконной слежки, пытаются выставить себя в качестве жертв, у которых мало того, что крадут информацию, так ещё и принуждают «сливать» данные. Таким образом, можно предположить, что крупнейшие технологические компании находятся где-то между молотом и наковальней. С одной стороны, пойти на прямую конфронтацию с американской разведывательной системой они не могут, а с другой – потеря доверия клиентов может обойтись им в 21,5–35 млрд дол. в течение трёх ближайших лет ***(Apple, Facebook и Google против слежки // InternetUA (http://internetua.com/Apple--Facebook-i-Google-protiv-slejki). – 2013. – 5.11).***

***

Кибернетическое командование США (United States Cyber Command, USCYBERCOM) может быть выведено из подчинения Агентства национальной безопасности (АНБ). Об этом со ссылкой на анонимные источники внутри спецслужбы 4 ноября сообщило издание The Hill.

Предполагается, что после ухода со своего поста действующего руководителя АНБ К. Александера, посты главы Агентства национальной безопасности и командующего USCYBERCOM будут разведены. При этом, по данным The Hill, формального решения относительно урезания полномочий АНБ еще не принято.

Тем не менее, информацию о возможном выведении кибернетического подразделения в отдельную структуру косвенно подтвердил председатель сенатского Комитета США по вооружённым силам К. Левайн. По словам К. Левайна, вопрос о разделении постов в настоящее время действительно рассматривается в сенате.

Сам К. Александер ранее заявил, что выступает против подобного разделения. «Я верю, что посты должны оставаться совмещенными. Если попытаться разделить нас, то мы получим две команды, работающие отдельно. Наша страна не может позволить себе этого. Особенно в сложившейся сегодня финансовой ситуации», – подчеркнул глава АНБ.

Слухи о реформе Агентства национальной безопасности появились на фоне продолжающейся в американском обществе дискуссии относительно законности многих программ, разработанных ведомством. После публикации летом 2013 г. рядом СМИ секретных документов, касающихся масштабной

слежки АНБ за пользователями сети, проверкой работы спецслужбы по просьбе президента Б. Обамы занялась специальная комиссия. Документы, переданные прессе бывшим сотрудником АНБ Э. Сноуденом, вызвали большой резонанс. В незаконном перехвате интернет-коммуникаций АНБ обвинили такие компании, как Google и Yahoo!, а также власти Германии, Италии, Бразилии и некоторых других стран.

Кибернетическое командование США было создано в июне 2009 г. Как говорится на официальном сайте командования, основными задачами подразделения являются проведение операций, направленных на обеспечение свободы действий США и их союзников в киберпространстве, а также ограничение этой свободы для стран-противников ***(СМИ узнали о планах лишить АНБ права вести кибервойны // InternetUA (http://internetua.com/smi-uznali-o-planah-lishit-anb-prava-vesti-kibervoini). – 2013. – 5.11).***

***

Таджикские интернет-провайдеры заблокировали доступ к видеохостингу YouTube. Об этом 6 ноября сообщила Русская служба «Би-Би-Си». Также ограничен доступ к новостному порталу «Озодагон».

Блокировка интернет-сайтов по времени совпала с проведением в стране выборов президента. Тем не менее, как пишет «Би-Би-Си», изначально представители интернет-компаний объяснили блокировку техническим сбоем, заявив, что не получали от властей указаний ограничить подключение к каким-либо ресурсам в сети.

Однако позже в Интернете появилась информация, свидетельствующая об обратном. По данным сайта news.tj, один из интернет-провайдеров на условиях анонимности сообщил, что действительно получил от Службы связи при правительстве Таджикистана распоряжение о блокировке портала «Озодагон» и видеохостинга YouTube.

Блокировка популярных сайтов в Таджикистане происходит не впервые. В мае 2013 г. Служба связи Таджикистана уже предписывала провайдерам заблокировать YouTube. В качестве возможной причины блокировки тогда называлось размещение на YouTube видео из передачи оппозиционного телеканала К+, посвященной свадьбе старшего сына президента Р. Эмомали. В разное время таджикских пользователей также лишали доступа к таким сайтам, как Facebook, Twitter и «ВКонтакте» ***(В Таджикистане заблокировали YouTube в день президентских выборов // InternetUA (http://internetua.com/v-tadjikistane-zablokirovali-YouTube-v-den-prezidentskih-viborov). – 2013. – 6.11).***

***

Нарушители закона общаются в соцсетях и не боятся называть свое местонахождение.

С появлением функции онлайн-розыска на официальном сайте МВД харьковчане ищут преступников, скрывающихся от правоохранителей, в соцсетях. Причем делают это довольно успешно: по словам «Шерлоков»,

каждый пятый беглец активничает в сети, выкладывая свежие фото, и нисколько не боится называть свое имя и местонахождение. «Сегодня» проверила, действительно ли можно помочь милиции, сидя за компьютером.

Из сотни подозреваемых нам удалось разыскать шестерых, правда, страницы троих оказались «заморожены за подозрительную активность». Еще в 2009 г. за «сводничество для разврата с привлечением несовершеннолетнего» милиционеры подозревали Екатерину Х., однако девушка скрылась от правосудия в другой области. Несмотря на то, что санкция статьи предусматривает до семи лет тюрьмы, Катя не пытается сохранить инкогнито: в соцсетях у нее более 800 друзей, и девушка не скрывает, что вышла замуж и занимается визажем. Впрочем, в Червонозаводском райотделе информации о ее местонахождении ничуть не удивились.

«Есть определенный закон, и мы не можем ее задержать, пока она находится в другой области. Конечно, местные правоохранители могут привести ее в райотдел и сообщить об этом нам, после чего отпустят. Я уже неоднократно писал рапорт с просьбой отправить меня в командировку. Но ехать из-за одного человека и тратить государственные деньги посчитали нецелесообразным», – рассказал нам сотрудник Червонозаводского райотдела Артем.

Оказалось, сложнее всего идентифицировать подозреваемых по черно-белому фото 10-, а то и 20-летней давности, ведь за это время человек мог очень измениться. Однако если всматриваться в черты лица, шанс распознать скрывающихся особовелик. Так, нам удалось разыскать 51-летнюю Татьяну К., которую более 10 лет назад подозревали в присвоении чужого имущества. Женщина, которой может грозить до восьми лет тюрьмы, переехала из Харьковской области и время от времени выкладывает семейные фото в соцсетях.

Но если Татьяну мы вычислили только по имени и внешнему сходству со снимком 10-летней давности, у 31-летнего Сергея Ш., уже восемь лет подозреваемого в хулиганстве с применением оружия, полное совпадение по дате рождения и фотографии. Мужчина фотографируется возле харьковских достопримечательностей с сыном и ищет в сети вторую половинку. Однако друзья Сергея, все как один, уверяют: мол, произошла какая-то ошибка, их приятель никому не причинял вреда и обязательно обратится в милицию, чтобы его вычеркнули из онлайн-розыска.

Информация харьковчан не часто помогает раскрыть преступления. «Когда в киевском супермаркете застрелили охранников, нам звонили по несколько человек в день. Зачастую звонят не ради вознаграждения, а просто чтобы поговорить. Но мы обязаны проверить любую информацию: принимаем заявление, направляем на место наряд милиции. Но, к сожалению, 99,9 % таких звонков – пустая информация», – рассказал «Сегодня» старший инспектор дежурной части облУВД А. Юшин. А вот вознаграждение за информацию о подозреваемом полагается лишь в том случае, если преступник оказался крупным аферистом или убийцей. В остальных случаях денежную

благодарность может выставить потерпевшая сторона, заинтересованная в поимке злоумышленников. Так что требовать деньги за свои старания можно лишь в том случае, если информация о сумме будет указана на сайте МВД ***(Доронина М. «Сегодня» разыскала преступников, которые скрываются от правосудия уже 10 лет // Сегодня (http://www.segodnya.ua/regions/kharkov/segodnya-razyskala-prestupnikov-kotorye-skryvayutsya-ot-pravosudiya-uzhe-10-let--473122.html). – 2013. – 6.11).***

***

Полиция скоро может взять на вооружение новые технологии, которые помогут им находить педофилов. Ученые из Амстердама создали компьютерного ребенка по имени Сладкая (Sweetie), который уже на практике доказал, что способен помочь правоохранительным органам в этом деле. Благодаря ему полиция получила координаты десятков тысяч любителей детского тела.

Создателем виртуальной 10-летней девочки из Филиппин является нидерландская детская благотворительная организация «Терре де Хоммс». Ее сотрудники активировали детский поддельный профиль в социальных сетях, и в течение 10 недель с виртуальным ребенком мог пообщаться каждый. Более того, желающие могли посмотреть, как она позирует в сеансе видеочата. Текстовую переписку вел сам ученый и его помощники.

Всего за время эксперимента с ней связалось свыше 20 тыс. мужчин со всей планеты и около тысячи предлагали компьютерной модели деньги за то, что она снимет одежду. Среди последних были 254 американца, 110 мужчин из Великобритании и 103 – из Индии. Всего же деньги в обмен на раздевание 3D-модели предлагали жители 71 страны. Исследователи передали данные об этих людях, включая их профили в социальных сетях и учетные записи Skype местной полиции.

Куратор проекта Г. Гюйт сказал на конференции, что преступления нуждаются в новых способах расследования. «Если хищник не будет первым делать ход, жертва не будет делать ход вперед. Мы просто назвались 10-летней филиппинской девочкой, – говорит он. – Мы не просили и не приставали до тех пор, пока нам этого не предлагали».

Результаты такого способа «отлова» любителей детского тела оказались настолько успешными, что «Терре де Хоммс» запустил глобальную кампанию, чтобы остановить «секс-туризм» по веб-камере. Он и его коллеги также передали все созданные ими технологии в руки полиции ***(Компьютерный ребенок поймал десятки тысяч охотников за детским телом // InternetUA (http://internetua.com/kompuaternii-rebenok-poimal-desyatki-tisyacs-ohotnikov-za-detskim-telom). – 2013. – 7.11).***

***

Коммуникации между органами государственной власти Бразилии с марта следующего года будут осуществляться исключительно внутри

собственных сетей, следует из подписанного президентом страны Д. Руссефф декрета, опубликованного в официальном вестнике Diario Oficial.

Как следует из декрета, «вся передача данных должна осуществляться по телекоммуникационным сетям и информационным службам организаций и ведомств Федеральной государственной службы». Решение было принято «в целях обеспечения защиты национальной безопасности», передает Digit.ru.

Согласно декрету, в течение четырех месяцев все органы госслужбы должны перейти на электронную почту, разрабатываемую Федеральной службой обработки данных (Serpro). В настоящее время в бразильских государственных ведомствах используется электронная почта, разработанная американской компанией Microsoft.

Напомним, ранее из материалов бывшего сотрудника американских спецслужб Э. Сноудена стало известно, что США совместно с Канадой вели перехват телефонных переговоров и электронной переписки бразильских чиновников с помощью специальной программы Olympia. Кроме того, из документов Э. Сноудена стало известно, что США якобы вели и промышленный шпионаж за бразильским нефтяным гигантом Petrobras, а также перехватывали электронную переписку и телефонные переговоры президента Бразилии ***(В Бразилии решили защититься от шпионажа со стороны США, отказавшись от почты Microsoft // InternetUA (http://internetua.com/v-brazilii-reshili-zasxititsya-ot-shpionaja-so-storoni-ssha--otkazavshis-ot-pocsti-Microsoft). – 2013. – 7.11).***

***

У Кемерово (Росія) журналіста і блогера С. Калініченка 6 листопада затримали за перепублікацію інформації в Інтернеті. Про це повідомив його колега Д. Шипілов на своїй сторінці в мережі Facebook.

С. Калініченко був «поміщений в ізолятор тимчасового утримання».

Д. Шипілов повідомляє, що «11 липня в квартирі, яку знімає С. Калініченко, був проведений обшук у рамках кримінальної справи за 280-ю статтею КК РФ – С. Калініченка перевіряли на причетність до поширення в Інтернеті інформації екстремістського змісту».

С. Калініченко перепублікував (ретвітнув) запис (твіт), зроблений користувачем @letokot 6 травня 2013 р., – на фотографії, знятій на Патріарших прудах якимось Д. Макналті, зображений принт листівки «Кинь ходити на мітинги і починай діяти!» авторства Першого загону опору. Це повідомлення ретвітнули 90 блогерів.

«Тобто це перший в сучасній Росії епізод кримінального переслідування за ретвіт, – пояснює Д. Шипілов. – За чотири місяці, що минули з дня обшуку, процесуальний статус С. Калініченка так і не змінився – він як був у цій справі свідком, так ним і залишався. Я розмовляв з ним декілька днів тому – і про які б то не було наміри з боку слідства, від спілкування з ним не дізнався».

При цьому журналіст уточнює, що листівка «Кинь ходити на мітинги і починай діяти!», у поширенні якої влада звинувачує С. Калініченка, досі не

числиться у Федеральному списку екстремістських матеріалів, що створюється Мін'юстом ***(У Росії блогера посадили в СІЗО за перепублікацію інформації в Інтернеті // Інститут масової інформації (http://imi.org.ua/news/42080-u-rosiji-blogera-posadili-v-sizo-za-perepublikatsiyu-informatsiji-v-interneti.html). – 2013. – 7.11).***

***

Власти Бельгии 6 ноября заявили, что начали расследование по факту происхождения шпионского программного обеспечения на компьютере премьер-министра страны Э. Ди Рупо. Установленный вредонос был кастомизированным и занимался слежкой за деятельностью премьер-министра.

Федеральная прокуратура Бельгии заявила, что она также расследует недавнюю атаку на правительственные сети, которая не связана с заражением компьютера премьер-министра. Также в прокуратуре сообщили, что указанное программное обеспечение собирало широкий спектр данных и передавало их на подставной сервер, а с него данные передавались конечным получателям.

В. Рогген, пресс-секретарь прокуратуры Бельгии, говорит, что сейчас следствие выясняет происхождение программы-вредоноса и пока не готово давать дальнейших комментариев.

Напомним, что в последнее время ряд европейских стран обвиняли США в шпионской деятельности в их адрес. В Бельгии пока ничего не говорят о подозрениях в адрес США. Впрочем, в ряде последних интервью Э. Ди Рупо также выражал недовольство программами США в Европе. Кроме того, на днях он был инициатором проекта, который обязывает местных федеральных чиновников и министров не приносить с собой на работу мобильные телефоны и не использовать рабочие компьютеры в личных целях ***(Бельгия расследует кибератаку на компьютер премьер-министра // InternetUA (http://internetua.com/belgiya-rassleduet-kiberataku-na-kompuater-premer-ministra). – 2013. – 6.11).***

***

Группа адвокатов и журналистов Нидерландов подала в суд на правительство государства, чтобы предотвратить использование голландскими спецслужбами телефонных данных, которые им предоставило Агентство национальной безопасности США.

Пятеро людей, среди которых известный хакер, и четыре организации подали исковое заявление в суд Гааги, согласно заявлению их адвоката К. Альбердинга Тима. Жалоба была подана после того, как обнаружилось, что АНБ отслеживало 1,8 млн телефонных звонков в месяц и передавало часть данных о звонках разведагентствам Нидерландов.

Министр внутренних дел Р. Пластерк, чье министерство выступает в суде ответчиком, подтвердил, что АНБ перехватывала данные телефонных звонков, сообщив национальному телевидению, что подобные действия являются недопустимыми как по отношению к политикам, так и по отношению к

обычному населению. Он сказал, что датские спецслужбы обменивались информацией с АНБ, но не знали, откуда поступала сама информация.

Среди истцов – журналист-детектив Б. де Винтер и хакер Р. Гонгрип. Последний известен тем, что против него в США ведется расследование из-за его связей с WikiLeaks.

Истцы считают, что правительство Нидерландов поступало противозаконно, получая данные от иностранных разведслужб, которые были собраны через программы слежения и шпионажа наподобие PRISM, нарушая тем самым закон.

Судебные слушания назначены на 27 ноября текущего года ***(На правительство Нидерландов подали в суд из-за шпионажа АНБ // InternetUA (http://internetua.com/na-pravitelstvo-niderlandov-podali-v-sud-iz-za-shpionaja-anb). – 2013. – 7.11).***

***

Вашингтону не удалось убедить правительство КНР прекратить экономический кибершпионаж против США. Китай продолжает предпринимать активные усилия по проникновению в информационные системы американских промышленных и финансовых компаний с целью хищения их коммерческих секретов.

Такие выводы содержатся в ежегодном докладе Комиссии по вопросам экономики и безопасности в отношениях между США и Китаем, сообщает ИТАР-ТАСС. Это происходит, несмотря на разоблачения подобной деятельности. Между тем официальный представитель Посольства Китая в Вашингтоне Г. Шуан отверг предположения, высказанные в новом докладе американской комиссии.

Правительство КНР ранее согласилось обсудить эту проблему с американской администрацией. Вашингтон и Пекин создали рабочую группу по этим вопросам и уже провели несколько раундов консультаций ***(КНР продолжает экономический кибершпионаж против США // InternetUA (http://internetua.com/knr-prodoljaet-ekonomicseskii-kibershpionaj-protiv-ssha). – 2013. – 7.11).***

***

Администрация фотосервиса Instagram начала блокировку хэштегов, использующихся для распространения в соцсети информации о наркотиках. Об этом 7 ноября сообщил сайт «Би-Би-Си».

Хэштеги, которыми помечаются фотографии и комментарии, содержащие сведения о продаже наркотиков, будут удаляться из поиска по сервису. Тем не менее, как заявили в Instagram, политика соцсети в отношении модерации размещенного контента не позволяет провести масштабный анализ фотографий и видеороликов и заблокировать их без жалобы со стороны пользователей. «Мы призываем всех, кто обнаружит изображения, видео или комментарии, касающиеся запрещенных веществ, сообщать об этом нам, помечая такой

контент с помощью специальной кнопки. В этом случае мы сможем удалить посты», – заявил представитель Instagram.

Как сообщает «Би-Би-Си», в ближайшие 48 часов подробный поиск запрещенной информации, пропагандирующей употребление наркотиков, также проведет социальная сеть Facebook, владеющая фотосервисом Instagram.

О том, что пользователи фотосервиса активно распространяют информацию о наркотических веществах, стало известно благодаря проведенному «Би-Би-Си» расследованию. Как удалось выяснить журналистам, несмотря на то, что непосредственно в Instagram невозможно продать или купить что-либо в принципе, сеть активно используется для продвижения сайтов, распространяющих наркотики. Чаще всего это делается с помощью комментариев, публикуемых под фотографиями с марихуаной и другими запрещенными веществами. В текстах таких комментариев указывается ссылка на сайт, а также описываются условия заказа. Сам комментарий обычно сопровождается хэштегами, позволяющими проще найти нужную фотографию в поиске по соцсети (#weedstache, #nodsquad, #junkiesofIG, #dankforsale, #pillsforsale и др.).

Социальные сети используются злоумышленниками для размещения рекламы наркотиков довольно часто. Так, в середине сентября пользователи Facebook из России обратили внимание на появление в соцсети рекламы запрещенных курительных смесей. Баннер содержал в себе логотип продающего смеси магазина и контактный телефон для заказа. Проверку в отношении Facebook тогда обещала провести Федеральная антимонопольная служба. Позже представители соцсети объяснили появление рекламы техническим сбоем ***(Instagram заблокирует хэштеги в постах с рекламой наркотиков // InternetUA (http://internetua.com/Instagram-zablokiruet-heshtegi-v-postah-s-reklamoi-narkotikov). – 2013. – 9.11).***

***

Британская спецслужба «Центр правительственной связи» (GCHO) внедрилась в деловую социальную сеть LinkedIn. Об этом пишет Deutsche Welle со ссылкой на Spiegel Online, сообщает «Компаньон груп» (http://www.companion.ua/articles/content?id=262736).

С помощью фальшивых профилей LinkedIn сотрудники GCHQ получали доступ к компьютерам, заинтересовавших их фирм.

Среди целей британской спецслужбы оказались, в частности, бельгийская телекоммуникационная компания Belgacom и производитель компьютерных программ Mach. Кроме того, GCHQ совместно с американской спецслужбой АНБ активно шпионила и за штаб-квартирой Организации стран-экспортеров нефти (ОПЕК).

«Мы должны со всей ясностью заявить, что никогда бы не одобрили такие действия, независимо от того какой цели они служат. Нас также никогда не информировали о таких действиях», – прокомментировали в компании LinkedIn информацию Spiegel Online по поводу повышенного интереса

спецслужб к их сети ***(Спецслужбы внедрились в деловую соцсеть LinkedIn // Компаньон Груп (http://www.companion.ua/articles/content?id=262736). – 2013. – 11.11).***

***

За поширення порнографії у мережі Інтернет у Вінницькій області лише за два останні тижні відкрито 15 кримінальних проваджень. Про це повідомляє сектор зв'язків із громадськістю УМВС у Вінницькій області, передає «Укрінформ».

«За два тижні працівники відділу боротьби з кіберзлочинністю обласного УМВС відкрили 15 кримінальних проваджень за розповсюдження порнографії. Більшість правопорушників розмістили в соціальних мережах відеоролики порнографічного змісту, які знаходилися у вільному доступі для користувачів вказаної мережі», – ідеться в повідомленні. Згідно з повідомленням, з початку року до кримінальної відповідальності в області притягується 28 осіб, які розсилали або розміщували порно на своїх сторінках у соцмережах.

Любителів поділитися «полуничкою» в мережі вінницькі міліціонери виловлювали в рамках операції «Павутина», спрямованої на профілактику та виявлення поширення протиправного контенту в мережі Інтернет ***(Вінницька міліція відкрила 15 кримінальних проваджень за порно в соцмережах // Інформаційне агентство «Регіональні Новини» (http://regionews.ua/node/120061). – 2013. – 14.11).***

***

По мнению эксперта О. Романюк, тайные агенты следят за каждым человеком, который ненароком или по причине излишней беспечности, оставляет какие-либо конфиденциальные данные в Интернете, пишет nua.in.ua.

Особенно активно мониторят страницы соцсетей. При этом спецслужбы не обходят своим незримым вниманием даже небольшие площадки для общения, созданные под определенный регион, область или город ***(Украинские спецслужбы следят за пользователями соцсетей // Ирта-fax (http://irtafax.com.ua/news/2013/11/2013-11-15-01.html). – 2013. – 14.11).***

***

Правоохранители хотят собрать отпечатки пальцев детей, прядь их волос и даже пароли в соцсетях в так называемую родительскую карту. Об этом сообщает 5 канал.

Образец родительской карты презентовали в Киеве. Он, по мнению милиционеров, поможет быстро разыскать ребенка в случае такой необходимости.

«Родители работают на престижных должностях. Их дети, не имея общения дома убегают. Мы по трое-четверо суток ищем таких детей в

Луганске, Мелитополе, Одессе», – говорит Н. Микула, начальник управления образования горисполкома.

Заводить родительскую карту ребенку или нет – дело добровольное, уверяют в МВД.

В документе будет фото ребенка, подробное описание цвета глаз, родинок и других особых примет. А еще есть специальные места: где будет прядь волос, для дальнейшего анализа ДНК, и отпечатки пальцев. Предлагают вписаться даже личные пароли в соцсетях, которыми пользуются школьники.

Все данные в документ будут вводить только с согласия родителей. Такая карта, объясняют правоохранители, поможет найти ребенка, если возникнет такая необходимость ***(Милиция хочет контролировать детей с помощью соцсетей // Комментарии (http://comments.ua/life/436131-militsiya-hochet-kontrolirovat-detey.html). – 2013. – 14.11).***

***

Шпионаж АНБ может превратить Интернет в «сеть из осколков»

Представители интернет-поисковика Google выступили с заявлением, в котором предупредили общественность и правительство США о риске превращения открытого Интернета в «сеть из осколков», если АНБ продолжит программы тотальной слежки.

Выступая перед конгрессом крупнейших технологических компаний, представители поисковика заявили, что общественность должна получить больше информации о влиянии правительства на пользовательские данные.

«Нынешнее отсутствие прозрачности государственного наблюдения в демократических странах подрывает свободу и доверие большинства граждан, а также оказывает негативное влияние на экономический рост, безопасность и использование Интернета в качестве платформы для открытого и свободного выражения своих позиций», – заявил глава отдела информационной безопасности и юридической поддержки Google Р. Салгадо.

Напомним, что члены Конгресса выступают за то, чтобы сделать более прозрачными действия властей и предотвратить внедрение новых программ шпионажа со стороны АНБ. По словам сенатора Э. Франкена, входящего в подкомитет по законодательной деятельности, правительство рассматривает возможность более прозрачной деятельности. Так, чиновник отметил, что новый законопроект о прозрачности разведки США обяжет АНБ раскрывать данные о слежке и о том, какое количество американцев находится под наблюдением спецслужбы.

Новый законопроект также позволит телефонным и интернет-компаниям оповещать общественность о предстоящих программах сбора информации, их масштабах и количестве пользователей, чьи данные будут мониториться в соответствие с этими программами. «В сложившейся ситуации большинство пользователей уверены, что американские интернет-компании передают правительствам огромные объемы информации, хотя, на самом деле, они таковыми не обладают», – отметил Э. Франкен ***(Шпионаж АНБ может***

превратить Интернет в «сеть из осколков» // InternetUA (http://internetua.com/shpionaj-anb-mojet-prevratit-internet-v--set-iz-oskolkov). – 2013. – 14.11).

***

Журналисты американского издания ProPublica опубликовали более 500 изображений, подвергшихся цензуре на китайском сервисе микроблогов Sina Weibo. Снабженные пояснениями фотографии размещены на странице специального проекта China's Memory Hole («Черная дыра китайской памяти»).

Фотографии создатели проекта разделили на несколько категорий, в зависимости от причины модерации. Больше всего изображений (около 200 фото) собрано в категории «политических текстов». Далее следуют фотографии, посвященные диссидентам, исключенному из Компартии Китая бывшему лидеру коммунистов г. Чунцин Б. Силаю, а также фотографии с протестных акций.

Коллекция изображений была собрана ProPublica летом 2013 г. Позже в издании была сформирована специальная группа из людей владеющих китайским, которые проанализировали и прокомментировали каждую из подвергшихся цензуре фотографий, объяснив ее содержание и контекст.

По словам авторов проекта, они надеются, что фотографии помогут понять образ мышления людей, которые стоят за политической цензурой в Китае. На сайте также размещено предложение ко всем, кто причастен к цензурированию китайского Интернета, связаться с авторами проекта и рассказать о своем опыте.

Сервис микроблогов Sina Weibo, который часто называют китайским аналогом Twitter, был запущен в 2009 г. На сегодняшний день на сервисе зарегистрировано более 500 млн пользователей. Все сообщения, публикуемые пользователями Sina Weibo, подвергаются модерации.

Популярность Sina Weibo во многом связана с тем, что большинство иностранных социальных сетей заблокированы на территории Китая с середины 2009 г. По решению властей тогда был ограничен доступ к Facebook, Twitter и ряду других интернет-ресурсов. Причиной блокировки стали массовые беспорядки в автономном районе Урумчи, где в ходе столкновений погибли более 200 человек. Официальной причиной беспорядков власти объявили сведения, распространявшиеся в социальных сетях недовольными режимом гражданами ***(СМИ опубликовали запрещенные в китайских соцсетях фотографии // InternetUA (http://internetua.com/smi-opublikovali-zapresxennie-v-kitaiskih-socsetyah-fotografii). – 2013. – 15.11).***

***

Чиновники Агентства национальной безопасности США готовятся к раскрытию Э. Сноуденом еще большего количества секретных документов и намерены не допустить дальнейших утечек. В ходе своего недавнего выступления глава ведомства К. Александер сообщил, что Э. Сноуден похитил

около 200 тыс. документов АНБ. Таким образом, можно предположить, что большая их часть еще не опубликована.

Сотрудники спецслужбы сообщили Национальному общественному радио США (National Public Radio, NPR), что информацию, которой владеет Э. Сноуден, можно распределить по четырем категориям. В первую категорию попадают данные о возможностях АНБ – способы и методы сбора информации о телефонных разговорах пользователей и их переписке через Интернет.

Ко второй категории относятся разведывательные отчеты об угрозах, лидерах иностранных государств и других подобных вопросах, созданные на основе данных, собранных в рамках Соглашения о радиотехнической разведывательной деятельности (Signals Intelligence agreement, SIGINT).

В третью категорию попадают документы о сотрудничестве АНБ с различными организациями и ведомствами, в том числе с частными технологическими компаниями и иностранными спецслужбами.

Информация, раскрытая Э. Сноуденом, до сих пор касалась только возможностей АНБ и его партнерских соглашений. Больше всего чиновники обеспокоены возможным рассекречиванием документов, относящихся к четвертой категории, в которых указана информация, собранная АНБ в рамках SIGINT у других ведомств (Государственного департамента, ФБР, Пентагона и ЦРУ). Раскрытие этой информации покажет пробелы в возможностях АНБ, а значит, откроет слабые места в обороне США.

Что касается пока неопубликованных документов, имеющихся в распоряжении у Э. Сноудена и его сообщников, то в АНБ готовятся к дальнейшему раскрытию не столь критической информации ***(АНБ намерено не допустить дальнейшего раскрытия критической информации Эдвардом Сноуденом // InternetUA (http://internetua.com/anb-namereno-ne-dopustit-dalneishego-raskritiya-kriticseskoi-informacii-edvardom-snoudenom). – 2013. – 17.11).***

Проблема захисту даних. DOS та вірусні атаки

Хакеры используют ранее неизвестную уязвимость в Microsoft Windows и Office, которые позволяет злоумышленникам заражать компьютеры вредоносным программным обеспечением. Используемый эксплойт представляет собой специальным образом сконструированный doc-файл, который распространяется по электронной почте, говорится в сообщении Microsoft Security Responce Center.

Сообщается, что пока атака имеет ограниченный ареал распространения, она ориентирована в первую очередь на получателей в странах Ближнего Востока и Южной Азии. Известно, что рассылаемый файл эксплуатирует баг в графическом интерфейсе продуктов Microsoft, что позволяет атакующим удаленно исполнить злонамеренный код.

При открытии хакерского кода в системе начинается исполнение его содержимого, причем исполняемый код получает те же привилегии в системе, что и пользователь, в сеансе которого происходит исполнение кода. В корпорации говорят, что так как ридеры doc встроены в Windows, то эксплоит подходит и для Windows, и для Office.

В Microsoft только что выпустили временное исправление, которое работает до момента релиза постоянного патча. Временный патч не устраняет причину уязвимости, но он временно блокирует рендеринг графического формата, который провоцирует баг. Кроме того, он блокирует обработку графических файлов TIFF средствами встроенного программного обеспечения.

Уязвимость затрагивает Windows Server 2008, Office 2003–2010 и все версии Microsoft Lync, а также клиентские системы Windows Vista – Windows 7. При этом если у пользователя установлен Office 2010, а сам он работает на базе Windows 7, 8 или 8.1, то баг ему не грозит.

Независимые специалисты по ИТ-безопасности говорят, что выявленный сегодня баг становится еще одним багом, который позволяет обойти встроенные технологии защиты от атак Microsoft DEP и ASLR ***(Хакеры используют новый баг в Windows и Office // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/11/06/bug-in-Windows-Office.html). – 2013. – 6.11).***

***

Новая версия троянской программы, атакующей системы онлайн-банкинга, также содержит код, осуществляющий поиск уязвимых клиентских приложений SAP на компьютере пользователя. При этом в настоящее время код не атакует системы, что указывает только на будущие планы хакеров.

Необычное вредоносное ПО было выявлено пару недель назад. Как сообщили в российской антивирусной компании «Доктор Веб», которая проводила исследования совместно с российским производителем систем ERPScan, осуществляющих выявление уязвимостей в приложениях SAP. «Мы проанализировали вредоносное программное обеспечение и установили, что оно сканирует компьютеры на наличие приложений SAP. Вероятно, это сделано для выявления целей будущих атак», – комментирует А. Поляков, технический директор ERPScan.

По его словам, когда вредонос осуществляет свою деятельность, он сканирует установленный на компьютере софт, пытаясь найти бреши, которые можно в будущем применять для атак на компьютеры. По данным ERPScan, выявленный троянец – первый вредонос, ориентированный специально на приложения SAP, причем созданный не исследователями для концептуальных целей, а реальными киберпреступниками.

Клиентское программное обеспечение SAP работает на десктопах, размещая на них конфигурацию, которую можно довольно легко прочитать и выявить, с какими SAP-серверами они контактируют. В будущем атакующие могут подобным образом выявлять пароли SAP, либо похищать их через

конфигурационные данные. В зависимости от конкретных настроек, хакеры также могут похищать и бизнес-данные или вынуждать компанию проводить несанкционированные платежи.

Обе компании отмечают, что SAP используется многими крупными компаниями, а общая база пользователей превышает 250 тыс. компаний по всему миру, причем 80 % из них – это участники списка Forbes 500 ***(Новый троянский код атакует целевые системы SAP // InternetUA (http://internetua.com/novii-troyanskii-kod-atakuet-celevie-sistemi-SAP). – 2013. – 5.11).***

***

Microsoft публично раскритиковала Google за то, что она сканирует письма пользователей для отображения релевантных объявлений. В компании говорят, что в Outlook.com такого нет, что является хорошей причиной сменить провайдера.

В Microsoft неоднократно критиковали Google за чтение переписки пользователей Gmail и теперь запустили рекламную кампанию, с помощью которой хотят донести этот факт до широких масс и расширить собственную клиентскую базу, сообщает The Telegraph.

На специально созданном для этих целей сайте keepyouremailprivate.com Microsoft привела примеры того, как Google сканирует сообщения для того, чтобы отображать релевантную рекламу, когда пользователь работает с ящиком через веб-сайт. Например, при упоминании в письме домашних животных Google отображает рекламу корма, при упоминании географических названий – рекламу путевок, болезней – медицинских учреждений, развода – адвокатских услуг и т. д.

Google читает каждое письмо, от начала до конца, утверждают в Microsoft. Причем она проделывает то же самое со всей входящей корреспонденцией, независимо от того, было ли отправлено письмо с аккаунта Gmail или любого другого провайдера, то есть и в тех случаях, когда люди не подписываются под правилами использования Gmail.

Объявления Gmail отображаются над списком писем и справа от него. В собственном почтовом сервисе Microsoft Outlook.com реклама тоже отображается, но объявления не сопоставляются с содержимым писем и выводятся случайным образом.

Несмотря на то, что сканирование писем в Outlook.com все равно имеет место – в целях защиты от спама и автоматической сортировки писем по папкам, – в Microsoft убеждены, что это не является нарушением прав пользователей на частную жизнь, тогда как отображение релевантной рекламы в Gmail является примером злостного нарушения этого права. «Google не уважает вашу конфиденциальность, а мы это делаем», – говорят в Microsoft, предлагая пользователям сменить почтового провайдера – не трудно догадаться, на какого.

Проблема чтения писем Google среди некоторых пользователей стоит остро. В сентябре суд в Калифорнии принял к рассмотрению коллективный иск по обвинению в незаконном чтении писем. В самой компании говорят, что таким образом обеспечивается работоспособность сервиса.

В Google считают, что чтение электронной почты – которое, кстати, как утверждают в корпорации, выполняется роботами – необходимо для «правильного функционирования сервиса» и для того, чтобы «предоставлять пользователям бесплатные услуги». В компании приводят в пример защиту от спама и фильтрацию сообщений – другие функции, которые также основаны на анализе содержимого.

В августе в Google заявили, что ни о какой неприкосновенности частной жизни и речи быть не может, если человек пользуется сторонним сервисом, к которым относится в том числе почта Gmail.

В конце прошлого месяца две американские компании объявили о намерении открыть почтовый сервис нового поколения, в котором сообщения будут шифроваться и пересылаться непосредственно между устройствами пользователей, а не через сторонний сервер ***(Microsoft сорвала покровы: «Google читает всю почту пользователей» // InternetUA (http://internetua.com/Microsoft-sorvala-pokrovi---Google-csitaet-vsua-pocstu-polzovatelei). – 2013. – 6.11).***

***

Создатели вируса CryptoLocker, который ограничивает доступ пользователя к его собственным данным и требует деньги за разблокировку, придумали ещё более изощрённый вредонос.

Новая версия CryptoLocker использует устойчивое ко взлому шифрование и блокирует доступ к файлам множества форматов, в том числе к документам, электронным таблицам, изображениям и даже файлам AutoCAD. Таким образом, избавиться от него становится значительно сложнее.

После заражения системы вирус уведомляет владельца зашифрованных данных о том, что у него есть 72 часа чтобы перечислить 300 дол. на счёт мошенников, иначе уникальный ключ шифрования для разблокировки системы будет безвозвратно удалён.

Новый вирус не просто блокирует Windows, но и шифрует большинство файлов. Эксперты, изучившие новую версию вируса, подсказывают, что пользователи, которые выполняют резервное копирование данных, могут очистить свою систему и восстановить утраченную информацию. Если же резервных копий нет, зашифрованные файлы можно считать безвозвратно утерянными ***(Новый вирус-локер блокирует Windows и зашифровывает данные пользователя // InternetUA (http://internetua.com/novii-virus-loker-blokiruet-Windows-i-zashifrovivaet-dannie-polzovatelya). – 2013. – 7.11).***

***

По меньшей мере пять интернет-сайтов, принадлежащих правительству Филиппин, подверглись атаке со стороны хакеров из группировки Anonymous. Об этом 4 ноября сообщила австралийская газета The Sydney Morning Herald.

По данным издания, хакерами также были взломаны несколько сингапурских сайтов. На каждом ресурсе злоумышленники разместили сообщения с призывом выступить против коррупции. «Коррупционеры, бойтесь нас. Правительство Филиппин подвело своих граждан. Настало время напомнить правительству, что справедливость, честность и свобода – больше, чем просто слова», – говорилось в размещенных Anonymous текстах.

При этом сами тексты снабжались ссылками, перенаправлявшими на главную страницу Anonymous Philippines, а также на страницу в Facebook, посвященную антикоррупционному «маршу миллиона масок», который приурочен ко дню Г. Фокса, ежегодно отмечаемому 5 ноября в Великобритании (маска Г. Фокса является одним из символов движения Anonymous).

Атака на филиппинские интернет-сайты проходит на фоне обострившейся внутриполитической обстановки на Филиппинах. Президент страны Б. Акино в настоящее время обвиняется в злоупотреблении служебным положением и растрате средств, выделенных ему юристами одного из общественных фондов. На прошлой неделе Б. Акино выступил на телевидении с официальным опровержением своей причастности к растрате. «Я не вор», – заявил президент в ходе прямого эфира.

Предшественница Б. Акино на посту президента страны, Г. Макапагал-Арройо, была арестована в 2012 г. Ее обвинили в хищении 8 млн дол. США из государственного фонда ***(Anonymous призвали жителей Филиппин выйти на марш против коррупции // InternetUA (http://internetua.com/Anonymous-prizvali-jitelei-filippin-viiti-na-marsh-protiv-korrupcii). – 2013. – 4.11).***

***

Хакеры из индонезийского подразделения международной группировки Anonymous взяли на себя ответственность за взлом 3 ноября более 100 сайтов различных австралийских компаний, сообщает Reuters.

На взломанных сайтах были опубликованы сообщения с требованием прекратить «шпионить за Индонезией». Таким образом хакеры ответили на сообщения, основанные на материалах, предоставленных бывшим сотрудником американских спецслужб Э. Сноуденом, об использовании австралийских посольств для перехвата электронных данных в азиатских странах при сотрудничестве с США и без ведома большинства австралийских дипломатов.

В частности, из документов, опубликованных 31 октября газетой The Sydney Morning Herald, следовало, что для шпионажа используется австралийское посольство в Джакарте. Согласно этим сообщениям, слежка осуществляется в рамках американской программы Stateroom по сбору разведданных усилиями пяти стран: США, Австралии, Канады, Великобритании и Новой Зеландии.

В пятницу, 1 ноября, внешнеполитическое ведомство Индонезии потребовало объяснений в связи с сообщениями в прессе у австралийского посла. С таким же требованием обратились к США и власти Китая ***(Индонезийские хакеры взломали десятки австралийских сайтов // InternetUA (http://internetua.com/indoneziiskie-hakeri-vzlomali-desyatki-avstraliiskih-saitov). – 2013. – 4.11).***

***

94,1 % посещений совершается при помощи автоматических вредоносных инструментов, используемых для поиска и эксплуатации уязвимостей.

Как сообщило издание Net Security, облачный провайдер Incapsula в течение 90 дней исследовал 1 тыс. интернет-ресурсов. В ходе исследования эксперты зафиксировали 1,4 млн случаев посещения сайтов неавторизованными пользователями, в 20,376 тыс. случаях посетители авторизовались.

Примечательно то, что только 2,8 % неавторизованных пользователей являлись живыми людьми. 1,8 % посещений были совершены «доброжелательными» ботами (поисковыми системами, читателями RSS и т. д.). Этот показатель был бы гораздо выше, если бы не общая практика блокирования страницы авторизации с помощью файла robots.txt.

Остальные 94,1 % посещений были совершены при помощи автоматических вредоносных инструментов, которые используются для поиска и эксплуатации уязвимостей, связанных с паролями. Проще говоря, в среднем 15 из 16 посетителей страницы авторизации имеют злой умысел.

Такое большое количество вредоносных посещений оказалось вполне ожидаемым, учитывая недавние волны крупномасштабных брут-форс и других видов атак. Эксперты отметили связь между резким увеличением количества попыток несанкционированного доступа к сайтам и сообщениями об атаках ***(Большинство посещений страниц авторизации совершается при помощи вредоносных инструментов // InternetUA (http://internetua.com/bolshinstvo-posesxenii-stranic-avtorizacii-sovershaetsya-pri-pomosxi-vredonosnih-instrumentov). – 2013. – 8.11).***

***

В Партии регионов сообщили, что 11 ноября официальный сайт политсилы подвергся массированной хакерской атаке. Об этом сообщила пресс-служба ПР, пишут Контракты.Ua (http://kontrakty.ua/article/69530).

«Таким примитивным образом накануне принятия Верховной Радой важных решений наши политические оппоненты пытаются “закрыть рот” представителям крупнейшей парламентской фракции, ограничить право доступа пользователей Интернета и представителей СМИ к достоверной информации», – объяснили причины атаки в партии.

В ПР также отметили, что из-за DDoS-атаки в работе сайта некоторое время могут наблюдаться сбои. В настоящее время сайт политсилы работает в обычном режиме ***(Партия регионов пострадала от хакеров // Контракты.Ua (http://kontrakty.ua/article/69530). – 2013. – 12.11).***

***

Д. Фримен, также известный как saurik, описал очередную ошибку, связанную с обработкой метаданных в Zip-архивах на всех версиях ОС Android до 4.4. Д. Фримен, который ранее провел анализ безопасности Google Glass, написал в своем блоге, что обнаружил уязвимость еще в июне, но решил дождаться выхода исправления в следующей версии мобильной ОС.

Уязвимость существует из-за ошибки при обработке имен файлов, содержащихся в метаданных ZIP-файла. Злоумышленник может изменить имя файла в метаданных, не меняя при этом имя файла, входящего в состав архива. Подобная брешь в структуре ZIP-архива позволяет злоумышленнику успешно пройти процесс проверки подлинности файла, поскольку во время проверки приложение считывает информацию о файлах внутри архива из метаданных архива (длина имени файла и имя файла). При этом С-код, который распаковывает, устанавливает и выполняет файлы из архива использует длину файла из локального заголовка. Таким образом, атакующий может заразить любое проверенное приложение, после чего модифицировать заголовок и выполнить произвольный код на уязвимой системе.

Эта брешь была устранена в последней версии Android 4.4 Kitkat, и теперь Java-апплет осуществляет проверку файлов, основываясь на тех же данных, что и архиватор ***(Уязвимость в Android позволяет загружать вредоносное ПО в обход системы безопасности // InternetUA (http://internetua.com/uyazvimost-v-Android-pozvolyaet-zagrujat-vredonosnoe-po-v-obhod-sistemi-bezopasnosti). – 2013. – 8.11).***

***

Интернет вступает в «оруэлловскую» эпоху

Каково обличие современного хакера, какова его мотивация, каких угроз от него ждать и как от них обороняться – вот ключевые вопросы повестки дня конференции по кибербезопасности RSA Conference2013, прошедшей в последних числах октября в Амстердаме. Мероприятие можно считать центральной отраслевой дискуссией по вопросам кибербезопасности, на него съезжаются крупнейшие компании, делающие погоду в этой области – Microsoft, RSA, Symantec, Qualys и многие др. На RSA Conference вендоры и независимые эксперты обсуждают ландшафт отрасли сегодня и в ближайшем будущем. В этом году наиболее горячая полемика велась вокруг следующих тем:

– Эпоха идейных хакеров закончилась.

Доля «хакер-активистов», практикующих взлом не корысти ради, а для привлечения общественного внимания к острым проблемам, исчезающе мала –

меньше 1 %. Остальные 99 % случаев зловредных действий мотивированы жаждой наживы – уверен Д. Джонс, специалист подразделения благонадежных вычислений (trustworthy computing) Microsoft. По его словам, киберпреступность прошла путь от кустарей-одиночек до развитой мировой индустрии. Выгодоприобретателю сегодняшних кибрепреступлений вовсе необязательно самому быть хакером – главное иметь деньги, за которые он получит «продукт» с полным жизненным циклом. Реклама, маркетинг, консультации, адаптация «продукта» под нужды «заказчика» и последующее сопровождение – все эти атрибуты развитой индустрии присущи сегодня мировой киберпреступности, считает Д. Джонс.

– Любая анонимная активность отныне воспринимается как подозрительная.

Честному человеку незачем избегать опознания – утверждают вендоры. К списку оруэлловских тезисов а-ля «свобода – это рабство» можно добавить новый: «анонимность – враг приватности». Именно такую формулировку выдал на-гора А. Ковьелло, глава компании RSA, организатора конференции. По его словам, приватность и анонимность – совершенно разные понятия, противоречащие друг другу. Приватность – право пользователя знать, кто и каким образом обрабатывает его персональные данные. В то время как под анонимностью, по мнению А. Ковьелло, может скрываться исключительно стремление избежать ответственности за свои злоумышленные действия в сети. RSA ожидает, что к 2017 г. анонимное пользование Интернетом станет невозможным, а каждое действие человека в сети будет регистрироваться и анализироваться на соответствие признакам угрозы.

– Киберугрозы «дематериализовались».

Закончилась эпоха угроз, которые можно локализовать на уровне инфицированного файла или дыры в браузере. Теперь дырой является сама экосистема – злоумышленники эксплуатируют слабые места в принципах взаимодействия отдельных её элементов. Соответственно, больше не действует «сталлоновский» подход «ты – болезнь, а я – лекарство», поскольку невозможно выпустить программный патч, латающий целую дырявую экосистему.

Т. Рейнс, сотрудник подразделения благонадежных вычислений Microsoft, приводит в качестве яркого примера «дематериализованной» атаки нового поколения чрезвычайно запутанный вирус Flame, который и вирусом назвать сложно. Одна из его особенностей в том, что атакуемые машины сами скачивали инфицированный код, закамуфлированный под полезное обновление ПО, выпущенное официальным разработчиком. Такой подлог стал возможен из-за несовершенства процедуры обновлений и взаимной идентификации сторон. Из-за этого атака Flame оставалась незамеченной годами, и кто знает, сколько еще аналогичных схем не выявлены по сей день.

В Microsoft считают, что борьба с угрозами такого вида должна происходить еще на этапе создания нового ПО. Как поясняет М. Риви, глава подразделения благонадежных вычислений Microsoft, в компании разработали

целую методологию под названием «гарантия операционной безопасности» (Operational Security Assurance – OSA). «Разработчики должны находиться в постоянном диалоге с заказчиками ПО, специалистами по безопасности и тестировщиками, начиная с самых ранних стадий разработки продукта. Постоянный диалог необходим, чтобы все участники экосистемы говорили на одном языке, обменивались друг с другом своей «головной болью», создавая новую программную экосистему, лишенную слабых мест», – поясняет М. Риви.

– Периметр сети прекратил существование.

Активное использование в работе социальных сетей, изобилие каналов коммуникации между людьми, удаленные рабочие места, разнообразие устройств, в т. ч. принесенных на работу из дому (концепция BYOD) окончательно размыли периметр сети. Принцип «моя сеть – моя крепость» больше не действует. Соответственно, оберегать корпорацию от «внешних» угроз, выстраивая защиту «по периметру» сегодня уже невозможно. Примечательно, что единого мнения о новой концепции, которая придет на смену защите периметра, у вендоров нет.

– «Острова» сливаются в циклопа из big data.

Под «островами» подразумеваются отдельные компании и госучреждения. Каждый «остров» накапливает внутренние знания о своих пользователях и моделях их поведения. В случае выявления атаки, её характерные черты сохраняются только в пределах «острова». Следующий шаг вендоры видят в объединении идентификаторов из отдельных «островов» в единую онлайн-систему опознания угроз, состоящую из циклопического объема big data, накопленного по всему миру. И уже к 2020 г. этот «циклоп» будет судить, насколько подозрительно каждое действие каждого пользователя, чтобы «в случае чего» отрезать его от внешнего мира до наступления «серьезных последствий».

В целом, из представлений компаний-участников, озвученных на конференции, вырисовывается мрачная картина автоматизированного будущего, в котором машины следят за каждым шагом людей «по их же просьбе и во их же благо». Впрочем, это не сильно удивляет, поскольку многие из компаний – приверженцы радикального или даже параноидального подхода к кибербезопасности – мол, всё зафиксировать, запротоколировать, изучить и взять «на карандаш». А кто избегает – тот потенциально неблагонадежен. В кулуарах многие из участников открыто симпатизируют системе PRISM, воспринимая её «колоссальный инженерный шедевр». Приверженцы «радикальной безопасности» сначала запугивают «страшилками» о нарастающем количестве неизученных угроз и об организованной мировой киберпреступности, и тут же успокаивает – мол, мы все преодолеем, но нужно тщательней изучить признаки злоумышленного поведения. В этом свете, «оруэлловские тезисы» вендоров выглядят вполне органичным базисом их «радикальной безопасности».

Б. Фитцджеральд, директор по маркетингу RSA, пытается сгладить категоричность своего босса, поясняя, что тезис «анонимность – враг

приватности» применим скорее к деятельности крупных корпораций. «Что касается слежки спецслужб и анонимности граждан, здесь, конечно, полемику нужно вести в другом ключе. Это палка о двух концах. С одной стороны – тоталитарная слежка, а с другой – вседозволенность, провоцирующая киберпреступность. Наша общая задача – найти золотую середину», – считает Б. Фитцджеральд.

В то же время, он признает, что дискуссия о «золотой середине» только начинается и сегодня еще никто не может четко описать, как много «степеней свободы» останется в Интернете через три-пять лет ***(Интернет вступает в «оруэлловскую» епоху // InternetUA (http://internetua.com/internet-vstupaet-v--oruellovskuua--epohu). – 2013. – 10.11).***

***

Антифишинговая рабочая группа опубликовала на этой неделе очередной отчет о фишинговой активности, в котором указывается, что количество новых компаний и сервисов, названия которых используются фишерами, достигло рекордных 639 в предыдущем квартале.

Наибольшей популярностью пользуются финансовые сервисы и платежные системы, набравшие 48 % всех используемых фишерами названий.

«Остальные популярные цели – ISP, облачные сервисы и хостинги», – говорит директор по маркетингу MarkMonitor Ф. Фелман. Похищение данных учетных записей от этих сервисов – ключ к получению финансовой прибыли.

Использование остальных приманок, включая сети розничной продажи, правительственные письма, аукционы и социальные сети, осталось в прежних рамках, как говорится в отчете. Исключением стали онлайн-игры – количество скомпрометированных названий снизилось до 2 % от общего числа, в то время как в прошлом квартале это число достигало 6 %.

На территории США в настоящее время размещается наибольшее количество фишинговых сайтов. Перед этим на первом месте находилась Германия. Что интересно – Россия, которая всегда находилась на высших местах рейтинга, почти исчезла из списка в июне, а ее место занял Казахстан. Скорее всего, это связано с увеличением количества мобильных платежей на территории второй страны.

Большинство фишинговых атак на мобильные устройства включали в себя получение поддельных ссылок через SMS. Д. Дебросс, директор Websense Security Labs, считает, что каждый житель планеты, имеющий мобильный телефон, непременно сталкивался с фишинговыми сообщениями.

Количество нового вредоносного ПО, использующегося в фишинговых атаках, возросло на 12 % по сравнению с аналогичным периодом в прошлом году. В этом году уровень уникальных вредоносных программ составляет 17 %, а 77 % от всего нового вредоносного ПО составляют трояны.

Количество зараженных по всему миру компьютеров составило 33 %. Лидер в этом сегменте – Китай: более половины всех компьютеров в стране заражено вредоносным ПО. Среди остальных стран с большим количеством

зараженных компьютеров стоит отметить Турцию, Перу, Боливию, Эквадор, Россию, Аргентину, Тайвань, Словению и Сальвадор. Наименьшее количество зараженных ПК – в Японии и странах Европы ***(Эксперты: Фишеры увеличили количество приманок среди популярных ресурсов // InternetUA (http://internetua.com/eksperti--fisheri-uvelicsili-kolicsestvo-primanok-sredi-populyarnih-resursov). – 2013. – 12.11).***

***

Одинадцать самых ярких компьютерных вирусов: от невидимки до монстра

11 ноября 1983 г. американский студент из Университета Южной Калифорнии Ф. Коэн составил программу, демонстрирующую возможность заражения компьютера. Скорость размножения вируса внутри компьютера VAX составила от пяти минут до часа, и дальнейшие опыты в этом направлении были запрещены как исключительно опасные.

Через год Ф. Коен написал об этом научную работу, в которой не только дал определение вирусу, но и предвосхитил распространение вирусов по компьютерным сетям и появление антивирусных программ.

Первый нелабораторный вирус появился позже – в 1986 г., он назывался Brain («Мозг») и пришел из Пакистана. Вирус был способен инфицировать лишь дискеты и ловко скрывал свое присутствие. Следующие два вируса – Lehigh и Jerusalem – появились в университетских кругах США и Израиля соответственно.

Первый антивирус, способный очищать дискеты от Brain, вышел в 1988 г. Вслед за этим число «бойцов» с обеих сторон стало расти как снежный ком.

Существующие технологии позволяют создать вирус, который распространится по всей планете менее чем за час. Digit.ru из миллионов вредоносных программ выбрал 11 наиболее печально запомнившихся вирусов и отсортировал их в хронологическом порядке.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). Вирусы могут повредить или полностью уничтожить файлы, данные и даже операционную систему со всеми файлами в целом.

1. Brain, 1986 г.: первый вирус, вызвавший эпидемию.

По сравнению с последователями, Brain практически безопасен, но он стоит нашего внимания в первую очередь потому, что первым вызвал настоящую вирусную эпидемию.

Передавался Brain по загрузочным секторам дискет. Разработка вируса лежит на совести братьев Амджата и Базита Алви, которые запустили его в 1986 г. Обнаружен Brain был летом 1987 г. Только в США вирус заразил более 18 тыс. компьютеров.

В основе разработки Brain лежали благие намерения: программа должна была наказать местных пиратов, ворующих программное обеспечение у фирмы братьев.

Вирус Brain ко всему прочему еще и первый стелс-вирус (вирус, полностью или частично скрывающий свое присутствие в системе). Так, при попытке чтения зараженного сектора, он «подставлял» его незараженный оригинал.

2. Jerusalem, 1988 г.: в пятницу 13-го удалял все данные с жесткого диска.

Вирус Jerusalem появился 13 мая 1988 г., он уничтожал зараженные файлы при попытке их запуска. Проявил себя в Европе, США, на Ближнем Востоке. Первые сообщения о заражении приходили из высших учебных заведений и от крупных компаний в самых различных странах.

Этот вирус был создан в Израиле – отсюда и основное имя. Второе его название – «Пятница 13-е». Это был первый вирус для MS-DOS, вызвавший грандиозную панику: скачанный с дискеты, он активировался при наступлении злополучного числа – пятницы 13-го – и удалял абсолютно все данные с жесткого диска.

В те времена еще мало кто верил в существование компьютерных вирусов. Антивирусных программ почти не существовало, а потому пользователи были беззащитны перед ними.

3. Червь Морриса, 1988 г.: вывел из строя весь Интернет.

Активность этого опасного вредителя пришлась на ноябрь 1988 г. «Червь Морриса» парализовывал работу компьютеров своим хаотичным и бесконтрольным размножением. Из-за него вышла из строя вся, тогда еще не слишком глобальная, сеть. И хотя сбой длился недолго, общие убытки тогда оценивались в 96 млн дол.

4. Michelangelo (March6), 1992 г.: сыграл на руку антивирусным компаниям.

Проникая через дискеты на загрузочный сектор диска, Michelangelo тихо сидел там, не напоминая о своем существовании до 6 марта. А в этот день «счастливчики», получившие «Микеланджело» на свой компьютер, обнаруживали, что все данные с их жесткого диска стерты.

Лютовал этот вирус в 1992 г. Он сыграл на руку компаниям, производящим антивирусы: пользуясь случаем, бизнесмены раздули истерию до невиданных масштабов, в то время как от него пострадали всего около 10 тыс. машин.

5. CIH, Win95.CIH или «Чернобыль», 1998 г.: заразил до полумиллиона ПК.

Один из самых знаменитых вирусов мира. Зараженный компьютер не «заводился», поскольку вирус уничтожал BIOS подчистую.

CIH создан в 1998 г. тайваньским студентом, по инициалам которого и назван. Вирус попадал в компьютер через Интернет, электронную почту и диски, прятался внутри других программ, а в определенный момент (26 апреля, совпадает с датой аварии на Чернобыльской АЭС) вирус активировался, стирая содержимое жесткого диска и нанося вред аппаратной части компьютера.

Эпидемия «Чернобыля» пришлась на апрель 1999 г. Тогда из строя было выведено более 300 тыс. компьютеров, в основном, в Восточной Азии. В

течение нескольких последующих лет 26 апреля вирус продолжал свое черное дело, что, по разным экспертным оценкам, нанесло урон до полумиллиона компьютеров во всем мире.

6. Melissa, 1999 г.: массово засорил корпоративную почту.

Пришествие «Мелиссы» пришлось на 26 марта 1999 г. Вирус после заражения системы находил адресную книгу программы MS Outlook и рассылал свои копии первым 50 адресам в этой книге. Пользователь об этом не подозревал, хотя рассылка производилась от его имени.

Из-за «Мелиссы» крупные IT-компании, в том числе Microsoft и Intel, в массовом порядке отключали корпоративные сервисы электронной почты. Вирус распространялся с бешеной скоростью, сумма нанесенного им ущерба оценивается экспертами более чем в 100 млн дол.

7. I Love You, Loveletter, The Love Bug, 2000 г.: «романтик», нанесший ущерб на 5,5 млрд дол.

Список самых опасных компьютерных вирусов продолжает вирус с романтическим названием I Love You, он же Loveletter, он же The Love Bug. Многие эксперты считают его самым вредоносным за всю историю существования Интернета.

Распространялся «романтик» по электронной почте, в теме письма при этом были слова: «я тебя люблю». К такому письму прилагалось вложение, в котором и сидел зловред, крадущий с зараженной машины пароли.

Механизм распространения Loveletter – как у «Мелиссы»: вирус искал адреса в Outlook и отправлял собственные копии. Loveletter заразил миллионы компьютеров по всему миру, 10 % всех существовавших на то время компьютеров были инфицированы, что нанесло ущерб в размере 5,5 млрд дол.

8. Nimda, 2001 г.: первый вирус-«администратор».

Вирус был создан в Китае 18 сентября 2001 г. Название произошло от слова admin, написанного в обратном порядке. Суть Nimda в том, что вирус мог создавать для себя на зараженных компьютерах права администратора, после чего изменял и нарушал конструкцию сайтов, блокировал доступ на хосты, IP-адреса и т. д.

На компьютеры Nimda проникал столь виртуозно, что уже через 22 мин. после своего создания он стал самым распространенным в Интернете.

9. My Doom, 2004 г.: чемпион по скорости распространения.

My Doom – самый быстрый вирус электронной почты. Работал он по нарастающей: каждый следующий компьютер отправлял спама еще больше, чем предыдущий. Также он модифицировал операционную систему, блокируя доступ к сайтам многих антивирусных компаний, новостным лентам и различным разделам сайта компании Microsoft.

Помимо этого, на его счету даже DDoS-атака на сайт Microsoft.

10. Conficker, 2008 г.: 12 млн жертв.

Этот вирус имеет славу опаснейшего из известных компьютерных червей. Атакует он операционные системы семейства Microsoft Windows. Вирус поразил более 12 млн компьютеров во всем мире.

Принцип действия Conficker таков: червь находит уязвимости Windows, связанные с переполнением буфера, и затем отключает сервисные службы и обновление Windows, а также блокирует доступ к сайтам ряда производителей антивирусов.

11. Win32/Stuxnet, 2010 г.: первый, заразивший промышленные системы.

И в заключение – об одном из наиболее страшных вирусов последних лет. Вирус был обнаружен не только на компьютерах рядовых пользователей, но и в промышленных системах, управляющих автоматизированными производственными процессами.

Win32/Stuxnet – компьютерный червь, поражающий компьютеры под управлением операционной системы Microsoft Windows. 17 июня 2010 г. его обнаружил антивирусный эксперт С. Уласень из белорусской компании «ВирусБлокАда» (в настоящее время работает в «Лаборатории Касперского»).

Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Таким образом, червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в автоматизированных системах управления технологическим процессом (АСУ ТП) промышленных предприятий, электростанций, аэропортов и т. п.

Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру. Существует предположение, что Stuxnet представляет собой специализированную разработку спецслужб Израиля и США, направленную против ядерного проекта Ирана. В качестве доказательства упоминаются завуалированные упоминания слова MYRTUS, содержащиеся в коде червя.

Кроме того, в коде однажды встречается никак не объясненная дата 9 мая 1979 г. (19790509). В этот день произошла казнь известного иранского промышленника Х. Эльганяна, еврея по национальности.

Американский журналист Д. Сангер в книге «Противостоять и скрывать: тайные войны Обамы и удивительное использование американской силы» утверждает, что Stuxnet был частью антииранской операции «Олимпийские игры» американского правительства.

Данный вирус использует четыре уязвимости системы Microsoft Windows (уязвимость «нулевого дня» (zero-day) и три ранее известные уязвимости), позволяющие ему распространяться при помощи USB-flash накопителей. Оставаться незамеченным антивирусными программами ему помогало наличие настоящих цифровых подписей (два действительных сертификата, выпущенных компаниями Realtek и JMicron) ***(11 самых ярких компьютерных вирусов: от невидимки до монстра // InternetUA (http://internetua.com/11-samih-yarkih-kompuaternih-virusov--ot-nevidimki-do-monstra). – 2013. – 12.11).***

***

Несколько уязвимостей нулевого дня, обнаруженных хакерами в веб-обозревателе Internet Explorer (IE), эксплуатируются в настоящее время злоумышленниками с целью компрометации систем пользователей и дальнейшей установки вредоносного ПО. Заражение компьютера происходит после того, как жертва посетила один из нескольких веб-сайтов, подконтрольных мошенникам, сообщают эксперты FireEye.

Как следует из отчета исследователей, речь идет о передовой и довольно сложной APT-атаке, в рамках которой хакеры использовали те же C&C сервера, что и во время кампании Operation DeputyDog.

Интересно также, что, по данным FireEye, злоумышленники использовали для своей атаки неназванный американский «стратегически важный веб-сайт», посетителями которого являются люди, заинтересованные в вопросах национальной безопасности.

«Эксплоит нацелен на английскую версию Internet Explorer, однако мы уверены, что вредоносный код может быть легко переписан для работы с другими языками, – отмечают эксперты. – Основываясь на нашем анализе, уязвимость затрагивает IE версий 7, 8, 9 и 10» ***(Новая уязвимость в Internet Explorer // InternetUA (http://internetua.com/novaya-uyazvimost-v-Internet-Explorer). – 2013. – 12.11).***

***

Если верить представителям RIAA и MPAA, любой торрент-портал несет в себе вредоносную угрозу пользователю, и каждый, кто хотя бы раз загрузил контент из файлообменника, подвержен риску потери важных данных или другим угрозам.

Несмотря на то что реальная ситуация не настолько плачевна, как бы хотелось некоторым представителям отрасли, пользователи торрент-трекеров регулярно становятся жертвами киберпреступников.

Так, по данным портала TorrentFreak, в феврале текущего года в сети появилась группировка MeGaHeRTZ, позволяющая скачивать свой контент бесплатно. Первым выложенным релизом от разработчиков стала пиратская копия BurnAware Professional v6.0 с дополнением, обходящим защиту продукта.

Далее группа выложила в сеть ряд других программ, среди которых SmartFTP, DVDFab, FlashFXP, Incredimail, Traktor и сотни других, с которыми поставлялись бесплатные обновления.

Несмотря на одобрение и популярность среди пользователей, оказалось, что группа MeGaHeRTZ вела «грязную игру». Так, установив предлагаемое пиратами ПО, пользователи начали замечать необычную активность межсетевого экрана. Проблема заключалась в том, что обновление для антивируса Malwarebytes Anti-Malware Pro использовало для исходящего трафика порт 25, обычно используемый для отправки электронной почты.

Обнаруживший несоответствие пользователь также отметил, что установленное ПО собирает информацию с компьютера. Данные, собранные с

инфицированной системы, включали имя пользователя, имя компьютера, серийный номер, полученный из Windows API и IP-адрес. Далее собранная информация передавалась на один из трех предопределенных электронных адресов, в которых в различных измененных формах присутствовало название группы MeGaHeRTZ.

В ходе дальнейшего исследования релизов, предоставленных пиратами, было установлено, что идентичный механизм кражи данных присутствовал в нескольких из предложенных программ.

По словам исследователей, пока неизвестно, с какой целью группа собирала пользовательские данные. Однако в настоящий момент MeGaHeRTZ прекратила свое существование (по крайней мере, в том виде, в котором действовала на протяжении девяти месяцев). Так, с 9 ноября пиратское сообщество заблокировало каждый возможный релиз группы.

Тем не менее, ранее загруженные в сеть релизы остаются в Интернете, и удалить их все просто невозможно, что делает инфицированные продукты потенциально опасными.

По мнению экспертов, единственным способом избежать инфицирования является полный отказ от загрузки какого-либо ПО, ранее выложенного в сеть представителями MeGaHeRTZ ***(Группа разработчиков пиратского ПО 9 месяцев шпионила за пользователями // InternetUA (http://internetua.com/gruppa-razrabotcsikov-piratskogo-po-9-mesyacev-shpionila-za-polzovatelyami). – 2013. – 12.11).***

***

Гощанский районный совет Ривненской области сообщил об атаке на свой официальный сайт хакеров-террористов из Албании, как заявил глава райсовета С. Гречич, передает NewsOboz.org со ссылкой на Корреспондент.biz.

По его информации, лица, выложившие на сайте www.grr.gov.ua призыв к борьбе за Косово, считают себя албанскими хакерами-террористами.

На сайте опубликовано видео и текст о том, что Косово было и будет частью Албании, а не Сербии, а также, что сербы – это славяне и не имеют ничего общего с албанцами ***(На Ровенщине райсовет заявил об кибератаке албанских хакеров-террористов // NewsOboz (http://newsoboz.org/proisshestviya/raysovet-v-rovenskoy-oblasti-zayavlyaet-ob-kiberatake-albanskih-13112013122600). – 2013. – 13.11).***

***

Администрация Facebook заблокировала учетные записи некоторых пользователей после того, как оказалось, что их учетные данные были скомпрометированы в результате взлома аккаунтов в онлайн-сервисах Adobe. Facebook просит пользователей, использующих для авторизации в Facebook и Adobe одни и те же пароли, сменить свои учетные данные.

При попытке войти в учетную запись в соцсети эти пользователи получают сообщение о том, что «произошел инцидент безопасности на сайте,

не связанном с Facebook», и их учетные записи подвергаются риску из-за использования одних и тех же паролей.

«Для того, чтобы обезопасить свою учетную запись, вам необходимо ответить на несколько вопросов и изменить свой пароль. Для вашей безопасности вы не будете видны никому в Facebook до тех пор, пока не закончите», – говорится в сообщении.

«Мы активно ищем в Интернете источники со скомпрометированными паролями», – заявил инженер по безопасности Facebook К. Лонг в ответ на публикацию эксперта безопасности Б. Кребса, посвященную этому вопросу. «Благодаря нашему опыту, мы можем эффективнее защищать учетные записи, логины и пароли были похищены. Для обеспечения безопасности этих аккаунтов мы используем автоматизированный процесс», – отметил К. Лонг.

Напомним, что в начале октября нынешнего года злоумышленникам удалось скомпрометировать 150 млн учетных записей в онлайн-сервисах Adobe. Эта утечка данных является самой масштабной за всю историю существования Интернета ***(Facebook просит пользователей сменить пароли // InternetUA (http://internetua.com/Facebook-prosit-polzovatelei-smenit-paroli). – 2013. – 13.11).***

***

13 ноября сайт национального проекта «Открытый мир» подвергается DDoS-атаке. Об этом НБН сообщили в пресс-службе Госинвестпроекта.

«DDoS-атака на сайт www.educom.ua началась около 10:00 и продолжается с разной интенсивностью. В атаке задействована сеть ботов, включающих более тысячи хостов. Поэтому возможны временные перебои в работе сайта», – сказано в сообщении.

Руководитель нацроекта «Открытый мир» Р. Свирский считает, что атака, начавшаяся за несколько дней до окончания конкурса «2000 школ», очевидно, направлена на то, чтобы помешать представителям школ подать заявки на участие в конкурсе. «Это очень обидно, ведь сейчас регистрация участников идет активно. Школы, до последнего тянули с подачей заявки, могут упустить свой шанс приобщиться к “Открытому мира” в этом году», – добавил руководитель нацпроекта.

В настоящее время Национальный проект принимает все необходимые меры для обеспечения нормального функционирования ресурса.

Национальный проект «Открытый мир» – один из 11 национальных проектов, утвержденных президентом Украины в 2010 г. как приоритет в социально-экономическом развитии страны.

Целью нацпроекта является создание единой национальной информационной среды. С помощью новейших информационно-телекоммуникационных технологий будет обеспечен доступ всех участников образовательного процесса: учащихся, учителей, родителей, администраторов образования к мультимедийным базам данных.

Проект предусматривает унификацию методик обучения и обеспечение обработки этих методических материалов в режиме реального времени методистами и педагогами. Проект создаст условия, которые бы поощряли учащихся к успешной учебе и обеспечили равные возможности доступа к качественному образованию каждого гражданина Украины, независимо от места проживания ***(Сайт национального проекта «Открытый мир» подвергся DDoS-атаке // Независимое Бюро Новостей (http://nbnews.com.ua/ru/news/105117/). – 2013. – 13.11).***

***

Исследователи из Кембриджского университета обнаружили необычный способ получения несанкционированного доступа к телефонам, сообщает BBC. Оказывается, узнать PIN-код устройства можно с помощью приложения, которое перехватывает данные с микрофона и фронтальной камеры.

Для этого исследователи написали программу PIN Skimmer, которая фиксировала звуки нажатий на сенсорную клавиатуру, выражение лица и движения глаз пользователя во время ввода пин-кода. С помощью этой информации и можно угадывать возможные варианты пароля.

Испытания проводились на аппаратах Google Nexus-S и Samsung Galaxy S3. С первой попытки PIN Skimmer вычислил 15 четырехзначных паролей из пятидесяти, а с пятой – более 20. С восьмизначным пин-кодом удалось угадать 60 % паролей после 10 попыток.

Чтобы не привлекать внимания пользователя к быстрой разрядке батареи, вычисления проводились в облаке. Таким образом, работа нелегального приложения оставалась незамеченной.

По словам исследователей Р. Андерсона и Л. Саймона, в будущем фронтальная камера и микрофон будут представлять серьезную угрозу для безопасности данных. Чтобы обезопасить себя, они рекомендуют работать в защищенной среде и при этом отключать как можно больше сенсоров ***(Пароль к телефону можно подобрать по выражению лица // InternetUA (http://internetua.com/parol-k-telefonu-mojno-podobrat-po-virajeniua-lica). – 2013. – 13.11).***

***

Неизвестные похитили логины и пароли всех 860 тыс. пользователей, зарегистрированных на посвященном продукции Apple форуме MacRumors. Об этом сообщила администрация сайта.

В сообщении отмечается, что похищение персональных данных пользователей произошло 12 ноября. Обстоятельства хакерской атаки в настоящее время выясняются. К расследованию привлечены сторонние эксперты. О ком именно идет речь, руководство сайта не уточняет.

Администрация форума рекомендует всем пользователям исходить из того, что доступ к их аккаунту теперь в любое время открыт для злоумышленников. В связи с этим пользователей просят срочно сменить

пароли. Кроме того, администрация рекомендует не использовать тот же пароль на других сайтах.

В свою очередь информационный портал Arstechnica со ссылкой на руководство сайта сообщает, что логины и пароли пользователей были похищены через аккаунт модератора, у которого был доступ ко всей такой информации. Хакеры, по всей видимости, сумели подобрать к нему пароль.

Руководство MacRumors сравнило случившееся с произошедшей летом 2013 г. хакерской атакой на форумы, посвященные операционным системам Ubuntu. Тогда неизвестные аналогичным способом похитили учетные данные всех пользователей сервиса, общее число которых насчитывает почти два миллиона человек. Организаторы кражи паролей так и не были найдены.

MacRumors входит в число крупнейших сайтов, аккумулирующих новости и слухи о продукции компании Apple. Он был открыт в 2000 г. На сегодняшний день на нем зарегистрированы 860 тыс. пользователей. Всего за время существования сервиса на нем были размещены около 15 млн постов ***(Хакеры украли пароли к 860 тысячам аккаунтов форума о продукции Apple // InternetUA (http://internetua.com/hakeri-ukrali-paroli-k-860-tisyacsam-akkauntov-foruma-o-produkcii-Apple). – 2013. – 13.11).***

***

Эксперты в области информационной безопасности заявили, что утверждения представителей Международного агентства по атомной энергии (МАГАТЭ) о том, что конфиденциальная информация организации не была скомпрометирована в результате недавнего хакерского нападения, вызывает серьезные сомнения. Об этом сообщает издание v3.co.uk.

Речь идет о произошедшем 12 ноября этого года инциденте безопасности, в ходе которого компьютерные системы IAEA, как сообщается, были инфицированы неизвестным вредоносным приложением, предназначенным для хищения информации. В рамках атаки хакерам удалось заразить несколько персональных компьютеров Международного Венского Центра (штаб-квартира агентсва), где также находится одна из атомных лабораторий. Согласно официальному комментарию IAEA злоумышленникам не удалось получить доступ к какой-либо конфиденциальной информации.

Вместе с тем, глава FireEye, Д. Стир уверен, что особенности сегодняшних вредоносных приложений, ориентированных на энергетическую индустрию, практически полностью лишают возможности гарантировать, что какие-либо данные не были скомпрометированы.

«Если говорить на чистоту, то каким образом в МАГАТЭ может быть уверено в том, что их информация не была похищена – что они сделали, чтобы удостовериться в этом?» – рассуждает руководитель FireEye.

Аналогичной позиции придерживается ведущий исследователь F-Secure Ш. Салливан, дополнивший, что отсутствие последствий этой атаки может быть подтверждено только после раскрытия подробностей инцидента ***(Хакеры могли похитить конфиденциальные данные в ходе атаки на***

Международное агентство по атомной энергии // InternetUA (http://internetua.com/hakeri-mogli-pohitit-konfidencialnie-dannie-v-hode-ataki-na-mejdunarodnoe-agentstvo-po-atomnoi-energii). – 2013. – 13.11).

***

В III квартале 2013 г. 99,9 % всех атак на мобильные платформы были нацелены на ОС Android, гласят данные Лаборатории Касперского, пишут «Экономические известия» (http://news.eizvestia.com/news_technology/full/prakticheski-vse-virusnye-ataki-na-smartfony-napravleny-na-android).

Аналитики отмечают среди новых угроз троян Svpeng, который в отличие от других вредоносных программ этого типа дает возможность злоумышленникам воровать деньги с банковского счета, заразив один только смартфон пользователя, информирует eizvestia.com.

Запрашивая баланс у сервиса мобильного банкинга и получая ответное SMS-сообщение с предложением пополнить баланс мобильного телефона, зловред переводил деньги с банковского счета пользователя на мобильный счет злоумышленников, минуя традиционную в подобных хищениях связку смартфон – компьютер.

Кроме того, эксперты отмечают новые трюки от создателей мобильных ботнетов – злоумышленники получили возможность более оперативно управлять троянцами на зараженных смартфонах, начав использовать в качестве дополнительного командного центра сервис Google Cloud Messaging (GCM), позволяющий отправлять на мобильные устройства небольшие сообщения.

«Большинство вредоносных приложений для Android ориентировано на кражу денег и лишь во вторую очередь – на кражу личной информации. При этом все механизмы инфицирования, распространения и сокрытия деятельности стремительно мигрируют с классических ОС. Сейчас злоумышленники делают все, чтобы украсть как можно больше, и, скорее всего, вирусописатели и далее будут наращивать число ботнетов, увеличивая темп заражения Android-систем», – поделился прогнозом В. Чебышев, антивирусный эксперт компании.

Подчеркнем, что всего за III квартал 2013 г. продуктами Лаборатории Касперского было задетектировано 500,2 млн атак, при этом 45,2 % веб-ресурсов, используемых для распространения вредоносных программ, были расположены в США и России.

Жертвами этих веб-угроз чаще всего становились жители стран СНГ: девять из этих стран попали в десятку самых «опасных» регионов с этой точки зрения ***(Практически все вирусные атаки на смартфоны направлены на Android // Экономические известия (http://news.eizvestia.com/news_technology/full/prakticheski-vse-virusnye-ataki-na-smartfony-napravleny-na-android). – 2013. – 15.11).***

***

Компания «Доктор Веб» сообщила об активном распространении вредоносных программ семейства Trojan.Hiloti.

Как сообщает «CyberSecurity», вредоносы предназначены для подмены поисковой выдачи. Злоумышленники организовали специальную партнерскую программу с целью увеличения количества установок вредоносного ПО, и используют в своих целях набор эксплойтов, при помощи которых троянские программы загружаются на компьютеры потенциальных жертв.

Термин «подмена выдачи» хорошо известен специалистам по информационной безопасности, а также многим пользователям Интернета, ставшим жертвами злоумышленников. Данную функцию реализует множество вредоносных программ: установившись на компьютере жертвы, такие троянцы отслеживают активность веб-браузеров, и при обращении пользователя к ресурсам поисковых систем вместо результатов поиска выдают пользователю ссылки на различные, в том числе мошеннические, сайты. К указанной категории относятся и троянцы семейства Trojan.Hiloti, отдельные представители которого получили распространение еще в 2010 г. На сегодняшний день в вирусных базах Dr.Web имеется более 80 записей, соответствующих различным версиям этой угрозы. Появление новых модификаций Trojan.Hiloti специалисты связывают с организацией партнерской программы Podmena-2014, к которой злоумышленники пытаются привлечь распространителей вредоносного ПО.

Вирусописатели предлагают владельцам сайтов разместить на своих площадках специальный сценарий, который с определенным интервалом загружает с сервера злоумышленников исполняемый файл вредоносной программы Trojan.Hiloti. Вместе с установщиком самого троянца распространяется модуль руткита, позволяющий скрывать работу вредоносной программы в инфицированной операционной системе. С целью усложнить детектирование Trojan.Hiloti исполняемый файл троянца автоматически переупаковывается на сервере злоумышленников через определенные промежутки времени.

Загрузка троянца на компьютеры потенциальных жертв осуществляется с использованием уязвимостей CVE-2012-4969, CVE-2013-2472, CVE-2013-2465 и CVE-2013-2551, а также методов социальной инженерии.

Злоумышленники предлагают распространителям достаточно простую схему работы: те способствуют установке Trojan.Hiloti на компьютеры пользователей, разместив определенный код на принадлежащих им интернет-ресурсах, после чего при попытке жертвы выполнить какой-либо запрос на поисковом сайте троянец будет демонстрировать в окне браузера оплаченные рекламодателями ссылки вместо ожидаемой поисковой выдачи. В некоторых случаях переход пользователя по подобным ссылкам приводит к загрузке различных нежелательных приложений, таких как поддельные антивирусы, требующие оплаты за «лечение» компьютера. Распространители же получают процент от дохода, полученного злоумышленниками в рамках данной

партнерской программы ***(Зараженные сайты раздают троянца для подмены поисковых запросов // InternetUA (http://internetua.com/zarajennie-saiti-razdauat-troyanca-dlya-podmeni-poiskovih-zaprosov). – 2013. – 15.11).***

***

Пользователь И. Мавлиев опубликовал у себя на странице запись, ссылка в которой вела на приложение, автоматически публикующее его пост на чужих страницах и сообществах. За полчаса ничем не примечательная запись набрала более 80 тыс. репостов, пишет tjournal.ru.

Запустившись после перехода по ссылке, приложение отправляло пользователя на его модифицированную страницу. На ней включалась анимация всех изображений, изменялся цвет, а фоном играла песня PSY – Gentleman. При этом репост оригинальной записи И. Мавлиева публиковался незаметно для пользователя не только на его странице, но и во всех публичных сообществах, в которых он числится администратором.

Таким образом пост И. Мавлиева попал в сотни популярных сообществ, включая официальные: LIVE, «Олимпийские игры», «Команда поддержки», «Подслушано», «Цукерберг Позвонит», страница блогера Дюрана и даже TJournal. В пике запись собрала около 85 тыс. репостов, но потом их количество резко снизилось почти до нуля.

Как объяснил И. Мавлиев TJournal, в приложении не было ничего вредоносного, кроме репостов. По его словам, возможность такого «взлома» не является виной разработчиков «ВКонтакте»: его суть кроется в «не совсем очевидной» работе класса ExternalInterface. XSS-уязвимость, позволявшая делать репосты, содержалась в плеере Flash. Экс-разработчик «ВКонтакте» Д. Ольшин конкретизировал: ошибка, позволившая распространиться эпидемии репостов, содержалась в коде сервиса видеозвонков, который он и писал.

Созданное И. Мавлиевым приложение администрация «ВКонтакте» удалила через 20–25 мин. после публикации. Появилось еще как минимум одно такое же приложение, однако и оно было заблокировано.

И. Мавлиев объясняет акцию желанием повеселиться, но она также была своего рода экспериментом: он хотел узнать, как быстро будет распространяться информация, и поделился статистикой своей страницы ***(Пользователей «ВКонтакте» атаковал хакер // InternetUA (http://internetua.com/polzovatelei--vkontakte--atakoval-haker). – 2013. – 15.11).***

***

Хакерам, связанным с международной группировкой Anonymous, удалось взломать компьютеры нескольких американских федеральных ведомств, используя брешь в программном обеспечении Adobe, и получить доступ к секретной информации. Об этом сообщает 15 ноября Reuters со ссылкой на материалы ФБР, оказавшиеся в распоряжении агентства. Официального подтверждения этой информации не поступало.

Согласно документам ФБР, кампания по взлому правительственных компьютеров продолжалась с декабря 2012 г. и затронула армию США, министерство энергетики, министерство здравоохранения и социальных служб и, предположительно, многие другие госучреждения.

По информации агентства, правоохранительные органы продолжают расследование действий хакеров и поиск новых взломов, поскольку неполадки до сих пор не были устранены. В записке ФБР, в частности, содержатся рекомендации для системных администраторов по выявлению возможных угроз.

В документе подчеркивается, что большую часть взломов еще предстоит обнаружить, и судить о масштабах кампании в настоящее время невозможно. Тем не менее, в распоряжении Reuters оказались отдельные численные свидетельства. Так, во внутриведомственном письме для сотрудников министерства энергетики сообщается, что злоумышленники получили доступ к персональным данным по меньшей мере 104 тыс. сотрудников учреждения, а также подрядчиков, членов семей и других лиц, в том числе к почти 2 тыс. банковских счетов.

По версии следствия, взломы могут быть связаны, среди прочего, с деятельностью Л. Лава и других хакеров, которые обнаружили уязвимости в платформе веб-разработки Adobe ColdFusion ***(ФБР выявило систематические взломы правительственных компьютеров // InternetUA (http://internetua.com/fbr-viyavilo-sistematicseskie-vzlomi-pravitelstvennih-kompuaterov). – 2013. – 16.11).***