СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16–28.02)

2015 № 4

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16–28.02)
№ 4

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

© Національна бібліотека України
імені В. І. Вернадського, 2015

Київ 2015

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Компания Facebook работает над созданием специальных версий своих приложений, которые будут предназначены для устройств виртуальной реальности, сообщает The Verge.

О том, что соцсеть работает над такими приложениями, рассказал директор Facebook по развитию продуктов К. Кокс. «Мы работаем над приложениями для виртуальной реальности», – сказал К. Кокс в ходе конференции Code Media, которая прошла в Калифорнии.

Топ-менеджер Facebook не уточнил, о каких именно приложениях идет речь, однако предположил, что в будущем с их помощью любой пользователь шлема или очков виртуальной реальности сможет делиться с окружающими событиями из своей жизни. Впрочем, по мнению К. Кокса, такое будущее наступит все же не очень скоро, поскольку технологии виртуальной реальности пока недостаточно развиты.

Напомним, что Facebook приобрела компанию Oculus VR, занимающуюся разработкой шлема виртуальной реальности Rift, в марте прошлого года. Стоимость сделки составила 2 млрд дол.

В сентябре Oculus VR представила новый прототип своего шлема виртуальной реальности, который получил кодовое имя Crescent Bay. Новая версия устройства получила встроенный звук, стала легче, а система отслеживания движений стала работать точнее. Кроме того, обновленный шлем виртуальной реальности оснащен дисплеем более высокого разрешения с повышенной частотой обновления ***(Facebook разрабатывает приложения для виртуальной реальности // InternetUA (http://internetua.com/Facebook-razrabativaet-prilojeniya-dlya-virtualnoi-realnosti). – 2015. – 20.02).***

***

Во всемирной паутине появится новая социальная сеть. Очередной Facebook на этот раз будет создан специально для мертвецов. Группа итальянских энтузиастов открыла кампанию по сбору средств на разработку мобильного приложения под названием RipCemetery на краудфандинговой платформе Indiegogo. Об этом сообщает Gizmodo.

Разработчики из Италии собрались создать первую в мире социальную сеть-кладбище. Благодаря новому приложению пользователи смогут создавать целые фамильные склепы в виртуальном мире. На «могилах» можно будет оставлять цветы, публиковать фотографии, видео и сообщения. Кроме того, в соцсети разрешат возводить «гробницы» для домашних питомцев. Пока не совсем ясно, будут ли у кошечек и собачек собственные поминальные аккаунты или же и для них найдется место в семейной «усыпальнице».

Главный разработчик приложения Д. Витали рассказал, почему решился на создание приложения: «Мой двоюродный брат, который был очень близким мне человеком, умер очень молодым, а семья решила его кремировать. Поэтому я не мог навещать его, когда мне этого хотелось. Вот я и придумал способ, как навещать брата в любой момент при помощи мобильного устройства».

Авторы социальной сети пообещали, что программа будет доступна на Andriod, Windows и iOS-устройствах. Следует отметить, что пока идея не вызвала у пользователей большого энтузиазма. Из запланированных 23 тыс. дол. удалось собрать только 579 дол. Перспектива создания виртуальной могилы людей не привлекла, а, напротив, шокировала. Не помогает пока даже рекламное видео, выложенное итальянцами на YouTube ***(Разработчики создадут первый в мире «Фейсбук для мертвецов» // InternetUA (http://internetua.com/razrabotcsiki-sozdadut-pervii-v-mire--feisbuk-dlya-mertvecov). – 2015. – 17.02).***

***

Facebook тестирует приложение с элементами «вещественного» дизайна

Приложение Facebook долгое время вызывало недовольство тех, кому хотелось бы единообразия дизайна Android-приложений. Но крупнейшая социальная сеть идёт своим путём и довольно медленно меняет направление движения. Тем не менее, небольшое число пользователей получили обновлённую версию популярного социального приложения, в котором чувствуется по крайней мере небольшое влияние так называемого «вещественного» дизайна (концепции построения и оформления пользовательских интерфейсов современных приложений и сайтов Google).

В частности, появилась плавающая кнопка действий. До полного переосмысления Facebook для Android в рамках рекомендаций Google ещё далеко, но в приложении, например, исчезла нижняя панель. Появление кнопки действий как раз и позволило избавиться от нижней панели, с которой знакомы текущие пользователи мобильной версии Facebook.

Нажимая появившуюся в «вещественной версии» Facebook кнопку, пользователь теперь может выбрать привычные варианты действий: «Статус», «Фото», «Где вы». Такой подход позволяет эффективнее использовать пространство экрана, выводя на него больше полезной информации и меньше элементов управления (хотя требует для совершения действия выполнить два прикосновения, а не одно).

Речь идёт, по-видимому, об изменениях интерфейса Android-приложения Facebook на стороне сервера – дело в том, что файлы APK у пользователей обновлённой версии ничем не отличаются от текущей сборки приложения. Стоит добавить, что эти изменения могут так и не стать общедоступными – Facebook постоянно экспериментирует с различными интерфейсами, и далеко не все эти эксперименты получают широкое

распространение ***(Facebook тестирует приложение с элементами «вещественного» дизайна // InternetUA (http://internetua.com/Facebook-testiruet-prilojenie-s-elementami--vesxestvennogo--dizaina). – 2015. – 16.02).***

***

Топ-менеджер соцсети Facebook рассказал об анализе поведения пользователей и планах относительно медиа-контента, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-otricaet-puzyr-filtrov-i-prizyvaet-smi-otdavat-emu-stati-43329/).

Facebook хотел бы договориться с изданиями о публикации их материалов прямо в социальной сети. Это поможет ускорить отображение информации в мобильных приложениях Facebook, сделать чтение более удобным, и в конечном итоге должно подарить СМИ больше внимания аудитории. Об этих планах рассказал директор по продукту Facebook К. Кокс на конференции Code/Media.

К. Кокс заявил, что понимает беспокойство издателей и их нежелание отдавать свой контент посторонним сайтам, и Facebook пока находится в поисках оптимальной модели сотрудничества. Однако с тем, что людям неудобно читать статьи на мобильных устройствах, тоже нужно что-то делать.

Интересно вспомнить, как еще в 2012 г. «ВКонтакте» позаботился о том, чтобы его пользователям удобно было читать материалы СМИ, и включил предпросмотр публикаций. Благодаря этой функции статья по ссылке открывалась в отдельном слое внутри соцсети, без перехода на страницу СМИ. Эта инициатива понравилась не всем изданиям, но со временем соцсеть достигла баланса интересов пользователей и издателей.

К. Кокс также рассказал об успехах Facebook как видеоплатформы – функция автоматического запуска видео в ленте оказалась крайне удачна, приносит много просмотров и стимулирует пользователей делиться видео. Возможность для создателей видео монетизировать его, как на YouTube, Facebook пока не рассматривает.

Несмотря на внимание к медийному контенту Facebook намерен оставаться в первую очередь средством связи людей с родными и друзьями. Соцсеть внимательно следит за тем, какой контент важен пользователям. Лайки и клики по ссылкам не являются достаточно точным способом понять отношение к постам. Facebook намерен более глубоко изучать паттерны взаимодействия людей с информацией и не ориентироваться на очевидные метрики поведения в Интернете.

Это, впрочем, не новость – в Facebook достаточно давно поняли, что алгоритмами анализа обратной связи и машинным обучением обойтись не получится («это дорого и долго», ранее отмечал К. Кокс). У компании есть фокус-группа, которая началась с 30 человек, разрослась до 600 и в ближайшем будущем увеличится до нескольких тысяч. Ее участники видят специальную версию Facebook с неранжированными записями, о каждом из

которых они должны ответить на восемь вопросов вида «важен ли вам герой поста», «хотите ли вы видеть такое в ленте», а также написать микроэссе о своих чувствах и мыслях по поводу этого поста. Кроме того, участников фокус-группы периодически интервьюируют сотрудники Facebook.

На конференции Code/Media К. Кокс высказался также об эффекте «пузыря фильтров», который алгоритмы рекомендации предположительно создают вокруг пользователя, искусственно ограничивая круг его интересов несколькими темами и гарантированно комфортными для него точками зрения.

«Основная масса контента, который вы видите на Facebook, производится вашими «слабыми связями», пользователями, с которыми вы не взаимодействуете вне соцсети. Наши исследования не доказывают, что Facebook создает пузырь фильтров, зато предоставляют некоторые свидетельства обратного» ***(Facebook отрицает пузырь фильтров и призывает СМИ отдавать ему статьи // Marketing Media Review (http://mmr.ua/news/id/facebook-otricaet-puzyr-filtrov-i-prizyvaet-smi-otdavat-emu-stati-43329/). – 2015. – 20.02).***

***

Сервис микроблогов Twitter представил своим пользователям новую функцию – возможность публиковать на своих страницах не только фото, но и видео.

Сообщение о новой функции администрация Twitter разослала в письмах своим пользователям.

Из письма Twitter пользователям: «Представляем функцию видеосъемки в Twitter. Запечатлейте самые важные моменты вашей жизни на видео в Twitter и покажите их всему миру».

Чтобы разместить видео с помощью гаджета, оснащенного видеокамерой, нужно нажать специальную кнопку, после чего ролик будет опубликован в микроблоге.

Ранее возможность добавлять видео появилась в социальных сетях Facebook и Instagram ***(Twitter разрешил пользователям публиковать видеоролики // Телекомпанія НТВ (http://www.ntv.ru/novosti/1327556/). – 2015. – 21.02).***

***

Twitter намекнул на масштабный редизайн в 2015 г.

По словам представителей Twitter, сервис микроблогов по-разному воспринимается новичками и опытными блогерами, поэтому в ближайшем будущем компания собирается адаптировать его под разные аудитории, упростив его использование. Об этом сообщает TechCrunch.

Как рассказали TechCrunch вице-президент по продукту Twitter К. Вейл и вице-президент по разработке А. Роттер, в настоящее время в компании

продолжается работа над тем, как сделать сервис более полезным для пользователей-новичков.

«Пользователи Twitter, которые смогли зарегистрироваться и подписаться на нужных людей, рассказывают о том, насколько неоценимым для них становится сервис. Но мы с Кевином сфокусированы на том, чтобы делать продукты, которые позволят каждому дойти до такого состояния», – делится А. Роттер, вице-президент по разработке Twitter.

А. Роттер говорит о распространённой проблеме слишком высокого порога вхождения. Для того, чтобы получить максимум от Twitter, пользователю нужно не только зарегистрироваться, но и найти интересные аккаунты, которые он будет читать, а также изучить то, как работает поиск, хэштеги и разделы вроде Discover («В курсе»), чтобы получать максимально релевантный контент.

«Я нашёл [новость о землетрясении] в Twitter за полчаса до того, как я увидел это где-либо ещё, но мне потребовалось поработать над этим. Мне нужно было знать правильный поисковый запрос и всё такое. На самом деле я просто хочу, чтобы мой телефон прислал мне push-уведомление, как только Twitter становится известно что-то интересное для меня», – утверждает А. Роттер.

По информации корреспондента TechCrunch, в Twitter уже тестируют новую главную страницу в виде сетки, а не одноколоночной ленты. Однако представители компании опровергают популярное мнение о том, что сервис микроблогов следует за алгоритмом новостей Facebook и собирается уйти от хронологической манеры отображения записей. По словам К. Вейла, эта функция «критична» для Twitter и будет оставаться таковой.

Кроме того, в комплекс изменений, запланированных в Twitter, входят в том числе «мгновенные ленты», считает автор TechCrunch. В начале февраля корреспондет газеты The New York Times рассказывал о новой функции, тестируемой в приложении Twitter для Android. Просканировав его список контактов на телефоне при регистрации, сервис предложил ему читать «мгновенную ленту» (instant timeline) из аккаунтов на основе его интересов, не требуя на них подписываться.

Представители Twitter также намекнули, что недавнее появление групповых чатов является лишь первым среди запланированных нововведений, связанных с личными сообщениями. Согласно источникам TechCrunch, сервис тестирует возможность прямой связи между брендами и пользователями, что позволит получать оперативные ответы на вопросы и быстрее оказывать услуги ***(Twitter намекнул на масштабный редизайн в 2015 году // InternetUA (http://internetua.com/Twitter-nameknul-na-masshtabnii-redizain-v-2015-godu). – 2015. – 24.02).***

***

Глава развития контента YouTube Р. Кинкл утверждает, что видео-сервис ускорил темпы роста, несмотря на конкуренцию со стороны Facebook и других компаний.

В настоящее время YouTube тестирует новую тактику, позволяющую лучше вознаградить своих лучших создателей контента. Р. Кинкл отметил рекламную платформу Google Preferred, позволяющую создателям видео использовать объявления, которые не могут быть пропущены. Участники этой программы увидели рост доходов на 70 % в годовом исчислении в отличие от 50 % у партнеров YouTube.

В этом году YouTube расширит программу для 11 новых рынков, а позднее – и для всего мира.

«То, что мы наблюдаем сейчас, – площадка действительно начинает развиваться», – заявил генеральный директор United Talent Agency Д. Зиммер. Он также прокомментировал видеопродукт от Facebook: «Я думаю, что у Facebook большие возможности, потому что сеть имеет огромную аудиторию, и люди любят и доверяют ей».

Директор United Talent Agency считает, что рекламодателям все еще не хватает правильной аналитики, чтобы помочь принять правильное решение о выборе платформы.

Р. Кинкл в свою очередь говорит, что в цифровом видео есть место для нескольких крупных игроков, помимо YouTube: «Есть несколько компаний, которые растут так же быстро, как мы. Мы ожидали замедления бизнеса, но он на самом деле ускорился».

Данные аналитической компании Socialbakers свидетельствуют о том, что бренды теперь загружают больше видео непосредственно в Facebook, минуя YouTube ***(YouTube ускорил темпы роста, несмотря на увеличение конкуренции со стороны Facebook // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/youtube_uskoril_tempy_rosta_nesmotrya_na_uvelichenie_konkurentsii_so_storony_facebook). – 2015. – 24.02).***

***

Google в официальном блоге своего видеохостинга заявила о выходе специального приложения YouTube для детей на iPhone и iPad – YouTube Kids.

Ключевые отличия YouTube for Kids от «взрослой» версии заключаются в существенно упрощенном интерфейсе, фильтрации контента, ориентированного на детскую аудиторию, а также дополнительных настройках родительского контроля.

Главный экран приложения состоит из четырех вкладок – Shows (Шоу), Music (Музыка), Learning (Обучение) и Explore (Развитие навыков). Первые две категории состоят из развлекательного контента, а в двух других превалируют видео образовательного содержания.

Функции родительского контроля позволяют настроить то, как ребенок будет проводить время в приложении. Можно выставить таймер на определенное количество времени, по истечении которого программа автоматически заблокируется. Среди доступных параметров есть возможность отключить звук в видео и запретить поиск роликов, предоставив ребенку доступ только к рекомендованому контенту ***(YouTube Kids вышел на iOS // iPhone и iPad Украина (http://ukrainianiphone.com/23/02/2015/211510). – 2015. – 24.02).***

***

Google разберет свою соцсеть на части и запустит рекламу в Google Play

Старший вице-президент по продуктам Google С. Пичай в интервью Forbes сказал, что общение (мессенджер Hangouts), работа с фотографиями и поток новостей, которые сейчас объединены в соцсети Google+, могут быть разведены по отдельным продуктами. Топ-менеджер не согласился с популярным мнением, что соцсеть стала провальным проектом для Google. По его словам, Google+ отлично справляется со своей главной задачей – держать пользователя залогиненным во все сервисы Google, обеспечивать их связь и «единую идентичность сквозь все продукты», пишет Marketing Media Review (http://mmr.ua/news/id/google-razberet-svoju-socset-na-chasti-i-zapustit-reklamu-v-google-play-43419/).

Google очень хотел бы вернуться на китайский интернет-рынок и думает, как это сделать. В стране крайне популярны телефоны на Android, но на этих устройствах нет сервисов Google – карт, почты, магазина Play и других. Доступ к Google Play особенно интересует китайских разработчиков приложений ***(Google разберет свою соцсеть на части и запустит рекламу в Google Play // Marketing Media Review (http://mmr.ua/news/id/google-razberet-svoju-socset-na-chasti-i-zapustit-reklamu-v-google-play-43419/). – 2015. – 27.02).***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Українці через соцмережі просять Президента П. Порошенка, Прем'єр-міністра А. Яценюка та голову НБУ В. Гонтареву пояснити, що нині відбувається в економіці держави.

Користувачі Facebook розпочали флеш-моб: вони фотографуються з аркушами паперу, на яких написано «Порошенко, поясни, що відбувається!», «Гонтарева, поясни, що відбувається!» та «Яценюк, поясни, що відбувається!», інформує «Вголос».

У такий спосіб люди закликають керівників держави поговорити з народом про ситуацію в державі.

Як відомо, останнім часом в Україні офіційний курс гривні до долара США є в межах 28–29 грн/дол., а в обмінниках валюту взагалі продають по 40 грн за долар. У вівторок, 24 лютого, під стіни Національного банку України активісти принесли автомобільні шини і залізні бочки ***(Українці через соцмережі просять Президента, прем'єра та голову НБУ пояснити, що відбувається в економіці держави // Новини Кіровоградщини (http://novosti.kr.ua/news/ukranci-cherez-socmerezhi-prosyat-prezidenta-premera-ta-golovu-nbu-poyasniti-shho-vidbuvaetsya-v-ekonomici-derzhavi.html). – 2015. – 25.02).***

***

Одинадцятий рік поспіль німецька медіа-компанія Deutsche Welle нагороджуватиме найкращі інтернет-проекти та активістів з різних країн світу.

Номінувати можна інтернет-сторінки різних форматів – блоги, мікроблоги, Facebook-сторінки, веб-сайти, YouTube-канали, подкасти та інше.

Для участі в конкурсі The Bobs приймаються проекти, написані однією з 14 мов: українською, англійською, арабською, бенгальською, гінді, індонезійською, іспанською, китайською, німецькою, перською, португальською, російською, турецькою або французькою.

Цього року Deutsche Welle вперше вручить приз «За свободу слова». Міжнародне журі та інтернет-користувачі вирішать, які проекти здобудуть інші призи.

Переможців конкурсу обиратимуть у трьох нових номінаціях: «Найкраща соціальна ініціатива в мережі», «Безпека й захист особистих даних», «Мистецтво та медіа». У цих номінаціях конкуруватимуть проекти з різних країн. Переможців визначатиме міжнародне журі. Україну в журі The Bobs представляє директор Інституту масової інформації О. Романюк.

У номінації «Найкраща соціальна ініціатива в мережі» журі обере проект, який використовує можливості цифрових комунікацій, аби прискорити позитивні зміни в суспільстві. Наприклад, у сфері освіти, рівноправ'я, охорони здоров'я, довкілля та ін.

Для номінації «Безпека й захист особистих даних» розшукуються рішення у сфері програмного забезпечення або сайти, які допомагають інтернет-користувачам захищати особисті дані та приватну сферу. Наприклад, за допомогою зручних мобільних додатків (apps) або докладного інформування. Інструменти, які дають змогу ефективно оминати цензуру в Інтернеті, теж пасують у цю номінацію.

«Мистецтво та медіа». Тут нагородять проект, який видатним чином використовує засоби цифрової комунікації, щоб мистецьки інтерпретувати важливі суспільні теми. Шанси на успіх також мають ініціативи, які сприяють інноваційному використанню інформації в мас-медіа – наприклад, зі сфери громадянської журналістики та журналістики даних.

Для кожної мови конкурсу є окрема номінація: «Вибір користувачів: найкраща сторінка…» (українською, англійською, німецькою, китайською та іншими мовами – загалом 14). Інтернет-користувачі подають свої пропозиції до 12 березня на сайті конкурсу. Потім член журі, який відповідає за кожну мову, обирає п'ятьох фіналістів. Переможців у мовних номінаціях обирають виключно інтернет-користувачі під час відкритого онлайн-голосування на сайті The Bobs. Голосування стартує 9 квітня.

Також уперше вручить приз «За свободу слова». Його отримає особистість або ініціатива, яка особливим чином захищає в Інтернеті право людей на вільне висловлювання думок.

Переможці трьох міжнародних номінацій будуть запрошені на церемонію нагородження, яка відбудеться 23 червня 2015 р. під час медіа-конференції Deutsche Welle Global Media Forum у Бонні ***(Розпочався The Bobs 2015: конкурс для інтернет-активістів // Високий Вал (http://newvv.net/culture/Culture/237630.html). – 2015. – 23.02).***

***

Міністерство інформаційної політики запустило сайт під назвою «Інформаційні війська України», який закликає волонтерів долучатися до інформаційної боротьби, пише Західна інформаційна корпорація (http://zik.ua/ua/news/2015/02/23/mininformpolityky_zapustylo_sayt_pid_nazvoyu_informatsiyni_viyska_ukrainy_567021).

«Кожен українець із доступом до Інтернету може зробити свій внесок в інформаційну боротьбу», – сказано на сайті.

У повідомленні додається, що «зараз прийшов час дати відсіч російським окупантам і на інформаційному фронті».

Потенційних волонтерів закликають ретельно виконувати отримані після реєстрації завдання та щодня приділяти час інформаційній боротьбі, повідомляє «Українська правда» ***(Мінінформполітики запустив сайт під назвою «Інформаційні війська України» // Західна інформаційна корпорація (http://zik.ua/ua/news/2015/02/23/mininformpolityky_zapustylo_sayt_pid_nazvoyu_informatsiyni_viyska_ukrainy_567021). – 2015. – 23.02).***

***

Іранська журналістка М. Алінеджад отримала міжнародну нагороду у сфері прав людини за створення популярної сторінки у Facebook. У ній вона, всупереч ортодоксальним традиціям, заохочує співвітчизниць розміщувати свої знімки без хіджабу (чадри).

На Женевському саміті з прав людини та демократії група 20 неурядових організацій вручила М. Алінеджад нагороду за права жінок, повідомила The Guardian.

Цим було відзначено заслуги журналістки, яка «надала голос тим, хто його не має, збудила совість людства, підтримавши боротьбу іранських жінок за основні права людини, свободу і рівність».

М. Алінеджад сказала, що нагорода сприятиме кращому розумінню у світі життя й боротьби її співвітчизниць.

«Від 7-річних школярок до 70-річних бабусь їх змушують носити хіджаб, – мовиться в заяві журналістки, опублікованій у мережі. – Сподіваюся, ця нагорода сприятиме тому, що їхні протестні голоси відгукнуться в ООН».

38-річна М. Алінеджад створила сторінку «Непомітні свободи іранських жінок» (Stealthy Freedoms of Iranian Women) у Facebook у травні минулого року. Нині її сторінка у Facebook має більше ніж 760 тис. підписників.

Раніше М. Алінеджад вже отримала низку міжнародних нагород ***(Іранську журналістку нагородили за жіночу сторінку у Facebook // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/social/iransku_zhurnalistku_nagorodili_za_zhinochu_storinku_u_facebook/). – 2015. – 25.02).***

***

Испанские политики используют приложение WhatsApp для предвыборной агитации, сообщает The Guardian.

Мэр испанского города Б. Иглесиас стал одним из первооткрывателей нового способа политической агитации. В рамках своей кампании под слоганом «Позвоните или напишите на мой номер» Б. Иглесиас раздал номер своего телефона жителям города.

«Я получил несколько сообщений с критикой моих действий. Но ведь для этого мы здесь – слушать людей», – подчеркнул градоначальник. По его словам, сообщения поступают постоянно, с шести часов утра до часа ночи.

Идею мэра переняли политики по всей стране. Они считают, что общение такого рода сближает их с избирателями и помогает решать многие муниципальные проблемы ***(Испанские политики агитируют избирателей по WhatsApp // InternetUA (http://internetua.com/ispanskie-politiki-agitiruuat-izbiratelei-po-WhatsApp). – 2015. – 18.02).***

***

В Татарстане спасли десятки людей благодаря социальной сети, которая объединяет доноров крови. Создал ее местный энтузиаст, вдохновленный примерами М. Цукерберга и П. Дурова. Раньше редкого донора могли искать неделями, это ставило под угрозу жизнь пациента, особенно если требовалось срочное переливание. Теперь процесс значительно упростился.

Житель Казани Р. Шекуров по привычке заходит в Интернет, чтобы убедиться, что созданная им соцсеть доноров крови работает без перебоев.

Этот ресурс уже объединил несколько тысяч человек – тех, кому срочно нужно переливание и тех, кто может в этом помочь.

Через две недели 11-классницу Юлю врачи обещают выписать домой, позади сложнейшая операция по замене клапана сердца, сопровождаемая переливанием крови, которую персонально для Юли сдавали сразу пять доноров, найденных через Интернет.

Как выяснил корреспондент НТВ М. Чернов, соцсеть, спасающую жизни, придумал Р. Шекуров, который не может быть донором по медицинским показаниям. Единственная попытка сдать кровь в 18 лет закончилась обмороком. О славе создателей Facebook и Twitter скромный казанский аспирант не грезил, но спустя 10 лет после не самого удачного посещения центра крови создал соцсеть, которая уже объединила десятки тысяч российских и иностранных доноров ***(Соцсеть доноров крови помогает спасать человеческие жизни // Телекомпанія НТВ (http://www.ntv.ru/novosti/1336797/). – 2015. – 26.02).***

***

У Запоріжжі активісти розпочали в соцмережах флеш-моб, спрямований на протидію панічним настроям серед населення, що спровоковані падінням курсу гривні. На сторінці акції розміщені плакати із закликами до припинення ажіотажу на продовольчому ринку, передає «Радіо Свобода».

«Ми самі у цьому винні, бо купуючи зайві 10 кілограмів цукру, ми призводимо до того, що продавці цього цукру, які бачать такий попит, піднімуть ціну на нього вдвічі», – розповів один з організаторів акції Ю. Хохлов.

У планах у активістів розмістити аналогічні, але паперові плакати в громадських місцях Запоріжжя.

«Окрім того, що ми поширюємо такі оголошення у Facebook, просимо перепост, ми такі оголошення по всіх зупинках, по магазинах будемо вивішувати. Коли написано “Стоп паніка”, це говорить про те, що ми не піддаємося паніці. Візуалізація цієї акції трохи заспокоює людей. Коли люди звичайні, не якісь лідери наші київські говорять один одному “Стоп”, люди дійсно зупиняються», – каже Ю. Хохлов.

У Запоріжжі та багатьох інших українських містах нині панує продовольчий ажіотаж, люди активно розкуповують у магазинах харчі тривалого зберігання – крупи, цукор, борошно ***(Активісти розпочали у Facebook флеш-моб «Стоп паніка» // Львівський портал (http://portal.lviv.ua/news/2015/02/26/105854.html). – 2015. – 26.02).***

***

У соціальній мережі Facebook з’явилася спеціальна сторінка допомоги для людей, які думають про суїцид, пише Корреспондент.net

(http://ua.korrespondent.net/business/web/3484558-Facebook-vriatuie-samohubtsiv).

Facebook, Forefront та Національна гаряча лінія запобігання самогубствам розробили спеціальну віртуальну допомогу для засмучених і пригноблених людей, повідомляє Time. Тепер кожен схильний до суїцидальних думок користувач може отримати підтримку в режимі онлайн.

Процес відстеження суїцидальних і тривожних настроїв Facebook почав ще у 2011 р. Тепер же мережа значно допрацювала свій проект і спростила процес подачі звернень для тих, хто цього потребує.

Користувачі також зможуть самі ідентифікувати пости з тривожним змістом. Над кожним постом Facebook доступна кнопка «Повідомити модератору», з набором опцій на вибір: повідомити зацікавленому користувачеві або ж звернутися за допомогою по гарячій лінії.

У США ця функція запрацює найближчим часом, а в найближчі кілька місяців виявлять схильних до суїциду людей і допомагати їм зможуть і в інших країнах ***(Facebook «врятує» самогубців // Корреспондент.net (http://ua.korrespondent.net/business/web/3484558-Facebook-vriatuie-samohubtsiv). – 2015. – 26.02).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Социальная сеть «ВКонтакте» 16 февраля запустила мобильную рекламу в собственных приложениях на базе iOS, рассказал Roem.ru евангелист «ВКонтакте» А. Усманов. Рекламодателям очень не хватало возможности размещать рекламу в мобильных приложениях для iOS, добавил он.

По мнению представителей социальной сети с помощью нововведения рекламодатели смогут охватить практически всех iOS-пользователей в российском сегменте Интернета. «Мы будем постепенно увеличивать рекламный инвентарь в iOS-приложениях социальной сети. Ожидаем, что этот процесс займет около двух недель» – добавил А. Усманов.

Реклама появилась в приложении после обновления до новой версии, вышедшей 11 февраля: «ВКонтакте» удалил из нее раздел музыки и, как выяснилось, добавил таргетированную рекламу.

Через браузер мобильную версию социальной сети посещают более 30 млн пользователей в сутки. Из них около 20 млн – пользователи Android и 10 млн – iOS. Ежедневно 35 % пользователей можно охватить только с помощью мобильных устройств, следует из данных соцсети.

«ВКонтакте» начал раскатывать мобильную рекламу в октябре 2014 года – вначале ее получили пользователи мобильных веб-версий на Android и iOS, а также пользователи приложения под Android ***(«ВКонтакте» добавил трафика мобильным рекламодателям //***

МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42461/118/lang,ru/). – 2015. – 17.02).

***

Приватбанк оголосив про припинення роботи та комунікації з клієнтами в російській соціальній мережі «ВКонтакте».

Відповідний запис зявився в офіційній спільноті банку кілька днів тому. З того часу спільнота більше не оновлювалась. Представники банку в коментарі для Watcher підтвердили нам інформацію про припинення роботи у «ВКонтакте». Натомість користувачам запропонували приєднатись до спільнот в інших соцмережах – Facebook і Twitter ***(Приватбанк закрив свою спільноту у Вконтакті // UkrainianWatcher (http://watcher.com.ua/2015/02/16/pryvatbank-zakryv-svoyu-spilnotu-u-vkontakti/). – 2015. – 16.02).***

***

В ленте Facebook все чаще можно заметить рекламные посты с использованием синемаграфики, сообщает AdWeek.

Синамеграфика – фотография, показывающая движение в отдельной части изображения, своего рода гибрид фото и видео – может стать отличным маркетинговым инструментом.

Facebook не поддерживает популярный на других площадках формат GIF, однако синемаграфики можно загружать как видео, и они будут прокручиваться в режиме автозапуска, заставляя пользователей остановиться и обратить внимание на ваш пост.

Возможно, в ближайшее время синемаграфика доберется и до Instagram, в котором недавно появилась функция бесконечной прокрутки видео ***(Facebook нашел замену GIF // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_nashel_zamenu_gif). – 2015. – 16.02).***

***

Pinterest готовит запуск кнопки buy (купить), которая позволит пользователям приобретать товары прямо в социальной сети. Ожидается, что кнопка будет запущена в течение ближайших трех-шести месяцев, также возможен вариант ограниченного тестирования.

В соцсети уже есть товарные пины (Product pins) с изображениями одежды, товаров, мебели и дополнительной информацией о цене, наличии и магазинах, где можно приобрести данный товар. Они даже позволяют пользователям получать уведомления о снижении цен.

Отметим, что кнопку «купить» ранее запустили такие социальные сети, как Twitter и Facebook ***(Pinterest готовит запуск кнопки «купить» // МедиаБизнес***

(http://www.mediabusiness.com.ua/content/view/42447/118/lang,ru/). – 2015. – 16.02).

***

«Первый канал» договорился о легализации своего контента в крупнейшей российской социальной сети «ВКонтакте», пишет Marketing Media Review (http://mmr.ua/news/id/krupnejshij-rossijskij-telekanal-legalizuet-video-v-socialnoj-seti-vkontakte-43283/).

«Первый канал» вступил в партнерство с «ВКонтакте» по размещению своего контента в социальной сети, рассказал «Ъ» руководитель дирекции интернет-вещания «Первого канала» И. Булавинов. Соглашение рассчитано на год с правом пролонгации. В сети «ВКонтакте» будут размещаться лицензированные видео проектов, правами на онлайн-показ которых распоряжается «Первый канал», в том числе «Вечерний Ургант», «Пусть говорят», КВН, «Здоровье», «Пока все дома», «Точь-в-точь», «Ледниковый период», «Познер», «Что? Где? Когда?», «Пока все дома», «Человек и закон». «ВКонтакте» будет получать архивные записи передач, а также их новые поступления сразу после эфиров. Нелегально размещенные видео «Первого канала» в социальной сети будут заменяться на лицензированные. Проект будет реализован через дистрибуционную онлайн-платформу Pladform.

В рамках партнерства «ВКонтакте» и «Первый канал» будут делить доходы от показа рекламы в роликах телеканала в социальной сети. В какой пропорции будет делиться выручка, стороны не раскрывают. Как правило, в подобных соглашениях речь идет о паритетном разделении, говорит собеседник «Ъ» на рынке онлайн-видео ***(Крупнейший российский телеканал легализует видео в социальной сети ВКонтакте // Marketing Media Review (http://mmr.ua/news/id/krupnejshij-rossijskij-telekanal-legalizuet-video-v-socialnoj-seti-vkontakte-43283/). – 2015. – 18.02).***

***

Хотите увеличить охват на Facebook? Забудьте про фото

Время фотографий в Facebook прошло. К такому выводу пришла аналитическая компания Socialbackers, пишет Marketing Media Review (http://mmr.ua/news/id/hotite-uvelichit-ohvat-na-facebook-zabudte-pro-foto-43273/).

Исследовав более 670 тыс. постов с 4445 страниц брендов (исключая знаменитостей, развлекательные и медиа-страницы) в период с октября по февраль 2015 г., Socialbackers обнаружила, что органический охват видеопостов составляет 8,71 %. У фотопостов ситуация хуже – всего 3,73 %, при этом органический охват текстовых статусов – 5,77 %, а постов со ссылками – 5,29 %.

Для маркетологов это не должно стать неожиданностью. Видео на Facebook показало огромный рост с июня 2014 г. В ноябре М. Цукерберг заявил, что через пять лет большую часть контента на Facebook будет

составлять видео, а в прошлом месяце он сказал, что посты с видео получают более 3 млрд просмотров в день.

А ведь совсем недавно – в апреле прошлого года – Socialbackers опубликовала исследование, в котором говорилось, что 75 % постов, размещаемых брендами, содержат фото и именно они обеспечивают максимальную вовлеченность – 87 % взаимодействий.

И, несмотря на заметное падение охвата у фотографий, посты с ними по-прежнему превалируют, сообщает Socialbackers.

Данные Socialbackers также показывают, что бренды стали продвигать еще больше постов. В 2013 г. продвигалось всего 9 % постов, а в IV квартале 2014 г. – 17 %.

У фотопостов результат был еще хуже в случае со страницами, у которых более 100 тыс. лайков.

Тем не менее эти данные вовсе не означают, что пора прекращать постить фотографии в Facebook. Убедительные изображения продолжают хорошо воздействовать на аудиторию, просто теперь нужно еще внимательнее относиться к выбору фотографий для поста ***(Хотите увеличить охват на Facebook? Забудьте про фото // Marketing Media Review (http://mmr.ua/news/id/hotite-uvelichit-ohvat-na-facebook-zabudte-pro-foto-43273/). – 2015. – 17.02).***

***

Глобальная соцсеть Facebook представила новый инструмент для продвижения продукции компаний, с помощью которого реклама каждого конкретного товара будет показываться соответствующей аудитории, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-anonsiroval-novuju-funkciju-dlja-reklamy-tovarov-43287/).

«Многие компании продают больше, чем один продукт. И если вашему бизнесу необходима реклама множества наименований, вы можете столкнуться с трудностями в продвижении такого разнообразия. Как же выгодно представить ваш широкий ассортимент? Как донести сообщение о конкретной единице нужной аудитории? Мы представляем product ads – решение, призванное помогать рекламодателям продвигать весь спектр их товаров на всех пользовательских устройствах», – говорится в сообщении социальной сети.

Новый инструмент предлагает компаниям несколько способов продвижения разнообразных продуктов в Facebook. Рекламодатели могут загружать целые товарные каталоги и создавать кампании, таргетируя рекламу каждой конкретной позиции на свою целевую аудиторию, или же позволить самой социальной сети автоматически показывать людям предложения, релевантные их интересам. Предлагаемая продукция может быть размещена в виде как одиночных, так и мультитоварных объявлений.

Компании при этом получают такие опции, как автоматическое расширение аудитории до всех, кто заходит на сайт / в приложение

рекламодателя или обладает релевантным кругом интересов, либо находится в нужной локации и т. д.; размещение мультипродуктового объявления, описывающего разные преимущества одного товара; усиление продвижения позиций, получивших множество просмотров на сайте / в приложении компании, либо освещение лучших продаж ***(Facebook анонсировал новую функцию для рекламы товаров // Marketing Media Review (http://mmr.ua/news/id/facebook-anonsiroval-novuju-funkciju-dlja-reklamy-tovarov-43287/). – 2015. – 18.02).***

***

Facebook добавляет новую метрику в рекламные отчеты – Показатель релевантности (Relevance Score), которая поможет рекламодателям лучше оценивать свои объявления.

Показатель релевантности основан на прогнозе Facebook – система рассчитывает, сколько позитивных (целевые действия) и негативных (блокировка объявлений) взаимодействий от таргетируемой аудитории получит реклама. Чем больше положительных взаимодействий ожидается, тем выше данный показатель для объявления.

Показатель варьируется от 1 до 10 и постоянно обновляется в зависимости от взаимодействий пользователей с рекламой.

Почему данный показатель важен:

– он может уменьшить стоимость объявления;

– он может помочь рекламодателям в тестировании разных таргетинговых опций перед запуском кампании;

– он может помочь оптимизировать кампании, которые уже запущены.

Facebook особо подчеркивает, что показатель релевантности не должен быть главной метрикой для оценки успешности кампании. Как и прежде, главным фактором успеха являются ставки, основанные на бизнес-целях кампании ***(В Facebook появился показатель релевантности объявлений // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/v_facebook_poyavilsya_pokazatel_relevantnosti_obyavleniy). – 2015. – 18.02).***

***

Google Inc. готовит к запуску модель платной подписки для принадлежащего ей сервиса онлайн-видео YouTube. Как сообщил директор по контенту и бизнес-операциям YouTube Р. Кинкл, новая схема будет внедрена через несколько месяцев, передает rbc.ru

YouTube в течение некоторого периода времени занималась прорабатывала платную схему показа и бесплатную схему с рекламой. В мае 2013 г. компания запустила пилотную программу, позволившую отдельным создателям контента привлекать абонентскую плату с пользователей за доступ к определенному видеоканалу.

В пилотном варианте приняли участие 53 канала, в том числе Digital Theatre, DHX Kids TV, Hombre Pix, On Cue, Rap battle network, TYTplus. Стоимость подписки – от 0,99 дол. в месяц ***(Google готовит к запуску модель платной подписки на YouTube // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42498/118/lang,ru/). – 2015. – 19.02).***

***

Facebook открыл свою рекламную платформу для большего количества партнеров.

Facebook подключил новые агентства и бренды к своей рекламной платформе Atlas, запущенной прошлой осенью. Партнерами компании стали группа Publicis и ее подразделение VivaKi, а также специализирующиеся на рекламных технологиях Mediaocean и Merkle. Выбор дает представление о планах по развитию Atlas. Сильные эксперты должны помочь Facebook выстроить успешную цифровую экосистему.

Ранее партнерами платформы стали Havas Media Group и Omnicom Media Group. Сервис Facebook обещает клиентам охват пользователей на различных устройствах, сближение онлайновых и оффлайновых действий покупателей на основе собственной базы данных. Такой подход заменил cookies, которые были самым популярным способом подобрать и измерить рекламу ***(Publicis подключилась к Atlas // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/publicis_podklyuchilas_k_atlas). – 2015. – 19.02).***

***

Facebook рассказал, как он считает показы рекламы

Facebook засчитывает просмотр объявления, только когда оно появляется на экране устройства пользователя. Если пользователь не видел объявление, значит – просмотр не должен фиксироваться. Такую позицию занимает Facebook в отношении рекламы, которая демонстрируется в соцсети, говорится в официальном блоге компании, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-rasskazal-kak-on-schitaet-pokazy-reklamy-43322/).

Facebook проводит четкую грань между так называемыми served и viewed показами объявлений. Засчитывая served показы, система фиксирует, сколько раз объявление отобразилось на странице, но видел ли его пользователь, уже неважно – а объявление могло отобразиться в нижней части страницы, или пользователь вообще ушел со страницы, а оно не загрузилось полностью. В свою очередь viewed показ означает, что объявление отобразилось на экране пользователя, и он точно его успел посмотреть.

Именно viewed показы объявления – это то, к чему должен двигаться рынок. По словам Facebook, в таком подходе есть свои преимущества:

Ценность. Исследования Facebook показывают, что реклама может оказать влияние на пользователя, даже если он видел часть объявления в течение короткого промежутка времени.

Целостность. Такой стандарт измерения применяется ко всем устройствам, интерфейсам и типам объявлений, что позволяет с легкостью проводить кросс-платформенные измерения и анализ.

Ценообразование. Использование данного стандарта позволяет рекламодателям платить только за те показы рекламы, которые действительно увидели пользователи.

В ближайшие месяцы такая система подсчета показов начнет применяться и к органическому контенту от брендов ***(Facebook рассказал, как он считает показы рекламы // Marketing Media Review (http://mmr.ua/news/id/facebook-rasskazal-kak-on-schitaet-pokazy-reklamy-43322/). – 2015. – 20.02).***

***

Facebook все глубже уходит в e-commerce

Как сообщается на форуме соцсети, будут добавлены новые возможности в специализирующиеся на электронной коммерции группы. В результате страницы торговцев станут более структурированными и будут напоминать полноценный интернет-магазин. «Мы будем продолжать внедрять новые функции в ближайшие месяцы, чтобы помочь людям с продажами через группы», – говорится в сообщении.

В частности, торговец сможет добавить в соцсети фотографию товара, описание, цену и место доставки в соответствующие поля. До этого вся эта информация подавалась хаотично, что затрудняло поиск пользователям необходимого товара по желаемой цене.

Кроме того, администраторы Facebook вынуждены были постоянно напоминать указывать цену или описание товара, а также способ доставки. Теперь же в этом не будет необходимости, да и покупателям не нужно будет дополнительно запрашивать у продавца интересующую информацию.

Новые опции предоставят возможность отмечать, есть ли товар в наличии, или уже подан, что опять-таки избавит продавцов и покупателей от лишней переписки.

В последнее время наибольшей популярностью в Facebook пользуются группы, через которые можно реализовать либо купить продукцию. Они дают возможность использовать соцсеть как альтернативу Amazon, eBay и других гигантов электронной коммерции.

Эти изменения облегчат торговлю через Facebook многим пользователям. Например, таким как Л. Дункан-Тайер из Флориды (США), которая создала Made By Mama Buy/Sell/Trade. В группе 4,5 тыс. членов, которые увлекаются рукоделием. Она является площадкой на которой женщины продают свои поделки. Изменения в социальной сети в сторону

электронной коммерции помогли многим из них превратить свое хобби в бизнес.

Профессиональный гитарист К. Карвалью из Рио-де-Жанейро (Бразилия) создал Facebook-группу, чтобы помочь музыкантам в Бразилии покупать и продавать инструменты. Почти за три года группа возросла до более чем 34 тыс. членов. Группа также подняла осведомленность о его музыкальной группе Swell.

Facebook становится все больше и больше «заточенным» под нужды e-commerce. Главные тренды в развитии соцсети – рост рекламных доходов, «мобилизация» интернет-рекламы. Одним словом, компания поворачивается к e-commerce лицом ***(Facebook все глубже уходит в e-commerce // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/facebook_vse_glubzhe_uhodit_v_e_sommerce). – 2015. – 20.02).***

***

Торговля аккаунтами в играх и социальных сетях: как на это смотрит закон

Геймеры относятся к своим аккаунтам как к очень ценному активу. Что логично: ведь в создание персонажа именно такого уровня, именно с такими навыками (или даже известностью) вложены сотни человеко-часов. Нередки случаи, когда угон аккаунта рассматривается как полноценное уголовное преступление: в прошлом году в Беларуси возбудили дело о краже аккаунта в World of Tanks с танком, на прокачку которого владелец потратил около 1000 грн, пишет AIN.UA (http://ain.ua/2015/02/21/565554).

То же можно сказать и о владельцах популярных аккаунтов в социальных сетях или на сайтах онлайн-аукционов: на майских выборах паблику «Типичный Киев» предлагали продаться за 1 млн дол. Но несмотря на то, что подобные аккаунты являются достаточно ценным нематериальным активом, в Украине их купля-продажа напрямую законодательством не регулируется.

Именно поэтому редакция AIN.UA попросила старшего юриста и руководителя практики интеллектуальной собственности AstapovLawyers И. Томарова объяснить пользователям, что с точки зрения украинского права происходит, когда вы пытаетесь купить или продать аккаунт в компьютерной игре, социальной сети или в онлайн-аукционе. А также – какие законодательные последствия и ответственность могут для вас при этом возникнуть.

Как происходит продажа аккаунтов в играх, сетях и аукционах

Если вы поищете в Интернете слова «продам аккаунт», то вам предложат купить бесконечное количество аккаунтов игроков в компьютерных играх (чаще всего это WoT). Цена некоторых «прокачанных» аккаунтов достигает десятков тысяч гривен. Существуют сайты и форумы, которые специализируются на покупке-продаже аккаунтов, посредничестве и гарантиях в таких сделках.

В Интернете можно купить аккаунты в социальных сетях «ВКонтакте», Instagram, Twitter и Facebook. Чаще всего их продают пакетами, и с учетом информационной войны в настоящее время это очень неплохой товар – сами продавцы пишут, что спрос и цены в последнее время возросли. Значительно реже покупают один отдельный аккаунт, который, к примеру, имеет несколько десятков тысяч активных читателей.

У каждого покупателя такого товара есть своя цель: либо мгновенно получить возможность воевать с соперниками в компьютерной игре, или получить определенную аудиторию, чтобы предлагать свои товары/услуги/идеи, или получить возможность обманывать пользователей онлайн-аукционов, предлагая хороший лот по низкой цене, а после получения денег исчезать бесследно.

Ценность аккаунта определяется по разным критериям – в зависимости от системы, в которой он существует. Если это компьютерная игра, то чем больше рейтинга, оружия или навыков имеет герой, тем дороже аккаунт игрока. Если речь идет об аккаунте продавца онлайн-аукциона – цена зависит от репутации лица, то есть, истории успешно завершенных сделок и позитивных отзывов покупателей.

Что юридически означает покупка или продажа аккаунта?

С бытовой точки зрения, покупка аккаунта – это передача (сообщение) логина и пароля (или другой информации, по которой идентифицируется владелец аккаунта в той или иной системе) от продавца покупателю, чтобы покупатель мог полностью управлять аккаунтом, включая изменение логина и пароля.

С юридической точки зрения все сложнее. Сначала попробуем применить нормы о покупке/продаже товаров к сделкам с аккаунтом. Очевидно, логин и пароль являются информацией, набором символов, а не вещью, поэтому остаются имущественные права, как предмет договора. Но такой подход нам не поможет, ведь нормы Гражданского кодекса Украины (далее – ГКУ) о покупке-продаже касаются именно вещей как предметов материального мира.

Посмотрим, в каких правовых отношениях возникает аккаунт. Очевидно, что при регистрации в социальной сети, форуме, компьютерной игре или аукционе вы как пользователь заключаете договор с компанией, которое предоставляет услуги в рамках того или иного сервиса. Собственно, аккаунт – это условие доступа к самой услуге: общению, игре или размещению предложений о покупке товаров. Аккаунт возникает в рамках обязательственных правоотношений с провайдером услуг.

Подчеркнем важное обстоятельство – компания, которая предоставляет услуги в сети, идентифицирует пользователей именно при помощи логина, а не настоящего имени человека, которое указано в паспорте. Суды Украины неоднократно подтверждают, что в социальных сетях может зарегистрироваться любое лицо под любым именем, так что создать и

поддерживать страницу человека в социальных сетях, в том числе путем размещения информации и фото, может любое лицо.

Другой способ объяснить природу продажи аккаунта – замена стороны договорных отношений путем уступки права требования. Это означает, что лицо, создавшее аккаунт, имеет право требования по отношению к лицу, которое предоставляет услугу (сервис). Далее путем передачи (сообщения) другому лицу логина и пароля, отказа от дальнейшего пользования услугой под этим аккаунтом, уступает это право покупателю.

Последний фактически становится новым пользователем, хотя для стороны, которая предоставляет услугу (сервис), формально пользователь не поменялся, пока действует тот же логин – имя аккаунта.

Такое объяснение имеет право на существование, если бы не одно обстоятельство – большинство сервисов в разделе «Правила использования», которые являются неотъемлемой частью договора с пользователем, прямо запрещают сообщать другим лицам свой логин и пароль к аккаунту. При таком условии договор купли-продажи вообще является недействительным, ведь стороны согласовали запрет уступки права требования по договору.

Собственно, можно пофантазировать и предложить еще несколько идей, которые бы объяснили природу такой сделки: аренда права пользования аккаунтом и всеми его возможностями (формально ГКУ позволяет это – ч. 2 ст. 760); услуга по предоставлению временного доступа к чужому аккаунту.

Существует ли возможность распорядиться правом пользования аккаунтом или же оно не подлежит передаче третьим лицам? На наш взгляд, ответ на этот вопрос имеет значение в двух ситуациях:

Кто будет отвечать за действия, осуществленные из аккаунта – новый владелец или старый?

Может ли лицо, заплатившее за чужой аккаунт, но не получившее логин и пароль для доступа, обратиться в суд, чтобы взыскать убытки с продавца или заставить его выполнить обязательство в натуре. Подлежит ли это право судебной защите?

На наш взгляд, критерием для признания такого права и его защиты должно быть соответствие поведения сторон общим требованиям к осуществлению субъективных граджанских прав и действительности сделок. Например, если аккаунт покупается с целью использования чужой репутации и эксплуатации доверия потребителей к определенному продавцу, то это – злоупотребление правом. Если же речь идет об аккаунте в компьютерной игре, тут вряд ли возможны злоупотребления.

Какими будут судебные последствия, если аккаунт купили с целью нарушить закон

Если чужой аккаунт использован для того, чтобы причинить вред третьему лицу – публикация недостоверной информации и т. д., тогда, если суд откажется признать нового владельца аккаунта (с которого осуществлены

действия, причинившие убытки), это не должно стать основанием для освобождения правонарушителя от ответственности.

Суд должен возложить возмещение ущерба на лицо, которое этот ущерб причинило (ст. 1166 ГКУ), тогда как первичный владелец аккаунта (человек, который изначально его зарегистрировал) по крайней мере непосредственно непричастен к размещению недостоверной информации, то есть, не совершил действия, причинившие вред. Это правильно до тех пор, пока использование аккаунта не отнесут к источникам повышенной опасности, когда за ущерб отвечает именно владелец такого источника.

Когда покупателя аккаунта обвинят в причинении вреда, он, чтобы избежать ответственности, очевидно откажется от покупки и будет указывать, что аккаунт принадлежит первичному владельцу, который и должен отвечать за информацию, распространенную с этого аккаунта.

Подлежит ли судебной защите право лица заставить продавца аккаунта выполнить обязательство в натуре – передать логин и пароль к аккаунту? Мы считаем, что при условии предоставления надлежащих доказательств заключения такой сделки суд не должен отказать лицу в защите. Конечно, если условия пользования сервисом запрещают передачу логина и пароля от своего аккаунта третьим лицам, суд может признать такую сделку недействительной.

Часто целью покупки логина и пароля к чужому аккаунту является совершение преступных действий.

Кроме покупки чужого аккаунта возможны сделки типа передачи аккаунта в пользование. Так в деле о защите чести, достоинства и деловой репутации оказалось, что информация об истце распространена следующим образом: первое лицо предоставило второму свой аккаунт – личную страницу на форуме, а второе лицо, авторизировавшись под аккаунтом первого на форуме, распространило определенную информацию об истце.

Рынок аккаунтов существует при отсутствии гражданско-правового регулирования и в настоящее время не набрал в Украине таких оборотов, которые бы повлияли на появление правоприменительной практики ***(Торговля аккаунтами в играх и социальных сетях: как на это смотрит закон // AIN.UA (http://ain.ua/2015/02/21/565554). – 2015. – 21.02).***

***

Facebook запустил первые тв-ролики в Великобритании в рамках более масштабной кампании, которая также включает outdoor рекламу, чтобы объяснить, как сервис помогает людям подружиться, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustil-svoju-pervuju-reklamnuju-kampaniju-v-velikobritanii-43358/).

Три тв-ролика больше сфокусированы на бренде, чем на продукте. Ролики рассказывают истории о разной дружбе. Кампания была разработана in-house агентством The Factory ***(Facebook запустил свою первую рекламную кампанию в Великобритании // Marketing Media Review***

(http://mmr.ua/news/id/facebook-zapustil-svoju-pervuju-reklamnuju-kampaniju-v-velikobritanii-43358/). – 2015. – 23.02).

***

Психология соцмедиа: Как оказывать влияние на клиентов в соцсетях

Образовательное учреждение Digital Marketing Institute регулярно публикует исследования, посвященные психологии социальных медиа, которые помогают разобраться в потребностях пользователей, пишет Marketing Media Review (http://mmr.ua/news/id/psihologija-socmedia-kak-okazyvat-vlijanie-na-klientov-v-socsetjah-43366/).

Издание «Цукерберг Позвонит» перевело две статьи и узнало, о чем нужно помнить маркетологам, чтобы получить широкий охват аудитории, повысить кликабельность публикаций и добиться положительного отношения пользователей, основываясь на когнитивной психологии.

Делитесь счастьем

Не секрет, что в реальном мире счастье заразительно. Однако, согласно одному из самых масштабных исследований в области психологии соцмедиа, такой же эффект оно оказывает в виртуальном мире. Психологи назвали это свойство эмоциональным заражением: велика вероятность, что после прочтения записи в социальной сети пользователи «подцепят» ее настрой.

Как этого добиться

Перестаньте быть скучным. Пишите заметки «энергичным» языком, призывайте к действию, чтобы ваши читатели и правда начали действовать. Если хотите увлечь их, сделайте так, чтобы они наслаждались чтением, пишите в легком и дружелюбном тоне: не бойтесь играть словами и разрушать деловой шаблон, от которого веет скукой и канцеляризмами.

Лайк решает

Людям крайне сложно делать первый шаг, поэтому они действуют с оглядкой на других – такая стратегия кажется им более комфортной и безопасной. Мы живем в обществе «я тоже», где количество лайков под записью влияет на степень ее восприятия и охвата. Чем больше людей оценило ваш контент, тем выше вероятность того, что так же поступят их друзья, партнеры и коллеги.

Как этого добиться

Чтобы быть уверенным в том, что запись соберет заслуженное количество лайков и репостов, найдите «агентов влияния» в пределах вашей отрасли и убедите их поделиться вашим контентом. Для этого воспользуйтесь сайтом BuzzSumo, который отображает наиболее цитируемых пользователей по разным темам и ключевым словам (данные по рунету можно отслеживать с помощью сервисов Klout и Favorities. – Прим. ред.). Затем попробуйте наладить с ними отношения.

За каждым лайком стоит своя потребность

Согласно исследованию New York Times, люди делятся контентом из-за потребности в самореализации и для выстраивания отношений с другими.

Пять причин, побуждающих пользователей ставить лайки и делать репосты:

– для 84 % пользователей это способ поддержать близкую им точку зрения;
– 78 % пользователей делают это, чтобы не терять связь с другими;
– 69 % – из-за потребности в самореализации;
– 68 % – для самоидентификации (показать, кто они такие и что им нравится);
– 49 % – ради развлечения.

Как этим воспользоваться? Убедитесь, что ваш контент всегда ценен. Помогайте людям определить, кто они такие, предлагая познавательные публикации. Также вы можете вызвать у подписчиков чувство вовлеченности от использования бренда. Старайтесь всегда отвечать на их вопросы и комментарии, не стесняйтесь работать с пользовательским контентом. Главное – развлекать. Если вы пишете посты с удовольствием, шансы «заразить» читателей становятся выше.

Только про них

Люди обожают говорить о себе и делиться своим мнением. Этот факт подтверждают данные гарвардских нейрофизиологов. Когда мы делимся чем-то, в головном мозге активируются те же зоны удовольствия, что при приеме пищи или получении денег.

Что это значит?

Перестаньте говорить о себе, своем бренде и своих продуктах. Вместо этого говорите непосредственно с аудиторией и обращайте внимание на их самые любимые вещи – сфокусируйтесь на их потребностях и желаниях. Выбирайте слова «вы» и «ваш», полностью забывая о «мы» и «наш».

Три психологические ловушки, которые либо помогут маркетологу, либо все испортят

Что стоит за теми решениями, которые принимают клиенты, когда они лайкают записи, делятся ими и покупают продукты? По мнению Advertised Mind, в основе принятия всех решений лежит нейромаркетинг: «Именно подсознание определяет наше отношение к рекламе, брендам и продуктам и влияет на все наши решения о покупке того или иного товара. Клиенты не знают, почему они покупают то, что они покупают, поэтому традиционные исследования рынка не достигают своих целей».

Если роль подсознания действительно такова, то маркетологам следует взять на вооружение основные психологические «зацепки», которые влияют на восприятие их бренда, продукта и рекламы.

Эффект ореола

В теории:

Эффект ореола – это когнитивное искажение, которое влияет на совокупность наших представлений о человеке или бренде, в основе чего лежит предыдущий опыт взаимодействия. Например, если мы встречаем привлекательного и дружелюбного человека, мы машинально приписываем

ему чувство юмора, доброту, щедрость, интеллектуальность – те качества, которыми в действительности он может и не обладать.

В чем проблема?

Как только покупатель сформировал первое впечатление о бренде или продукте, его дальнейшее отношение будет опираться на первоначальный опыт. Проблема возникает в том случае, если впечатление было негативным. Маркетологи должны поставить перед собой цель – создавать у клиента только яркое и запоминающееся первое впечатление и поддерживать его на всем пути следования сквозь воронку продаж.

Как это сделать?

Одобрение агентов влияния или знаменитостей может оказать мощный эффект на восприятии вашего бренда (зачастую помочь может даже такая мелочь, как ретвит).

Один отличный продукт часто оказывает влияние на восприятие других товаров. Наиболее ярким примером служит iPod.

Всегда помните о важности качества обслуживания клиентов. Если покупатель дотошно расспрашивает вас о товаре или услуге, создайте хорошее первое впечатление, проведя презентацию дружелюбно, грамотно и с пользой для него.

Предложите потенциальным покупателям ознакомиться с брендом, вашей миссией, персоналом или даже офисом.

Предвзятость подтверждения

В теории:

Теория предвзятости подтверждения означает, что люди скорее всего отвергнут выводы, которые противоречат их убеждениям, нежели изменят убеждения. Им не поможет даже знакомство с логикой и статистикой.

В чем проблема?

Клиенты могут просто не поверить впечатляющей презентации на лендинге, даже если она истинна и опирается на факты и статистику.

Как обойти предвзятость подтверждения?

В некоторых случаях лучше давать более реалистичные обещания, чем искать аргументы с дополнительной информацией.

Чтобы подтвердить обещания, используйте позитивные рекомендации, а не статистику. Люди скорее поверят другим людям, чем сухим цифрам, которые легко подправить.

Инстинктивная реакция покупателей сильно влияет на их решение о покупке. При написании продающего текста старайтесь убеждать через эмоции, а не с помощью чистой логики.

Фрейминг-эффект

В теории:

Фрейминг-эффект предполагает, что люди готовы рисковать, когда последствия представлены в качестве избежания потери чего-либо. Соответственно, они не захотят рисковать, когда последствия представляются в качестве полученной выгоды.

В чем проблема?

Зачастую, создавая рекламные или информационные материалы, мы стремимся сразу перейти к выгодам от нашего продукта или бренда. Возможно, стоит остановиться и подумать: «Не станет ли реклама гораздо эффективнее, если я представлю выгоду в качестве потери, которую удастся избежать?» Конечно, все зависит от целевой аудитории – необходимо найти ее желания и страхи.

Как воспользоваться фрейминг-эффектом?

В объявлении о скидках делайте акцент не на потере, а на сохранении средств. Пусть вместо «Товар за 60 % от стоимости» будет «Сохраните 40 %».

Заголовки и призывы к действиям, которые советуют покупателям, как избежать потери, тоже эффективны. Например, вместо «7 способов получить выгоду от распродажи» нужно написать «7 способов не переплатить на распродаже».

Аккуратно сравните свой продукт с конкурентными, акцентируя внимание на вашем уникальном коммерческом предложении. Например: «Компания Х сохранит вам время. Мы – деньги» ***(Психология соцмедиа: Как оказывать влияние на клиентов в соцсетях // Marketing Media Review (http://mmr.ua/news/id/psihologija-socmedia-kak-okazyvat-vlijanie-na-klientov-v-socsetjah-43366/). – 2015. – 24.02).***

***

«Дельта Банк» запустил сервис онлайн-переводов денег через Facebook

Сервис Pay2You от «Дельта Банка» на днях пополнился новой функцией – теперь с его помощью можно перечислить деньги любому Facebook-пользователю, у которого есть гривневая карта любого украинского банка. Для совершения трансферов у отправителя и получателя денег должно быть установлено Facebook-приложение Pay2You. При этом отправителю не нужно знать банковские реквизиты получателя – при получении денег тот самостоятельно указывает номер карты, на которую будут зачислены средства, пишет AIN.UA (http://ain.ua/2015/02/25/566388).

При отправке средств через Facebook взимается фиксированная комиссия в размере 5 грн. Максимальная сумма одного перевода составляет 9 тыс. грн, при этом в сутки можно перевести до 75 тыс. грн, а в месяц – до 135 тыс. грн. Функция отправки денег через Facebook пока работает только в веб-версии приложения.

В банке рассчитывают, что новая функция будет востребована среди онлайн-магазинов, волонтеров и благотворительных организаций, а также обычных интернет-пользователей, которые пользуются услугами перевода средств ***(«Дельта Банк» запустил сервис онлайн-переводов денег через Facebook // AIN.UA (http://ain.ua/2015/02/25/566388). – 2015. – 25.02).***

***

YouTube запустил в тестовом режиме сервис, позволяющий рекламодателю узнать, почему пользователь отключил его рекламу.

Пропуская рекламу, пользователь должен ответить на вопрос о причине, по которой ему не интересно предложение. Выбрать можно из трех вариантов:

– повторяющаяся;
– неинтересная, несоответствующая;
– нерепрезентативная, нерелевантная.

Исследования Ericsson показали, что 95 % всех юзеров пропускают стандартные рекламные ролики на YouTube. При этом 40 % пользователей желали бы выбирать какое предложение им не будут больше показывать. Около трети респондентов хотели бы видеть только ту рекламу, которая будет полностью соответствовать их интересам ***(YouTube представил сервис анализа причин отключения рекламы // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/youtube_predstavil_servis_analiza_prichin_otklyucheniya_reklamy). – 2015. – 25.02).***

***

Facebook официально объявил о том, что программа для поиска партнёров Facebook Marketing Partners вступила в силу, сменив Preferred Marketing Developer (PMD).

О предстоящей реструктуризации сервиса, призванной улучшить поиск партнёров, компания сообщила в октябре 2014 г.

Новая структура даёт компаниям возможность найти партнёров в конкретных странах и отраслях. Кроме того, также был усовершенствован инструмент поиска. Теперь он позволяет искать по специальности, стране, отрасли и затем напрямую контактировать с партнёром.

В программе участвуют сотни партнёров. Они распределены по девяти категориям на основе областей их компетенции: рекламные технологии, медиабаинг; Facebook Exchange; управление сообществами в социальных сетях (комьюнити-менеджмент); контент-маркетинг; решения для малого бизнеса; построение аудитории; провайдеры данных аудитории и измерения.

Один из партнёров программы, Adobe, отправил редакции WebProNews несколько комментариев по поводу изменений в сервисе:

«Программа Facebook даёт маркетологам возможность найти технологических партнёров на основании своих потребностей. Поскольку пространство цифровых медиа становится всё более фрагментированным, а нужды маркетологов – более конкретными, становится понятно, почему Facebook произвёл эту реорганизацию. Новая структура отходит от API-центрированного подхода в сторону дескрипторов, управляемых маркетингом».

«Интересным было внедрение новых игроков. Это важный шаг для индустрии, поскольку агентства должны будут пройти сертификацию в

Facebook. В настоящее время в отрасли присутствует выраженная потребность в повышении квалификации в области продвижения в социальных сетях, особенно учитывая то, как быстро меняется эта среда» ***(Программа Facebook Marketing Partners вступила в действие // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/programma_facebook_marketing_partners_vstupila_v_deystvie). – 2015. – 27.02).***

***

Социальная сеть Facebook объявила о внедрении новой системы управления взаимоотношениями с клиентами, специально для работы с рекламодателями.

Система разработана в тесном сотрудничестве с компанией Salesforce, и опирается на их систему управления данными Sales Cloud. Новая разработка, предназначенная для внутреннего пользования, позволит улучшить взаимодействие социальной сети и рекламодателей, которые смогут мгновенно реагировать на любые проблемы с рекламными объявлениями. В свою очередь администрация соцсети будет немедленно видеть на экране, сколько и каких объявлений, роликов и баннеров прокручивается. В случае возникновения технических неполадок соответствующее уведомление автоматически отправится системному администратору.

Наконец, система будет предоставлять полезную информацию и пользователям – конечным потребителям рекламы. Так, если срок действия чьей-нибудь кредитной карты будет подходить к концу, система автоматически вышлет соответствующее уведомление.

Предполагается, что интеграция новых функций, в первую очередь, облегчит существование рекламных агентов, работающих с социальной сетью, и привлечёт ещё больше рекламодателей ***(Facebook внедряет улучшенную систему контроля рекламы // Blog Imena.UA (http://www.imena.ua/blog/facebook-productivity/). – 2015. – 25.02).***

***

Профессиональная социальная сеть деловых контактов LinkedIn выпустила новый рекламный продукт LinkedIn Network Display.

Продукт позволяет рекламодателям купить место для рекламы LinkedIn на других сайтах по всему Интернету. Специалисты по маркетингу могут ориентироваться на конкретные группы людей – например, показать руководителям отделов медиа-продаж из Bay Area объявления на LinkedIn, а затем использовать куки, чтобы показывать рекламу пользователям даже после того, как они покинули LinkedIn.

Таким образом, компания продает рекламные площади на других сайтах. Значит ли это, что LinkedIn в настоящее время действует как рекламная сеть? Руководитель отдела маркетинговых решений продуктов LinkedIn Р. Гласс говорит, что он так не считает. Р. Гласс называет сервис

«сетью аудитории», где рекламодатели таргетируют рекламу на конкретные группы людей, а не определенные сайты.

Аналогичный рекламный продукт под названием Audience network предлагает Facebook. Но Facebook использует широкий спектр персональных данных, а LinkedIn – профессиональных, объясняет Р. Гласс.

Новый продукт связан с приобретением сетью LinkedIn рекламного стартапа Bizo, который предложил подобную технологию. Р. Гласс на момент приобретения занимал должность генерального директора Bizo.

Среди сайтов-партнеров, на которых LinkedIn будет продавать рекламное пространство, – CNN и Weather.com.

LinkedIn также представил еще один инструмент под названием Lead Accelerator. Продукт представляет собой алгоритм, определяющий местоположение конкретного пользователя LinkedIn в процессе покупки. Он будет автоматически показывать нужное объявление этому пользователю в надежде подтолкнуть его к последующей деятельности. Другими словами, эта технология LinkedIn помогает рекламодателям узнать, когда и какие объявления показывать определенным пользователям.

Спонсируемый контент, который является частью рекламных предложений LinkedIn's Marketing Solutions, является самым быстрорастущим бизнесом компании. Новые инструменты призваны продолжить этот рост ***(LinkedIn начал показывать рекламу за пределами сети // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/linkedin_nachal_pokazyvat_reklamu_za_predelami_seti). – 2015. – 27.02).***

***

Аналитики Socialbakers исследовали данные по объявлениям, размещенным в прошлом году в Facebook, и вывели несколько трендов, которые могут быть полезны маркетологам сегодня.

1. Цели рекламных кампаний – понятные и измеримые

Маркетологи предпочитают тратить деньги на рекламу, которая дает понятный результат, и выбирают в качестве рекламных целей установки мобильных приложений, просмотры видео, переходы на сайт.

Видео стало неоспоримым трендом – примерно 5 % бюджетов рекламодателей тратится на увеличение просмотров роликов.

2. Большее внимание точно настроенному таргетингу

Несмотря на то что большая часть объявлений все еще запускается через кнопку «Продвигать публикацию» и без настроек целей и таргетинга, маркетологи начинают более вдумчиво подходить к рекламным кампаниям. В IV квартале 2014 г. только 27 % объявлений создавалось из автопродвигаемых постов, на что уходило 14 % бюджетов. По сравнению с данными за I квартал 2014 г. – 40 % и 26 % соответственно – изменения налицо.

Однако, отмечают специалисты Socialbakers, работать еще есть над чем – и прежде всего это касается таргетинга: только 44 % объявлений настроены по интересам пользователей, только 26 % объявлений настроены на индивидуализированные аудитории.

3. Новостная лента – самая эффективная

Сравнивая CTR и CPC объявлений с разными настройками размещения, специалисты пришли к выводу, что реклама в Новостной ленте не только обходится дешевле всего, но и приносит максимальную эффективность.

Маркетологи, по всей видимости, тоже это заметили – что можно проследить по растущим бюджетам именно на это место размещения ***(Реклама в Facebook: тренды 2015 года // ProstoWeb (http://www.prostoweb.com.ua/internet_marketing/sotsialnye_seti/novosti/reklama_v_facebook_trendy_2015_goda). – 2015. – 23.02).***

***

Twitter Ads запустил два новых инструмента – «стоимость транзакции» (transaction values) и «тег ключевой конверсии» (key conversion tags). Нововведения позволяют владельцам сайтов видеть продажи, привлечённые непосредственно продвигаемыми твитами, и доступны для рекламодателей во всём мире, пишет Marketing Media Review (http://mmr.ua/news/id/twitter-dobavil-dva-novyh-instrumenta-dlja-izmerenija-roi-reklamy-43429/).

Обе функции требуют размещения тегов отслеживания конверсий на сайте. Такие теги ранее использовались для ремаркетинга. Теперь они могут использоваться для отслеживания показателей продаж.

Продакт-менеджер Twitter А. Шривастава пояснил суть нового функционала в рекламном блоге компании:

«Если вы уже внедрили тег нашего сайта, вы можете внести в него несколько несложных изменений для начала сбора данных о стоимости конверсий и количестве заказов по каждой из них. Эти данные агрегируются и доступны на аналитической панели управления Twitter Ads, позволяя видеть ROI (коэффициент возврата инвестиций) для кампаний, основанных на продвигаемых твитах. Если вы ещё не используете отслеживание конверсий, начать можно, создав тег в пользовательском интерфейсе Twitter Ads и внедрив его на вашем сайте».

Тег ключевой конверсии позволяет ещё больше улучшить измерение эффективности кампании, давая маркетологам возможность оптимизации кампании под конкретное событие конверсии.

«Например, цветочный магазин хочет использовать Twitter Ads для увеличения продаж букетов. Как только владелец магазина установит тег сайта на страницу финальной конверсии для букета и выберет этот тег как ключевой тег для кампании, Twitter автоматически начнёт оптимизировать кампанию, направляя больше конверсий на страницу продажи букетов. Магазин также будет иметь возможность видеть количество покупок букетов

на аналитической панели в Twitter Ads сразу, как только эта конверсия произошла. Поскольку отслеживание конверсий в Twitter действует на кросс-платформенной основе, даже если пользователь увидел объявление цветочного магазина на мобильном устройстве, а финальная конверсия произошла на десктопе, Twitter Ads сможет отследить это событие и сообщить о нём».

Напомним, что Twitter запустил рекламные или так называемые «продвигаемые» твиты в хронике в июне 2011 г.

В этом месяце стало известно о том, что продвигаемые твиты выходят за пределы сервиса микроблогов. Первыми партнерами Twitter в новой программе стали мобильное приложение для чтения новостей Flipboard и Yahoo Japan ***(Twitter добавил два новых инструмента для измерения ROI рекламы // Marketing Media Review (http://mmr.ua/news/id/twitter-dobavil-dva-novyh-instrumenta-dlja-izmerenija-roi-reklamy-43429/). – 2015. – 27.02).***

***

Компания Facebook объявила о запуске приложения, которое позволит маркетологам создавать и редактировать объявления на ходу. На сегодняшний день оно доступно только для iOS, пишет Marketing Media Review (http://mmr.ua/news/id/facebook-zapustila-prilozhenie-dlja-raboty-s-reklamoj-43377/).

По сообщению Facebook, рекламодатели могут пользоваться приложением для отслеживания эффективности рекламы, редактирования уже существующих объявлений, корректировки плана по расходам и времени публикаций, просмотра push-уведомлений и создания новых рекламных объявлений.

Приложение, которое пока доступно только на iOS, было анонсировано вскоре после того, как Facebook объявил о привлечении более 2 млн рекламодателей. Версия для Android будет выпущена позже в этом году. Пока сервис доступен только в США, в ближайшие недели он должен появиться во всем мире ***(Facebook запустила приложение для работы с рекламой // Marketing Media Review (http://mmr.ua/news/id/facebook-zapustila-prilozhenie-dlja-raboty-s-reklamoj-43377/). – 2015. – 24.02).***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Почему мы откровенничаем в Интернете?

Сегодня шанс узнать, что друг купил новую машину, выше в Instagram, чем за чашкой кофе. Мало видимся, редко созваниваемся. Социальные сети расскажут, кто женился или развёлся, кто куда переехал, у кого ребёнок пошёл в школу… Люди щедро делятся интимными событиями с миром. Почему так происходит? И стоит ли судить о человеке по его профилю в социальных сетях? Обсудим в этой статье, передает Day.Az со ссылкой на 5Сфер.

Интернет задумывался как канал получения и передачи информации. Но быстро стал каналом коммуникации. От обмена мнениями в LiveJornal до создания «микромиров» в MySpace, Facebook и других социальных сетях.

Социальные медиа, а также электронная почта и мессенджеры изменили природу общения. В том числе отношение ко лжи.

Я – версия 2.0

Люди охотно выкладывают в сеть фотографии и рассказывают про своих мужей и жён, детей (даже новорождённых), домашних питомцев, жилища…

Мы решили разобраться в психологии и обратились с вопросом, зачем люди устраивают «стриптиз» в социалках, к профессионалу. А. Кутинова – практикующий психолог, гештальт-терапевт, семейный консультант:

Эгоцентризм и тщеславие.

Есть такой тип личности – истероидный или демонстративный. Такие люди склонны к театрализации. Активность в социальных сетях позволяет им постоянно обращать на себя внимание. Они уверены, что обязаны подарить миру свой «богатый внутренний мир».

Лайки и положительные комментарии тешат самолюбие таких людей. Они не терпят конкурентов, поэтому банят всех, кто не восхищается ими.

Истероиды – актёры, любят примерять на себя различные маски. Вот я дрянная девчонка, а вот я хозяюшка / вот я спортсмен, а вот я на крутой тачке.

Подмена понятий

Вторая причина в личностном дефиците. Неуверенность в себе, отсутствие стабильности, проблемы в личной жизни – всё это человек пытается компенсировать через социальные сети.

Девушку, неуверенную в своей привлекательности и ценности, видно сразу: у неё 1679 фотографий, множество альбомов, статусы а-ля «Меня трудно найти, но легко потерять» и прочее.

Человека, неустроенного в жизни и зацикленного на успехе, тоже несложно вычислить. В его ленте только хорошие новости, бизнес-советы, рекомендации, как достичь успеха, и т. д. Он считает, что если его мир не идеален, то он недостоин любви.

Пары, демонстрирующие в соцсетях «идиллию», как правило, далеки от неё в жизни. Взаимные искренние чувства не требуют публичности. Напротив, люди стараются скрыть от посторонних то, что им дорого. Если мужчина или женщина постоянно пишет «Я люблю тебя» на стене партнёра вместо того, чтобы говорить это лично, значит, между ними нет контакта. В отношениях им важны не отношения как таковые, а статус «влюблён в такую-то» или «замужем за таким-то».

Таким образом, социальные медиа выдают желаемое за действительное:

у неуверенных в себе повышается самооценка;

лузеры «приближаются» к своей мечте;

а несчастные в любви получают иллюзию крепких отношений.

Признание окружающих, их любовь и внимание в умеренной степени нужны всем. Даже самодостаточный человек улыбнётся, увидев приятный комментарий под своим фото. Но в социальных сетях эта потребность зачастую приобретает гипертрофированный характер. Личности с неустойчивой самооценкой подсаживаются на лайки и комментарии, как на наркотик. Такие люди не любят себя и не видят своей ценности. Гармоничному человеку лайки и комментарии не нужны.

Последствия

К чему приводит подобная откровенность в социальных сетях? К укоренению психологических проблем и всё большему разрушению реальных межличностных связей.

Можно разучиться общаться. Перестать быть самим собой, быть спонтанным. Ведь в сети у вас всегда есть время на то, чтобы обдумать сообщение, чтобы подстроить его под свой образ.

Но самая большая опасность не в виртуальных ролях как таковых, а в переносе их в реальную жизнь.

Жизнь не блог, её нельзя поставить на паузу или перемотать. Советчики в «Моём мире» не помогут вам помириться с мужем или, к примеру, найти девушку. Пока вы лайкаете и репостите, лишние килограммы остаются при вас, дома сохраняется бардак, а друзья становятся знакомыми ***(Почему мы откровенничаем в интернете? // Day.Az (http://news.day.az/unusual/559639.html). – 2015. – 28.02).***

***

Влюбленные, которые выставляют свои отношения напоказ в социальных сетях, выкладывая общие фотографии или размещая сообщения о своей любви, счастливее тех, кто так не делает.

К такому выводу пришли ученые из общественного исследовательского Университета Хьюстона (США). Специалисты провели эксперимент, в котором приняли участие 188 студентов, состоящих в стабильных отношениях.

Те участники исследования, которые постоянно оповещали своих друзей и подписчиков в социальных сетях о свиданиях с возлюбленными и выкладывали совместные селфи, оказались более счастливыми, чем те, кто не выставлял свою личную жизнь на всеобщее обозрение. Как считают ученые, если партнеры публично берут на себя обязательства – качество их отношений повышается, поскольку человек открыто объявляет, что возлюбленный – важная часть его жизни. Те, кто относятся к отношениям со всей серьезностью, скорее всего, имеют внутреннюю мотивацию для того, чтобы поведать о своей любви в социальных сетях. Сам этот факт уже может оказать положительное влияние на отношения в паре.

Кстати, научные сотрудники Колледжа Олбрайт подтвердили результаты исследований своих коллег о том, что именно счастливым парам свойственно делиться подробностями своих взаимоотношений в Интернете. Однако ученые также выяснили, что так поступают и те, кто имеет чересчур завышенную самооценку, зависящую от качества отношений. Проблемы в личной жизни являются для них серьезным ударом и наносят больший вред, чем пользователям с низкой самооценкой. Именно поэтому для таких людей важно продемонстрировать остальным, в том числе и своему возлюбленному, что их отношения – идеальны. Помимо этого, подробности своей личной жизни выкладывают в сеть интроверты и невротики.

А вот исследователи из Технологического института Джорджии взялись выяснить, как на человека влияет изменение статуса отношений в социальных сетях. Оказалось, что как только человек сообщает в Интернете о своей помолвке, его словарный запас и восприятие времени кардинально меняются.

Сразу же после обручения люди начинали почти на 70 % чаще использовать слово «мы», заменив им местоимение «я». Мужчины увеличивали количество комплиментов своим вторым половинкам. Наиболее часто использовались такие слова, как «сексуальная», «великолепная» и «красавица». Женщины также начинали выражать свои чувства более эмоционально. У них популярными становились слова «любовь» и «прекрасный». Кроме того, после помолвки, возлюбленные реже использовали глаголы прошедшего времени, заменяя их на будущее время ***(Совместные фото в социальных сетях положительно влияют на отношения пары // Электронная газета «Век» (http://wek.ru/sovmestnye-foto-v-socialnyx-setyax-polozhitelno-vliyayut-na-otnosheniya-pary). – 2015. – 22.02).***

Маніпулятивні технології

Незалежна іспанська репортерка й авторка М. Карраско викрила ісламістських тролів і звернулася із закликом до Європи ефективно протидіяти антимедійному свавіллю у соціальних мережах, пише Західна інформаційна корпорація (http://zik.ua/ua/news/2015/02/16/ispanska_zhurnalistka_zaklykaie_yevropu_protydiyaty_anonimnym_pogrozam_u_sotsmerezhah_564837).

Про це пише на сайті віденського Міжнародного інституту преси (IPI) координатор із цифрових медіа Х. Луке.

Після показу документального фільму про ісламський фундаменталізм з її коментарем М. Карраско відразу отримала на Twitter «шквал» образ і погроз. Слова «брехуха» та «блудна дівка» надходили на її адресу з кількох анонімних Twitter-акаунтів і «повністю координувалися», заявила репортерка.

Також М. Карраско погрожували на Twitter убивством. Це збіглося з публікацією її книги про війну у Сирії. Дві погрози вона добре пам'ятає. В одній з них говорилося: «У сутінках твоїх днів ти почуєш наш сигнал», в іншій – «Ти помітиш це у власному тілі».

Автор другого твіту вилучив його після того, як журналістка вирішила повідомити про це іспанську владу. «Повідомлення було видалене, однак ці слова застрягли у моїй пам'яті», – говорить М. Карраско.

Мета цієї акції – залякати професійних журналістів, вважає вона. «Ті, хто висвітлював арабські революції, знають про що йдеться, – пояснює М. Карраско.

Іспанська репортерка вирішила публічно викрити те, що з нею сталося. Вона заявила, що заохочує своїх колег, які також зазнають переслідувань у мережі, «зробити крок вперед» і «просити європейську владу покласти край анонімним погрозам у соціальних мережах».

Інцидент із М. Карраско, – не поодиноке явище. Організація з захисту свободи слова Index of Censorhip тільки в останньому семестрі 2014 р. зареєструвала десятки випадків образ, погроз і порушень прав онлайн-журналістів у Європі.

В опитуванні репортерів, проведеному британським Університетом Центрального Ланкаширу, 70 % респондентів засвідчили, що їх ображали через Twitter за професійну роботу. Половина журналістів зазнала особистих образ, а 27 % – прямих погроз. Як наголошується в доповіді, зазвичай респонденти блокували акаунти, з яких надходили образи, чи принаймні вилучали зловмисні твіти.

М. Карраско вважає, що це явище існує, оскільки деякі колеги применшують образи й наклепи тролів у соціальних мережах і дають їм можливість тривалий час перебувати в мережі.

«Вони (тролі) існують тому, що ми їх не викриваємо і дозволяємо, щоб такі злочини лишалися безкарними аж поки справа не доходить до фізичних погроз», – наголошує іспанська журналістка.

Протягом майже десятиліття М. Карраско висвітлювала конфлікти в Афганістані, Сирії, Лівії, Малі, Чечні, Інгушетії, у Грузії. Працювала кореспондентом у Москві.

40-річна М. Карраско співпрацювала з іспанськими та закордонними медіа: El País (Іспанія), iTELE -Canal Plus (Франція), DPA, Die Welt (Німеччина), Publico, La Nacion (Аргентина), Cadena SER, Yo Dona, Telecinco News, Foreign Policy (Іспанія), OpenDemocracy (Велика Британія) та з іншими.

Вона – авторка таких книг, як «Хочемо знати» (2012), «Камікадзе» (2012) та співавторка електронної книги «Я буду у раю» (2012), повідомляє «Телекритика» ***(Іспанська журналістка закликає Європу протидіяти анонімним погрозам у соцмережах // Західна інформаційна корпорація (http://zik.ua/ua/news/2015/02/16/ispanska_zhurnalistka_zaklykaie_yevropu_protydiyaty_anonimnym_pogrozam_u_sotsmerezhah_564837). – 2015. – 16.02).***

***

У сервісі мікроблогів Twitter з'явилися фейкові сторінки російськомовних служб «Радіо Свобода» та «Голосу Америки».

Як повідомляє radiosvoboda.org, фейкова сторінка російської редакції RFE/RLз'явилася у Twitter 9 лютого. Візуально вона дуже схожа на справжню, оскільки головне фото копіює емблему компанії.

В описі сторінки зазначено: «Вільні новини на Радіо Свобода. Міняємо вашу Батьківщину на наші кросівки». Додано також номери телефону, які, як з'ясувалося, належать Службі зовнішньої розвідки РФ.

Напередодні в мережі з'явився подібний несправжній акаунт – клон російськомовного «Голосу Америки».

На цих сторінках поширюються як реальні матеріали цих медіа, так і посилання на сайти з російською пропагандою.

Обидві сторінки не є популярними серед користувачів. Фейк на Twitter-профіль «Радіо Свобода» читає лише три особи, а фейкову сторінку «Голосу Америки» – 33.

Керівництво «Радіо Свобода» у зв'язку з цією ситуацією поскаржилося до адміністрації Twitter ***(У Твіттері з'явився фейковий аккаунт «Радіо Свобода», який поширює пропаганду // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/social/u_tvitteri_zyavivsya_feykoviy_akkaunt_radio_svoboda_yakiy_poshiryue_propagandu/). – 2015. – 17.02).***

***

Следователь Голосеевского РОВД г. Киева М. Литовченко (родом из Луганска), которая принимала участие в блокировании песчаного карьера на Жуковом острове, поддерживает действия Беркута и дружит с сепаратистами

ДНР. Об этом свидетельствует личная страничка М. Литовченко в социальной сети «ВКонтакте».

Главной фотографией профиля М. Литовченко сделала свой снимок в нижнем белье. В фотоальбоме следователя присутствуют и другие фотографии эротического характера. Однако более интересно другое. М. Литовченко подписана на группу «Типичный Беркут», где прославляются действия сотрудников Беркута во время избиения активистов на Евромайдане.

«Хотим всем вам напомнить кто стоял, кто горел, кто погибал за Украину, за Родину, за Мир! Против нацистской, бандеровской, фашистской мрази. Стояли, ни смотря не на что, чьи-то сыновья, чьи-то мужья, отцы, чьи – то дети. Замерзали в резиновых берцах, грелись чаем заваренным тут же на баррикадах. Спасибо за попытку спасти разорванную теперь уже Украину», – такое по вечерам читает киевский следователь.

Изучив список друзей М. Литовченко, удалось обнаружить, что она поддерживает связь с террористами. Так, в частности, в списке есть некие Д. Цацкин и А. Луганский, которые, судя по их профилям, воюют в составе пророссийских банд против украинской армии. Не исключено, что, работая в киевской милиции, М. Литовченко передает боевикам необходимую информацию.

Кроме этого, в друзьях у М. Литовченко есть действующие сотрудники МВД Украины, которые не скрывают своих политических взглядов. Так, например, пользователь М. Савченко подписал словом «хунтамобили» фотоснимок машин, которые разукрашены в цвета украинского флага. В списке друзей М. Литовченко указано более 200 человек – преимущественно сотрудники милиции или выпускники милицейских вузов. Не исключено, что при детальном изучении каждого, можно найти и другие примеры сепаратизма ***(Следователь Голосеевского РОВД Киева дружит с сепаратистами «ДНР» // Дорожный контроль (http://roadcontrol.org.ua/node/2490). – 2015. – 17.02).***

***

Прес-служба Міністерства оборони закликає українців уважніше ставитися до джерел інформації.

«У соціальних мережах, зокрема у Twitter та Facebook, з’явилися нібито персональні сторінки Міністра оборони України генерал-полковника Степана Полторака. Офіційно заявляємо, що ані Міністр особисто, ані прес-служба не веде подібні сторінки. Інформація розміщена на даних ресурсах не є офіційною позицією Міністра.

Просимо представників ЗМІ не посилатися на дані ресурси, а використовувати інформацію лише з офіційних джерел», – ідеться в повідомленні ***(Заява Міністерства оборони щодо фейкових сторінок у соцмережах // Новини Полтавщини (http://np.pl.ua/2015/02/zayava-***

ministerstva-oborony-schodo-fejkovyh-storinok-u-sotsmerezhah/). – 2015. – 18.02).

***

Финские власти обеспокоены российскими интернет-троллями

Представители финского Госсовета заявили, что российские интернет-тролли становятся все более активными после присоединения Крыма. Об этом сообщает финский портал Yle.

По словам пресс-службы Госсовета, одна из целей троллей – раскол Евросоюза и недоверие к местным политикам. Ответной реакцией финских служб является опровержение ложных утверждений и дезинформации. При этом пророссийскую позицию в Интернете защищают не только россияне, но и финны, уточнил представитель Госсовета М. Мантила.

Как сообщает Yle, «завод троллей» находится в Санкт-Петербурге на улице Савушкина. В штате «завода» работают не только русскоязычные тролли, но и те, кто специализируется на англоязычных СМИ ***(Финские власти обеспокоены российскими интернет-троллями // InternetUA (http://internetua.com/finskie-vlasti-obespokoeni-rossiiskimi-internet-trollyami). – 2015. – 19.02).***

***

В Интернете ФСБшные структуры начали массово распространять информацию о «трофеях», которые якобы бросили наши бойцы в Дебальцево. Об этом сообщает волонтер М. Дворянчук.

«Типа сотни танков и бронемашин, десятки “Градов” и тысячи минометов, автоматов и БК. Особое внимание уделили волонтерам – типа благодарят их за обеспечение наших солдат тепловизорами, рациями, медикаментами, бронежилетами и касками, которые они тоннами собирают по всему городу. Это УЖЕ массово тиражируют российские СМИ. Так вот, этот “вброс” должно поднять еще одну волну недовольства властью и армией. Эти “благодарности” должны разочаровать простых людей и заставить НЕ помогать волонтерам деньгами, соответственно, армии техникой.

Задумка №2. “Легализовать” присутствие огромного количества российской техники, которая сейчас переправляется через границу и той, что ждет своей очереди. Об этом уже написал Д. Тымчук. О “трофеях” мы уже неоднократно слышали.

Задумка №3. Посеять сомнения в наших западных союзников относительно предоставления оружия нового поколения. Типа, вы давайте, а они ее покидают в очередных “котлах”.

Поэтому!!! Очень прошу нещадно банить всех распространителей этой дезинформации. Думаю, в СБУ вычислят основные украинские центры распространения очередной волны паники и дезинформации, поэтому применимы соответствующие меры», – сообщил волонтер ***(ФСБ вбрасывает***

в Интернет фейк о брошенной ВСУ технике // Донецкие вести (http://www.donetskie.com/news/fsb-vbrasyvaet-v-internet-feyk-o-broshennoy-vsu-tekhnike/46443/). – 2015. – 20.02).

***

Литва заявляє, що Росія почала розпалювати інформаційну війну в литовських ЗМІ і соцмережі

Департамент держбезпеки (ДГБ) Литви повідомив, що спостерігає «все більш очевидні» зусилля Росії з розпалювання інформаційної війни та поширення пропаганди в ЗМІ та соціальних мережах Литви. Про це повідомляє видання delfi.lt.

«Останнім часом фіксуються все більш очевидні зусилля Росії по розпалюванню інформаційної війни і прагненню широкого поширення своєї пропаганди в засобах масової інформації, в електронних ЗМІ та соціальних мережах Литви», – ідеться в повідомленні ДГБ, поширеному на сайті відомства.

Як наголошується в документі, Росія шукає засоби, як під прикриттям зареєстрованих в інших країнах підприємств інвестувати в ЗМІ Литви, або підтримувати їх фінансами, і таким чином впливати на зміст публікованої інформації або трансльованих радіопередач.

За даними ДГБ, представниками зарубіжних держав, необов'язково Росії, може бути запропоновано функціонуючим у Литві ЗМІ співпрацювати в поширенні сприятливою для Росії інформації, у підготовці інформаційних кампаній або прямої публікації замовних статей.

У повідомленні наголошується, що ворожий для Литви інформаційний фон прагнуть формувати і в регіональних ЗМІ країни.

ДГБ закликає журналістську спільноту Литви не піддаватися на можливі провокації Росії, а в разі навмисних або підозрілих дій з поширення пропаганди, спроб надання фінансового впливу або прагнення вплинути на зміст підготовлювану інформації просить інформувати про це Департамент державної інформації ***(Литва заявляє, що Росія почала розпалювати інформаційну війну в литовських ЗМІ і соцмережі // Телекритика (http://www.telekritika.ua/kontekst/2015-02-24/104128). – 2015. – 24.02).***

***

Як Кремль нагнітає паніку щодо гривні в соцмережах

Як давно стало зрозуміло, російська пропагандистська машина активно втручається в будь-які невдачі суспільного та економічного життя в Україні, розкручуючи теми поразок та близького кінця в соціальних мережах – не кажучи вже про паніку військового характеру.

Інтернет-експерт В. Мороз виявив таку ж активність ботів Кремля з приводу падіння курсу гривні, які розкручували паніку впродовж останніх кількох діб. Детальніше читайте на сайті видання ***(Як Кремль нагнітає паніку щодо гривні в соцмережах // Watcher***

(http://watcher.com.ua/2015/02/26/yak-kreml-nahnitaye-paniku-schodo-hryvni-v-sotsmerezhah/). – 2015. – 26.02).

***

Фейкові акаунти в соцмережах, що мають ознаки бот-мережі, почали розкручувати тему фінансового Майдану.

Як відомо, 26 лютого правоохоронці розігнали нечисленну акцію протесту під будинком НБУ, яку називали "фінансовим Майданом". Тема була одразу підхоплена проросійськи налаштованими ботами та сайтам. Детальніше читайте на сайті видання ***(Боти Кремля розкручують тему "фінансового Майдану" // Watcher (http://watcher.com.ua/2015/02/27/boty-kremlya-rozkruchuyut-temu-finansovoho-maydanu/). – 2015. – 27.02).***

***

У Генеральній прокуратурі України прокоментували інформацію про фальшиву сторінку Генпрокурора В. Шокіна в соціальній мережі Facebook.

Як інформує управління зв'язків із громадськістю та ЗМІ ГПУ, ідеться про акаунт за адресою: https://www.facebook.com/viktor.shockin?fref=ts

«Вказаний акаунт не має жодного стосунку ні до генерального прокурора України В. Шокіна зокрема, ні до відомства Генеральної прокуратури взагалі», – ідеться в повідомленні ***(У Facebook з'явився фальшивий акаунт Шокіна // Інформаційна агенція «Вголос» (http://vgolos.com.ua/news/u_facebook_zyavyvsya_falshyvyy_akaunt_shokina_foto_173109.html). – 2015. – 24.02).***

***

Twitter модернизирует уведомления о нарушениях и разработает систему противостояния действиям злостных троллей, основанную на хранении телефонных номеров. Об этом сообщает The Verge.

Twitter начнёт отслеживать активность серийных троллей по их телефонным номерам: если прежде пользователь, аккаунт которого был заблокирован, мог создать новую страницу и снова нарушать правила сервиса, то с обновлённой системой безопасности он не сумеет зарегистрировать аккаунт на дискредитированный телефонный номер.

На момент публикации этого материала привязка профиля к телефону не является обязательной, однако пользователи, заблокированные за оскорбления и издевательства, будут вынуждены привязать его по новым правилам. Впоследствии этот номер и почтовый адрес, использованный при создании учётной записи, будут сверяться со списком уже уличённых в троллинге пользователей. Это решение не универсально, так как нарушитель вполне может создать ещё один аккаунт без привязки его к телефону и начать всё заново.

Также Twitter намерен развить инициативу 2014 г., когда третьим лицам разрешили оповещать модераторов об издевательствах. После того как

компания позволила сторонним наблюдателям сообщать о случаях нарушения, ей пришлось в три раза увеличить число модераторов, так как количество жалоб возросло в пять раз. Это разрешение распространили и на случаи фальсификации личности и публикации приватной информации ***(Twitter создаст телефонную базу «серийных» троллей // InternetUA (http://internetua.com/Twitter-sozdast-telefonnuua-bazu--seriinih--trollei). – 2015. – 28.02).***

Зарубіжні спецслужби і технології «соціального контролю»

Британские службы контрразведки (MI5) и разведки (MI6) разместили на своих сайтах объявление о наборе сотрудников, в совершенстве владеющих русским языком.

Тем, кто поступит в MI5, предлагается работать в составе следственных групп. Работа будет состоять в прослушивании записей телефонных разговоров и изучении перехваченных и изъятых документов на русском языке. Ценится не только прекрасное владение языком, но и «знания о российской культуре, истории, политике, идеологии и экономике». Целью работы является создание «обоснованного представления о потенциальных угрозах национальной безопасности» страны.

Соискателей предупреждают, что у них должно быть британское гражданство, и они должны быть достаточно «осмотрительными, чтобы не писать в Twitter о своих успехах».

Службу в разведке ведомство MI6 обещает «одновременно увлекательную и полезную». «Это свидетельство того, что отношения с Россией достигли напряженности, которой не было со времен холодной войны», – комментирует объявления на сайтах спецслужб The Telegraph ***(Спецслужбы Британии набирают русскоговорящих агентов // Mignews.com.ua (http://mignews.com.ua/sobitiya/inworld/4840660.html). – 2015. – 16.02).***

***

Французские судебные органы постановили, что работодатели, выдающие сотрудникам служебные мобильные телефоны, имеют право читать sms-сообщения на этих аппаратах, передает Les Echos.

Исключением в этом правиле будут только те сообщения, которые отдельно помечены пользователями как «личные».

Соответствующее решение принял Кассационный суд Франции по итогам разбирательства между двумя финансовыми компаниями, одна из которых отслеживала sms своих сотрудников.

Суд постановил, что sms, отправленные и полученные при помощи служебного телефона, по определению носят рабочий характер и поэтому могут стать достоянием работодателя ***(Французским работодателям дали право читать SMS на служебных телефонах // InternetUA***

(http://internetua.com/francuzskim-rabotodatelyam-dali-pravo-csitat-SMS-na-slujebnih-telefonah). – 2015. – 22.02).

***

Агентство национальной безопасности США взломало внутреннюю систему крупнейшего в мире производителя SIM-карт и имело возможность следить за трафиком миллионов абонентов тайком от сотовых компаний. Об этом сообщает издание The Intercept со ссылкой на секретные документы, полученные от Э. Сноудена.

Согласно документам от 2010 г., АНБ и Центр правительственной связи (GCHQ, британская спецслужба) взломали внутреннюю сеть голландской компании Gemalto, производящей чипы для кредитных карт и около 2 млрд SIM-карт для мобильных телефонов ежегодно.

В ходе проникновения во внутреннюю сеть Gemalto были украдены секретные ключи, обеспечивающие безопасность глобальной коммуникации, утверждает издание. Взлом дал спецслужбам возможность следить за абонентами около 450 сотовых операторов по всему миру, включая как голосовые звонки, так и текстовые данные, а также расшифровывать уже перехваченные ранее зашифрованные данные.

Издание поясняет, для чего агентствам нужны были ключи безопасности. При производстве SIM-карту снабжают таким ключом, а его копию получают операторы сотовой связи через Интернет или курьерской доставкой всего массива данных на отдельном носителе.

Чтобы подключиться к сети, SIM-карта авторизуется с использованием этого ключа, сравнивая его с тем, что имеет оператор: если они совпадают, то устанавливается зашифрованное подключение. Поэтому вместо того, чтобы расшифровывать трафик абонентов, агентства выкрали ключи безопасности, чтобы мониторить его в чистом виде.

Имея такие ключи, АНБ и другие правительственные агентства могли следить за пользователями без необходимости получать на это разрешение у самих провайдеров и зарубежных правительств. Чтобы получить доступ к ключам, спецслужбы в том числе следили за сотрудниками Gemalto через Facebook и электронную почту на Google и Yahoo при помощи утилиты X-KEYSCORE.

По словам исполнительного вице-президента Gemalto П. Беверли, ни он, ни остальные сотрудники компании не подозревали о взломе.

«Я встревожен, весьма обеспокоен тем, что это произошло. Главное для меня – это понять, как именно это было сделано, так что мы сможем принять всё необходимое для того, чтобы это не случилось вновь, и также убедиться, что это не повлияет на операторов, которым мы с преданностью служили долгие годы», – заявил П. Беверли, исполнительный вице-президент Gemalto.

Даже спустя сутки после того, как к представителям Gemalto обратилось издание, служба безопасности производителя SIM-карт не смогла

выявить никаких следов проникновения. По словам П. Беверли, АНБ никогда не обращалось к компании с просьбой предоставить им ключи безопасности.

По данным с одного из слайдов GCHQ, британское агентство получило доступ к сети Gemalto, разместив вредоносное ПО на нескольких компьютерах. Кроме того, сотрудники спецслужб смогли проникнуть в системы нескольких неназванных операторов сотовой связи, где они могли узнать информацию об абонентах с компьютеров сотрудников отделов продаж и получить карты зон покрытия из рук технических специалистов ***(АНБ добилось слежки за миллионами абонентов взломом крупнейшего производителя SIM-карт // InternetUA (http://internetua.com/anb-dobilos-slejki-za-millionami-abonentov-vzlomom-krupneishego-proizvoditelya-SIM-kart). – 2015. – 21.02).***

***

Производитель SIM-карт ответил на заявления Э. Сноудена о взломе системы спецслужбами

25 февраля крупнейший в мире производитель чипов для мобильных и банковских карт – голландская компания Gemalto – созвал в Париже пресс-конференцию, чтобы отреагировать на разоблачения Э. Сноудена.

Согласно данным, опубликованным на днях в Интернете, американская и британская разведки провели операцию по взлому компьютерной сети компании. В результате этого в руках спецслужб, как утверждается, оказались ключи шифрования телефонных SIM-карт, а это дает доступ практически к любым разговорам по мобильному. Скандал вышел настолько громким, что в Gemalto вынуждены были объясниться.

Руководство компании Gemalto в основном оправдывалось. Главная претензия к корпорации, мировому лидеру по производству чипов для кредитных карт и сим-карт для мобильных телефонов, заключается в том, что она пять лет хранила молчание, зная о взломе своей внутренней операционной системы еще в 2010 г.

О. Пиу, президент Gemalto: «Ничего подобного раньше не было. И это не походило на кибератаку хакера или мафии».

Оказалось, что взлом организовало американское Агентство национальной безопасности. В результате этого спецслужбы США и Британии получили возможность следить за трафиком миллионов абонентов тайком от сотовых компаний.

Хотя руководство Gemalto несколько раз повторяло, что данные Э. Сноудена во многом ошибочны. Там также заявили, что все не так страшно, как кажется на первый взгляд ***(Производитель сим-карт ответил на заявления Сноудена о взломе системы спецслужбами // Телекомпанія НТВ (http://www.ntv.ru/novosti/1335417/). – 2015. – 25.02).***

***

Несколько дней назад весь Интернет облетела новость о том, что АНБ программным путём внедряет «закладки» в прошивки HDD. Эти зловреды называли чуть ли не «самыми сложными» среди всех вредоносных программ, обнаруженных к настоящему времени. Специалисты «Лаборатории Касперского» проследили связь авторов этого бэкдора и других модулей шпионского фреймворка Equation с авторами Stuxnet.

Но специалисты обращают внимание, что «закладки» в прошивке HDD – не такая уж и новость. Во-первых, этот инструмент из арсенала АНБ упоминается в документах Э. Сноудена. Во-вторых, примеры таких программ как минимум год рассматриваются на хакерских конференциях.

Например, в марте 2014 г. группа восьми исследователей из Eurecom (Франция), IBM Research (Швейцария) и Северо-Восточного университета (США) опубликовала работу Implementation and Implications of a Stealth Hard-Drive Backdoor, которая почти в точности повторяет описание вредоносной программы из отчёта «Лаборатории Касперского».

Один из авторов работы – известный хакер Т. Гудспид, завсегдатай хакерских конференций. В своих выступлениях он часто рассказывал об эксплоите для прошивки HDD, который разработали они с коллегами. Сторонний код можно внедрить в прошивку даже не имея физического доступа к жёсткому диску. Если иметь такой доступ, то процедура значительно упростится.

Например, см. выступление Гудспида на конференции 0x07 Sec-T в прошлом году: https://www.youtube.com/watch?v=8Zpb34Qf0NY.

«Программа может работать как бэкдор», – говорил Т. Гудспид. Именно такой возможностью воспользовалось АНБ.

Бэкдор способен незаметно перехватывать все операции считывания и записи на диск. В этом случае скорость работы HDD снижается примерно на 1 %, что не должно быть заметно для пользователя, говорит Т. Гудспид.

Для внедрения бэкдора в прошивку HDD не требуются какие-то секретные знания. Достаточно публично доступной информации. Т. Гудспид с коллегами по ходу дела успешно взломали около 15 моделей винчестеров от Seagate и Western Digital ***(Бэкдоры в прошивках HDD известны как минимум год // InternetUA (http://internetua.com/bekdori-v-proshivkah-HDD-izvestni-kak-minimum-god). – 2015. – 21.02).***

***

Сотрудники Службы безопасности Украины в Луганской области обвиняют в терроризме гражданина Украины за посты в социальной сети «ВКонтакте».

Об этом сообщили силовики.

По их словам, подозреваемый размещал «ВКонтакте» материалы в поддержку «ЛНР». Подозреваемому 23 года.

Уголовное производство открыто по ч. 1 ст. 258-3 УК Украины (террористический акт с целью нарушения общественной безопасности, устрашения населения, провокации военного конфликта) ***(СБУ Луганской области разоблачила онлайн-террориста // InternetUA (http://internetua.com/sbu-luganskoi-oblasti-razoblacsila-onlain-terrorista). – 2015. – 23.02).***

***

Слідчий Служби безпеки України протягом доби може відкрити кримінальну справу проти автора антимобілізаційного поста в будь-якій соціальній мережі в Інтернеті. Про це йдеться у відповіді СБУ на запит видання «Корреспондент.net».

Інформацію про таке правопорушення слідчий СБУ може отримати від інших осіб або самостійно виявити протизаконний пост в Інтернеті. У тому або іншому випадку співробітник СБУ зобов'язаний протягом 24 годин відкрити кримінальне провадження.

Повідомлення з антимобілізаційним характером кваліфікують за статтею 114-1 Кримінального кодексу (перешкоджання законній діяльності ЗС України та інших військових формувань в особливий період), яка передбачає відповідальність у вигляді позбавлення волі на термін від п'яти до восьми років.

Стаття Кримінального кодексу, за якою СБУ пропонує судити авторів антимобілізаційних повідомлень у соцмережах, дуже розмита і не має підстав для вироку. Таку думку в коментарі «Корреспондент.net» висловив адвокат компанії «Юскутум» Д. Овчаров.

Наприклад, за його словами, якщо журналіст напише щось проти мобілізації, то у статті 114-1 прямо не зазначено, що саме він порушив. Навіть більше, у статті чітко не прописано, що саме є перешкоджанням дії Збройних сил України.

«Стаття 114-1, на яку послалися в СБУ, дуже розмита, а коли немає чіткого розуміння, за що я буду сидіти в тюрмі, то не буде чіткого розуміння й у суду. Тому потрібно дотримуватися поняття «правова відповідальність» – це коли людина знає, за що вона несе покарання», – сказав Д. Овчаров.

Експерт зазначає, що в цьому випадку, щоб судити людину, потрібно мати конкретну статтю Кримінального кодексу, потім згідно з цією статтею провести лінгвістичну експертизу і встановити основні меседжі повідомлення, оприлюднені у соцмережах.

«Але основне тут – наслідки, оскільки стаття 114-1 спрямована саме на них. Потрібно розуміти якими дійсно є наслідки, знайти причинно-наслідковий зв'язок між статтею і її результатами, знайти журналіста і довести, що це він навмисне зробив для перешкоджання роботи Збройних сил України або він сам зізнався. І тільки після цього можна про щось говорити», – сказав юрист.

Він також заявив, що СБУ не уповноважена коментувати норми кваліфікації відповідальності, оскільки не має судової практики як у першій інстанції, так і в інших судах.

Зазначимо, що стаття 114-1 була прийнята у квітні минулого року в рамках Закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за вчинення злочинів проти основ національної безпеки України)» ***(СБУ погрожує в'язницею авторам антимобілізаційних постів у соцмережах // Телекритика (http://www.telekritika.ua/pravo/2015-02-23/104113). – 2015. – 23.02).***

***

Інститут Горшеніна, портал LB.ua звернулися до колег-журналістів, головних редакторів і власників інтернет-ЗМІ з закликом тимчасово відключити можливість коментування матеріалів на своїх ресурсах з метою захисту українського інформаційного простору. Про це йдеться у зверненні, опублікованому на сайті LB.ua.

«Зараз Україна активно протидіє зовнішньої військової агресії, на полях битв наші воїни мужньо захищають нашу Батьківщину. Але Україна також знаходиться під впливом інформаційної агресії, на яку нападаюча сторона витрачає величезні ресурси. Інформаційна війна ведеться з не меншою запеклістю, ніж артобстріли і танкові атаки на полі бою. Одним з інструментів інформаційної та пропагандистської війни є інтернет-ЗМІ. Кількість ботів країни-агресора, які коментують на сторінках українських інтернет-ресурсів, безпрецедентно. За допомогою коментарів сіються панічні настрої в суспільстві, розпалюється міжнаціональна ворожнеча, дискредитується українська влада, здійснюється вкидання дезінформації військового і політичного характеру», – зазначається у зверненні.

З огляду на це Інститут Горшеніна і портал LB.ua закликають всі українські інтернет-ЗМІ тимчасово, на період війни, відключити можливість коментування матеріалів на своїх ресурсах.

«Таким чином, ми частково захистимо наш інформаційний простір від пропагандистської та інформаційної агресії», – упевнені ініціатори звернення.

Портал LB.ua також запевняє, що відключення можливості коментування не впливає на відвідуваність сайту. «Рік тому ми прийняли рішення відключити функцію коментування під матеріалами порталу LB.ua. Для нас стало очевидним, що функція коментування матеріалів на сайті втратила свій початковий сенс – вільний обмін думками між читачами, який би доповнював зміст кожного тексту. Побоювання редакторів, що це вплине на відвідуваність ресурсу, не виправдалися – свою аудиторію ми зберегли. Обговорення матеріалів було перенесено в соціальні мережі і орієнтоване на сфокусовану аудиторію», – підкреслюють у LB.ua.

Інститут Горшеніна і портал LB.ua сподіваються, що ініціатива буде прийнята з розумінням у колег і отримає підтримку у РНБО та Міністерства

інформаційної політики ***(Інститут Горшеніна і портал LB.ua заликають відключити коментарі на сайтах, аби позбавити роботи «кремлівських троллів» // Телекритика (http://www.telekritika.ua/kontekst/2015-02-23/104083). – 2015. – 23.02).***

***

Администрация соцсети Twitter заявила о готовности к переговорам с Роскомнадзором, сообщил interfax.ru пресс-секретарь российского ведомства В. Ампелонский 24 февраля.

По его словам, в частности, компания согласилась проработать вопрос определения суточной посещаемости популярных российских аккаунтов на уровне технических специалистов. «Более подробный и развернутый ответ администрация компании обещала предоставить позже», – уточнил В. Ампелонский.

13 февраля Роскомнадзор направил официальный запрос администрации Twitter с просьбой разъяснить позицию соцсети в связи с последовательным невыполнением положений российского законодательства, в том числе законов, направленных на противодействие экстремизму.

Ранее глава Роскомнадзора А. Жаров заявил, что Twitter систематически не выполняет требования законодательства РФ. При этом глава ведомства привел данные официального отчета компании, согласно которым социальная сеть в прошлом году удовлетворила почти 3 тыс. запросов правительства США о раскрытии личной информации пользователей.

«Из 108 запросов на раскрытие данных о посещаемости аккаунтов популярных пользователей, направленных администрации соцсети Роскомнадзором, не удовлетворен ни один. У нас возникает закономерный вопрос о приемлемости такой позиции для компании, которая осуществляет свою деятельность на территории РФ», – сказал А. Жаров ***(Twitter пошел на диалог с Роскомнадзором // МедиаБизнес (http://www.mediabusiness.com.ua/content/view/42552/118/lang,ru/). – 2015. – 24.02).***

***

У Міністерстві зв’язку та інформатизації Білорусі блокуватимуть доступ до проксі-серверів та анонімних мереж, що дають змогу отримувати доступ до заборонених на території країни інтернет-ресурсів.

Про це пише сайт dev.by з посиланням на постанову Оперативно-аналітичного центру при президенті Білорусі та Міністерства зв’язку та інформатизації від 19 лютого 2015 р.

Цей документ детально регламентує порядок обмеження доступу користувачів до інтернет-ресурсів на території Білорусі.

«Державна інспекція при виявленні інтернет-ресурсів, засобів забезпечення анонімності (проксі-сервери, анонімні мережі типу Tor та інші), що дають можливість користувачам інтернет-послуг отримувати доступ до інтернет-ресурсів, ідентифікатори яких включені у список обмеженого доступу, додає у список обмеженого доступу ідентифікатори цих інтернет-ресурсів, засобів забезпечення анонімності», – ідеться в тексті постанови.

Також до ресурсів обмеженого доступу, згідно з документом, належать: ті, власники яких протягом року отримали два і більше письмових попередження від Міністерства інформації; такі, що містять інформацію про незаконний обіг наркотиків або інші заборонені законом відомості; ті, що не виконали вимогу державного органу про усунення порушень законодавства про ЗМІ.

Документ зобов'язує інтернет-провайдерів обмежувати доступ до ресурсів, занесених до «чорного списку» та визначати відповідальних за їх використання. Крім того, постачальників інтернет-зв'язку зобов'яжуть

Раніше в Білорусі було прийнято «антинаркотичний декрет», який дозволяв оперативно обмежувати доступ користувачів до інтернет-ресурсів, що містять матеріали «спрямовані на незаконний обіг наркотиків». Крім того, були прийняті поправки до закону про ЗМІ, згідно з якими будь-який сайт у Білорусі можна прирівняти до ЗМІ та заблокувати після двох письмових попереджень міністерства в позасудовому порядку ***(У Білорусі влада блокуватиме проксі-сервери // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/media_law/law/u_bilorusi_vlada_blokuvatime_proksiserveri/). – 2015. – 25.02).***

Проблема захисту даних. DDOS та вірусні атаки

Хакери з Росії, України та інших країн викрали приблизно мільярд доларів із 100 банків

Операцію хакерського угруповання з назвою Carbanak вважають однією із найбільших банківських крадіжок у світі.

Загрозу було виявлено пыд час спільного розслідування «Лабораторії Касперського», Європолу та Інтерполу, повідомляє сайт компанії.

Кіберпограбування, що тривало два роки, торкнулося близько 100 фінансових організацій у всьому світі. За словами експертів, організувало його міжнародне угруповання хакерів з Росії, України, низки інших європейських країн, а також Китаю.

Угруповання кіберзлочинців використовувало методи, характерні для цільових атак. Проте, на відміну від багатьох інших операцій, цього разу хакери викрадали гроші напряму із банків, а не від користувачів, підкреслює «Лабораторія Касперського».

Експерти підсумовують, що діяльність Carbanak зачепила близько 100 банків, платіжних систем та інших фінансових організації з майже 30 країн.

Серед них – Росія, США, Німеччина, Китай, Україна, Гонконг, Тайвань, Франція, Іспанія, Норвегія, Польща, Великобританія, Швейцарія, Бразилія та ін.

«Ці атаки слугують черговим підтвердженням того, що зловмисники незмінно експлуатуватимуть будь-яку вразливість у будь-якій системі. У таких умовах жоден сектор не може почувати себе в абсолютній безпеці», – зазначив С. Вірмані, директор центру Інтерполу, що займається розслідуванням кіберзлочинів.

За словами фахівців, найбільші грошові суми було викрадено в процесі вторгнення в банківську мережу. За кожен рейд зловмисники викрадали до 10 млн дол. У середньому пограбування займало від двох до чотирьох місяців: від зараження першого комп'ютера корпоративної мережі до крадіжки коштів та згортання діяльності.

Схема розпочиналася з проникнення в комп'ютер одного працівника за допомогою фішингу. Коли була заражена одна машина, хакери отримували доступ до внутрішньої мережі установи, знаходили комп'ютери адміністраторів грошових трансакцій та розпочинали стеження за їхніми екранами. Угруповання Carbanak дізнавалося таким чином детальну послідовність роботи персоналу банку та могло імітувати звичні дії працівників під час переведення коштів на рахунки шахраїв ***(Хакери з Росії, України та інших країн викрали приблизно мільярд доларів із 100 банків // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/cybersecurity/khakeri_z_rosii_ukraini_ta_inshikh_krain_vikrali_priblizno_milyard_dolariv_iz_100_bankiv/). – 2015. – 16.02).***

***

Разъем Lightning, появившийся в устройствах Apple в 2012 г., до недавнего времени оставался защищенным и полностью безопасным. Однако ничто не вечно: хакерской группе Ramtin Amin удалось получить доступ к ядру iOS, используя для этого фирменный разъем мобильных устройств Apple.

В подтверждение своего успеха хакеры опубликовали видео, в котором можно увидеть процесс и основные принципы взлома Lightning. В перспективе это позволит использовать проприетарный разъем мобильных устройств Apple для джейлбрейка, создателям которого больше не потребуется долго и упорно искать уязвимости для интеграции в систему.

Тем не менее, в настоящее время еще рано бить тревогу или радоваться за джейлбрейкеров. Без цифровой подписи, необходимой для запуска кода на iOS-устройстве, достижение Ramtin Amin выглядит интересным, но пока совершенно не угрожающим пользователям.

Та же уязвимость Thunderstrike при наличии доступа к компьютеру является куда более опасной.

Кроме того, в распоряжении хакеров не оказалось никакой уникальной информации, касающейся разъема Lightning. Все сведения, добытые Ramtin

Amin, уже доступны производителям, обладающим лицензией MFi от Apple. Есть вероятность, что находка позволит производителям несертифицированного оборудования корректно работать с мобильными устройствами американской компании, но эта идея пока также далека от практической реализации ***(Хакеры взломали разъем Lightning // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/khakery-vzlomali-razem-lightning.html). – 2015. – 17.02).***

***

Платежная система Visa готова представить сервис шифрования данных кредитных карт в платежном терминале – токенизацию. Теперь эта возможность будет доступна для интернет-платежей.

Д. Маккарти, директор отдела инноваций в Visa, отметил, что в полной мере сервис шифрования данных будет внедрен в сервис онлайн-платежей от Visa весной текущего года.

Принцип работы токенизации заключается в шифровании номера платежной карты. При обработке транзакции 16-значный номер карты Visa превращается в набор символов. В таком виде реквизиты покупателя будут поступать на сайт торговой точки. Преступник, укравший зашифрованные номера (токены) вследствие кибератаки на интернет-портал, не сможет использовать их для доступа к средствам, потому что системы безопасности смогут зафиксировать повторное использование шифра и отклонить покупку.

Руководство платежной системы намерено шифровать данные платежной карты для каждого магазина отдельно для более эффективной защиты. Так, токены, украденные из одного интернет-магазина, не могут быть использованы в другом даже в случае сбоя в системе безопасности, передает ЛигаФинансы.

Как сообщал MIGnews.com.ua, ранее приостановленные в аннексированном Крыму расчеты по картам международные платежные системы Visa и MasterCard, должны возобновиться на полуострове с 1 апреля с полным запуском Национальной системы платежных карт ***(Visa будет шифровать данные платежных карт в интернете // Mignews.com.ua (http://mignews.com.ua/sobitiya/inworld/4841018.html). – 2015. – 16.02).***

***

Индекс критичности утечек данных (BLI), предоставленный компанией Gemalto, показал, что в 2014 г. по всему миру было скомпрометировано порядка одного миллиарда записей личных данных пользователей. Количество утечек личной информации возросло на 49 %, а число украденных или пропавших данных увеличилось на 78 % по сравнению с 2013 г.

Число похищений пользовательских данных составило 54 % от всех утечек и превысило остальные категории, включая доступ к финансовой

информации. Утечки личной информации составили одну треть самых опасных утечек, которые были охарактеризованы BLI как катастрофические (9,0–10 баллов по шкале BLI). Две трети из 50 самых серьезных похищений были осуществлены в 2014 г.

В розничной торговле количество скомпрометированных данных составило 11 % от всех утечек 2014 г. Данный рост происходит в связи с увеличением числа кибератак на POS-терминалы. Для сектора финансовых услуг количество утечек данных остается относительно стабильным из года в год, но средней показатель увеличился в 10 раз – с 112 тыс. до 1,1 млн ***(В 2014 году злоумышленники похитили 1 миллиард личных данных пользователей // InternetUA (http://internetua.com/v-2014-godu-zloumishlenniki-pohitili-1-milliard-licsnih-dannih-polzovatelei). – 2015. – 17.02).***

***

З 16 лютого близько 10 міських сайтів, що входять в українську мережу City Sites, було піддано DDoS-атаці. Про це повідомляє сайт 0642.ua.

Найбільший удар був нанесений хакерами по сайтах Харкова 057.ua, Запоріжжя 061.ua і Миколаєва 0512.com.ua.

Також постраждали сайти міст Артемівська (Донецька область), Луганська, Сум та ін.

За інформацією служби технічної підтримки мережі, атаки на міські сайти мають випадковий характер. На думку фахівців, хакери наосліп промацують захист ресурсів. Також повідомляється, що сайти Донецька 62.ua і Маріуполя 0629.com.ua – поза досяжністю хакерів.

Нагадаємо, у жовтні минулого року мережа міських сайтів City Sites зазнала потужних DDoS-атак. За даними технічної служби мережі, кібератаки на сайти ведуться з-за кордону. Першим зазнав кібер-атаки сайт Маріуполя 0629.ua, згодом сайти Кривого Рогу, Луганська та Львова. На сайті Кривого Рогу хакери атакували новину про указ Президента П. Порошенка щодо відзначення Дня захисника України 14 жовтня ***(Хакери знову атакували сайти української мережі City Sites // Телекритика (http://www.telekritika.ua/kontekst/2015-02-17/103853). – 2015. – 17.02).***

***

Kaspersky Lab раскрыла первую из известных кампаний кибершпионажа арабского происхождения, основной удар которой направлен на стратегически важные организации в странах Ближнего Востока. Наибольшее число жертв операции, получившей название Desert Falcons, зарегистрировано в Египте, Палестине, Израиле и Иордании, однако немало пострадавших есть и в других странах, в том числе в Украине. В общей сложности арабские кибернаемники атаковали более 3 тыс. пользователей в 50 с лишним странах и украли свыше миллиона файлов.

Пустыня Соколы целенаправленных атак

Кибернападениям подверглись правительственные учреждения, особенно те их сотрудники, которые отвечают за предотвращение отмывания денег, а также занимаются вопросами здравоохранения и экономического развития. Целью киберпреступников стали также военные ведомства, ведущие СМИ, исследовательские и образовательные учреждения, энергетические компании и коммунальные предприятия, активисты и политические лидеры, охранные агентства, а также ряд других организаций, владеющих важной геополитической информацией.

Кампания кибершпионажа Desert Falcons находится в активной фазе по меньшей мере два года. Несмотря на то что первые атаки были зафиксированы в 2013 г., к разработке и планированию кибероперации злоумышленники приступили еще в 2011-м. Пик активности Desert Falcons пришелся на начало 2015 г.

Эксперты Kaspersky Lab предполагают, что организаторами атак являются хакеры арабского происхождения: группа из приблизительно 30 человек разбита на три команды, которые ведут свою деятельность в разных странах.

Основным способом доставки вредоносного ПО на компьютеры пользователей является целевой фишинг. Организаторы DesertFalcons отправляют потенциальным жертвам сообщения с вредоносными вложениями или ссылками по электронной почте, в социальных сетях или чатах. При этом киберпреступники маскируют зловреды под легитимные приложения. Так, они используют специальный прием, позволяющий менять порядок символов в названии файла на обратный, благодаря чему файловое разрешение, очевидно указывающее на вредоносную программу (.exe или .scr), оказывается в середине названия, а в конце появляется набор символов, характерный для безобидного ПО: например, файл, чье название оканчивается на .fdp.scr, после подобной обработки будет выглядеть как .rcs.pdf.

В случае успешного заражения компьютера жертвы атакующие используют либо основной троянец Desert Falcons, либо DHS бэкдор. Оба зловреда созданы киберпреступниками «с нуля» и находятся в процессе постоянной доработки. Эксперты Kaspersky Lab выявили более 100 различных образцов вредоносного ПО, используемого злоумышленниками в этой операции. С их помощью хакеры делают снимки экранов, перехватывают нажатия клавиш на клавиатуре, загружают и скачивают файлы, собирают информацию обо всех имеющихся на компьютере файлах в форматах Word и Excel, крадут пароли и делают аудиозаписи. Кроме того, были найдены следы активности вредоносного ПО, напоминающего по своему функционалу бэкдор для Android, который способен красть информацию о звонках с мобильного телефона и sms.

«Организаторы этой кампании кибершпионажа крайне целеустремлены, активны, имеют хорошую техническую подготовку и прекрасно понимают политическую и культурную ситуацию. Имея в своем

арсенале лишь фишинговые приемы, социальную инженерию и самодельные зловреды, они смогли заразить сотни компьютеров и мобильных устройств на Ближнем Востоке и заполучить ценную информацию, – отмечает Д. Бестужев, ведущий антивирусный эксперт Kaspersky Lab. – Мы предполагаем, что операция Desert Falcons будет развиваться и дальше, а ее организаторы будут совершенствовать свои методы и инструменты. Например, при достаточной финансовой поддержке они смогут купить или создать эксплойты – и тогда эффективность их атак возрастет» ***(Сокол в пустыне: кампания кибершпионажа затронула более 50 стран // Украинский телекоммуникационный портал (http://portaltele.com.ua/news/internet/sokol-v-pustyne-kampaniya-kibershpiona.html). – 2015. – 18.02).***

***

Антивирусная компания Kaspersky Lab разоблачила деятельность международной группы Equation Group, которая считается лидером в области кибершпионажа, пишет Blog Imena.UA (http://www.imena.ua/blog/equation-group-questions/).

В Интернете в настоящее время свирепствует разработанный ими вирус, который внедряется в зоны жёстких дисков компьютеров и не поддаётся удалению даже посредством форматирования винчестера.

Хакеры, используя данный вредонос, получают возможность беспрепятственно считывать всю необходимую информацию. Аналитики «Лаборатории Касперского» подтвердили уже 30 тыс. фактов инфицирования ПК данным вирусом.

Заражённые компьютерные системы обнаружены в более чем 30 странах, включая Иран, РФ, Пакистан, Афганистан, Китай, Мали, Сирию, Йемен, Алжир, Великобританию, США, Германию, Францию и др.

Рядовые пользователи, впрочем, могут пока что отложить панику. Основные цели слежки вируса – правительственные и военные учреждения, телекоммуникационные и энергетические компании, банки, атомные исследовательские центры, СМИ и исламские активисты.

Специалисты пока что не выяснили, какая страна или отдельная организация стоит за группировкой Equation Group ***(«Лаборатория Касперского» предупреждает об эпидемии неубиваемого шпионского вируса // Blog Imena.UA (http://www.imena.ua/blog/equation-group-questions/). – 2015. – 17.02).***

***

Зловмисники зламали сайт Львівської обласної ради та встановили на ньому пропаганду самопроголошеної ДНР.

«Звісно, програвати завжди погано. Звісно, це біда для тих, хто програв. Особливо, коли програєш вчорашнім шахтарям чи трактористам», – такі титри містяться в ролику.

Вони є цитатою російського президента В. Путіна. Так він висловився під час спільної із прем'єр-міністром Угорщини Ві. Орбаном прес-конференції.

У Львівській обласній раді підтвердили, що їхній сайт зламали. Прес-служба заявляє, що фахівці працюють над відновленням ресурсу.

Нагадаємо, восени на сайті Астраханської обласної державної думи невідомі особи розмістили повідомлення про вихід Астраханській області зі складу Росії ***(Хакери розмістили на сайті Львівської облради пропаганду «ДНР» // Osvita.MediaSapiens.ua (http://osvita.mediasapiens.ua/web/cybersecurity/khakeri_rozmistili_na_sayti_lvivskoi_oblradi_propagandu_dnr/). – 2015. – 18.02).***

***

Тот факт, что Android сегодня является самой подверженной вирусным атакам мобильной операционной системой, оспорить невозможно. Опытные пользователи при этом редко сталкиваются с вредоносным ПО, однако процент зараженных устройств высок. На самом деле очень высок, если обратиться к последним данным от Alcatel-Lucent Motive Security Labs. Все идет к тому, что в ближайшие годы количество зараженных устройств на Android превысит даже количество зараженных компьютеров на Windows.

ZDNt сравнили данные исследовательской компании с показателями 2013 г. Количество зараженных Android-устройств успело возрости на 25 %, а это не менее 16 млн смартфонов и планшетов. Иными словами, 0,68 % устройств во всем мире работают с вредоносными программами, которые в большинстве своем собирают данные о владельцах устройств, информацию об их звонках, сообщениях и местоположении.

Google наверняка расскажет нам о своих данных, касающихся количества зараженных устройств в рамках грядущего Google I/O. Если верить Motive Security Labs, компания склонна недооценивать реальное количество случаев заражения. Только во второй половине 2014 г. было замечено столько же зараженных Android-устройств, сколько и ноутбуков под управлением Windows ***(Android догоняет Windows по количеству вредоносного ПО // InternetUA (http://internetua.com/Android-dogonyaet-Windows-po-kolicsestvu-vredonosnogo-po). – 2015. – 20.02).***

***

На Android появился вирус, который шпионит за пользователем даже после выключения смартфона

Аналитическая компания AVG рассказала об Android-вирусе, который может продолжать использовать ресурсы смартфона вроде камеры и GSM-модуля даже после отключения устройства.

Как отмечают специалисты AVG, в действительности смартфон, заражённый вредоносным кодом, не выключается. Вирус встраивается в сам

процесс завершения работы, показывает пользователю соответствующую анимацию и деактивирует дисплей, вибрацию и звуковые сигналы.

После этого на первый взгляд выключенный смартфон превращается в шпионское устройство: хакер может удалённо записывать звук, делать снимки, а также отправлять сообщения.

AVG, обнаружившая угрозу, назвала вирус Android/PowerOffHijack.A. Он поражает устройства на Android ниже версии 5.0 и требует root-доступа (прав администратора), так что пользователи с «заводской» сборкой этой ОС риску не подвержены.

По прикидкам AVG, PowerOffHijack.A поразил уже более 10 тыс. устройств, преимущественно находящихся в Китае. В этой стране он распространяется в местных неофициальных магазинах приложений.

AVG отмечает, что её антивирусные решения уже могут обнаружить и устранить новый вирус, однако всё же рекомендует владельцам Android-смартфонов не рисковать и извлекать батарею из устройств в тех случаях, когда надо гарантировать их отключение.

В последние годы сообщения об изощрённых вирусах для iOS и Android – не редкость, однако в большинстве случаев они требуют, чтобы устройство было изначально взломано самим пользователем (root-доступ в случае Android, джейлбрейк – в случае iOS) ***(На Android появился вирус, который шпионит за пользователем даже после выключения смартфона // InternetUA (http://internetua.com/na-Android-poyavilsya-virus--kotorii-shpionit-za-polzovatelem-daje-posle-vikluacseniya-smartfona). – 2015. – 20.02).***

***

Как понять, что за вами шпионят, и защититься от хакера

Каждый раз, когда появляется очередная новость о том, что спецслужбы следят за компьютерами и смартфонами, мы думаем, что нам такая слежка не страшна. Действительно, вряд ли наша переписка или фотографии интересны ЦРУ и ФСБ. Эта информация может представлять интерес только для тех, кто знаком с нами лично и хотел бы знать о нас больше. Не исключено, что среди таких знакомых есть те, кто умеет взламывать почту или настраивать на компьютере перехватчики сообщений, тем более, что для этого не требуется много ума. Проверить, следят ли за вами, иногда бывает полезно – вдруг и правда следят.

Слежка по телефону

Некоторые операторы предоставляют услугу по отслеживанию местоположения чужого телефона. Предполагается, что его владелец ваш близкий родственник (ребенок или супруг/супруга) и дает на это согласие оператору отправкой sms на определенный номер. Если вы оставите телефон без присмотра, такой жучок может появится и без вашего ведома – кто-нибудь отправит sms-сообщение, сотрет его и будет следить за вашими перемещениями. Проверить, подключена ли вам такая «услуга», можно в

личном кабинете на сайте оператора, но лучше – позвонив на номер техподдержки.

Если вы пользуетесь смартфоном на базе Android, то ваше перемещения можно отследить на сайте Google, нужно лишь знать ваш пароль. Подозреваете, что ваш пароль известен кому-то еще – поменяйте его.

Доступ к облачным хранилищам

Возможно, вы с другом смотрели совместные фотографии на компьютере и он решил перекинуть их вам в облако со своего компьютера. Даже если он потом разлогинился, не факт, что компьютер не запомнил пароль. В большинстве облачных сервисов можно посмотреть, каким устройствам разрешен доступ. Зайдите в настройки и удалите все сомнительные компьютеры и приложения. Если видите, что заходил кто-то посторонний, поменяйте пароль.

Слежка в соцсетях

Пароли от аккаунтов в соцсетях подбирают и воруют все кому не лень. «ВКонтакте» можно посмотреть последние действия с аккаунтом: с какого IP-адреса, компьютера или приложения заходили. Если вы обнаружили подозрительную активность, просто завершить все сеансы недостаточно, нужно поменять пароль, а можно еще и настроить двухфакторную аутентификацию.

Чтение почты

Взлом почты – самое простое и порой единственное, на что способны доморощенные хакеры. Проверьте IP-адреса в истории входа. Даже если нет ничего подозрительного, все равно поставьте двухфакторную аутентификацию с помощью приложения (Google Authenticator или Яндекс.Ключ) или кода, который приходит по sms.

Перехват переписки на компьютере

Обнаружить на компьютере трояна, который перехватывает все, что вы пишете, делает скриншоты и отправляет их куда-то, визуально бывает трудно – как правило, он скрыт и из запущенных процессов, и из списка установленных программ. В этом случае пригодится какой-нибудь хороший антивирус (например Avast) – он найдет трояна, заблокирует и удалит.

Как обезопасить себя от взлома и слежки?

Помимо банальных советов, вроде «не храните пароль от почты на листочке, прикрепленном к монитору» и «не используйте легкие пароли типа 123456» мы можем дать еще несколько:

– Заведите менеджер паролей. Он позволит вам не запоминать сложные комбинации цифр и букв, но все все время хранить их под рукой. Вход в такой менеджер нужно защитить паролем.

– Удаляйте из почты письма, в которых в открытом виде содержатся пароли. Особенно, если вы используете один и тот же пароль на разных сайтах и сервисах. Очищайте корзину вручную.

– Избегайте ввода данных от почты, соцсетей и облачных сервисов в сторонних приложениях. Одно дело, кода приложение просто предлагает вам

подтвердить вход нажатием кнопки ОК в вашем аккаунте и совсем другое – когда оно открывает какое-то окно и просит ввести логин и пароль. Нет никакой гарантии, что эти данные не уйдут злоумышленникам.

– Когда продаете смартфон, планшет или компьютер, сотрите с него всю личную информацию, переустановите операционную систему (или сбросьте ее к заводским настройкам), а затем пройдитесь шредером – программой, которая несколько раз перезапишет удаленные файлы случайной информацией ***(Как понять, что за вами шпионят, и защититься от хакера // InternetUA (http://internetua.com/kak-ponyat--csto-za-vami-shpionyat--i-zasxititsya-ot-hakera). – 2015. – 20.02).***

***

Обнаруженная летом 2014 г. уязвимость BadUSB стала одной из горячих тем в сфере кибербезопасности. Брешь позволяла злоумышленнику перепрограммировать периферийные устройства, подключающиеся через USB-порт. Подключив такой аксессуар к компьютеру, хакер мог полностью скомпрометировать систему.

Как сообщает ThreatPost, подобные атаки могут затронуть промышленное оборудование. Во время саммита Kaspersky Lab Security Analysts Summit специалист Context Industrial Security М. Токер объяснил, каким образом уязвимость может быть проэксплуатирована на промышленных устройствах. Эксперт заявил, что злоумышленник теоретически может скомпрометировать систему с помощью переходников с USB на 9-контактный последовательный разъем.

Токер говорит, что инженеры промышленных систем предпочитают использовать 9-контакные последовательные разъемы вместо сетей Ethernet. Эксперт решил проверить безопасность такого способа соединения устройств.

Для того чтобы подтвердить свою теорию, Токер приобрел 20 различных переходников в online-магазинах, разобрал их и использовал ряд ресурсов, чтобы перепрограммировать их в стиле BadUSB. Большая часть устройств (15 из 20) не позволяла их перепрограммирование и была неуязвима к атакам по BadUSB.

Остальные переходники оказались подвержены атаке. К примеру, Texas Instruments TUSB3410 позволял себя перепрограммировать. По словам М. Токера, это позволяет взломщику модифицировать прошивку устройства, что позволит ему выполнять произвольный код.

У TUSB3410 есть два сценария работы. В первом случае прошивка извлекается из чипа на плате, во втором – из драйвера на хост-машине. Токер говорит, что в этой ситуации драйвер предоставляет устройству прошивку, после чего запускает ее и следует инструкциям микропрограммы ***(Уязвимость BadUSB может затрагивать промышленное оборудование // InternetUA (http://internetua.com/uyazvimost-BadUSB-mojet-zatragivat-promishlennoe-oborudovanie). – 2015. – 19.02).***

***

Пользователи устройств производства Apple оказались подвержены крупной уязвимости Masque Attack II (MA2), которая позволяет вредоносным приложениям маскироваться под существующие программы для дальнейшего распространения вредоносного ПО. В отличие от первого варианта уязвимости, MA2 включает в себя похищение URL-схем iOS, что позволяет распространять вредоносное ПО напрямую через App Store. Об этом сообщает компания FireEye, которая в ноябре прошлого года обнаружила первый вариант уязвимости.

По словам специалистов FireEye, MA2 специально применяет те же URL-схемы, которые используются в других приложениях. Создавая и распространяя вредоносное ПО с корпоративной подписью, которое регистрирует URL-схемы, аналогичные использующимся в легитимных программах, злоумышленники могут похищать их URL-схемы. Это позволяет вредоносному ПО имитировать интерфейс других приложений, что может использоваться для осуществления фишинговых атак. iOS не обеспечивает защиту пользователей от подобных атак, поскольку ОС не запрашивает подтверждения действия при запуске приложения с корпоративной подписью через URL-схему в первый раз.

Одно из обнаруженных исследователями вредоносных приложений использовало одинаковый набор URL-схем на iOS 8.1.3. Оно позволяло похищать веб-ссылки, когда пользователь переходит по ним в приложении Gmail, браузере Safari или через sms-сообщения.

Оказалось, что уязвимость была преднамеренной. App Store и iOS разрешают приложениям от разных разработчиков использовать одинаковые URL-схемы.

MA2 также позволяет обойти запрос iOS на подтверждение действий пользователя, но это было исправлено в iOS 8.1.3. Когда пользователь открывает приложение с корпоративной подписью, система запросит у него разрешение на запуск. Обход этого запроса позволяет вредоносным приложениям эксплуатировать уязвимость без ведома пользователя.

Несмотря на то, что Apple выпустила исправление безопасности, большое количество пользователей до сих пор остаются подвержены уязвимости. 28 % iOS-устройств до сих пор используют устаревшую версию iOS 7. К тому же, далеко не все пользователи, установившие iOS 8, имеют обновление 8.1.3. ***(Уязвимость Masque Attack II позволяет атаковать пользователей iPhone через App Store // InternetUA (http://internetua.com/uyazvimost-Masque-Attack-II-pozvolyaet-atakovat-polzovatelei-iPhone-cserez-App-Store). – 2015. – 22.02).***

***

Компания Twitter представила новую функцию под названием TweetDeck Teams, которая поможет пользователям общаться между собой, не передавая пароли.

TweetDeck Teams предоставляет возможность делегировать различные уровни доступа к учетной записи Twitter тем, кому пользователь посчитает нужным, и убирать доступ в любое подходящее для него время. Пользователю будет приходить уведомление на телефон о том, что он должен внести изменения в настройках пароля и логина. Данная двухфакторная система аутентификации поможет защитить пароли от злоумышленников.

Учетные записи в Twitter не раз подвергались хакерским нападением. Напомним, что ранее стало известно о взломе аккаунта финансового директора Twitter. Кроме того, группировка «Киберхалифат» угрожала М. Обаме и всей ее семье, взломав учетную запись издания Newsweek. Именно популярность Twitter среди злоумышленников говорит о необходимости внесения дополнительных мер в систему безопасности личных данных пользователей сети микроблогов ***(Новая функция в Twitter поможет защитить пароли от похищения // InternetUA (http://internetua.com/novaya-funkciya-v-Twitter-pomojet-zasxitit-paroli-ot-pohisxeniya). – 2015. – 20.02).***

***

В последнее время кибербезопасность стала ключевым вопросом в сфере платежей и коммерции. Независимо от рода деятельности, компании обсуждают случаи взлома системы безопасности и методы защиты своих предприятий от этой угрозы. В первую очередь, компании стараются защитить электронную почту своих пользователей. Ведущая платежная компания PayPal рассказала о том, как защищает своих клиентов от мошеннических писем.

В блоге компании PayPal на прошлой неделе старший консультант по интернет-безопасности Д. Адамс сообщил о том, чем компания занималась последние шесть лет в области кибербезопасности и как она продолжает эту деятельность совместно с крупными игроками в отрасли. Ссылаясь на стандарт безопасности, который был принят во всей отрасли для защиты адресов электронной почты клиентов от мошеннических атак, Д. Адамс рассказал об основных акцентах PayPal.

«Мы посвятили решению этой проблемы шесть лет. Благодаря нашей усердной работе, безопасность электронной почты клиентов стала действительно выше», – пишет Д. Адамс. «Наша работа привела к созданию DMARC (спецификация, предназначенная для снижения количества спамовых и фишинговых электронных писем, основанная на идентификации почтовых доменов от правителя. – Ред.), и мы видим, как она защищает наших клиентов. Хотя это всего лишь один из многих видов атак, PayPal может теперь переключить свое внимание на реализацию следующих проектов и работать над защитой наших клиентов от всех видов атак».

Стандарт безопасности DMARC используется и другими известными и крупными компаниями: Google, Microsoft, Yahoo. Недавно к ним

присоединились также Facebook, LinkedIn и Twitter, а также 7 из 10 крупнейших финансовых учреждений США ***(PayPal ведет войну с кибермошенничеством // ООО «Центр информационной безопасности» (http://www.bezpeka.com/ru/news/2015/02/24/paypal-protects-customers-from-fake-email.html). – 2015. – 24.02).***

***

Руководство LinkedIn согласилось заплатить 1,25 млн дол. компенсации после слушаний в суде, связанных с групповым иском, пишут Новости ИТ.

По мнению авторов иска, руководство соцсети нарушило права клиентов, когда позволило злоумышленникам похитить личные данные пользователей платных услуг службы.

В июне 2012 г. компания заявила, что группа хакеров из России похитила пароли более чем 6 млн пользователей. Таким образом, в руках преступников оказались учётные данные более чем 5 % клиентов социальной сети. Вскоре после этого один из пользователей инициировал подачу группового иска, утверждая, что администрация LinkedIn нарушила собственные условия соглашения.

Из отчёта о взломе стало известно, что LinkedIn не использовала так называемую “соль”, то есть случайное изменение хеша хранимых паролей, что на порядок уменьшило уровень защищённости пользователей. Персональные данные пользователей были похищены с помощью SQL-инъекции, которая позволила хакерам подключиться к базе данных соцсети через веб-сайт.

На выплаты могут претендовать пользователи, которые оплачивали премиум-подписку в LinkedIn в период с 15 марта 2006 г. по 7 июня 2012 г. В общей сложности будет выплачено 1,25 млн дол., которые будут распределены между пострадавшими, а также правозащитными общественными организациями.

Для получения компенсационных выплат необходимо подать заявление, получаемая сумма будет зависеть от количества жертв, которые заявят на свои права. Если каждый пользователь получит меньше 10 дол., общая сумма будет пересмотрена.

В своём заявлении представители LinkedIn заявили, что компания согласилась на компенсацию «во избежание отвлечения и расходов от судебного процесса» ***(LinkedIn выплатит пользователям $ 1,25 миллиона за утечку личных данных // Новости ИТ (http://www.novostiit.net/linkedin-vyiplatit-polzovatelyam-1-25-milliona-za-utechku-lichnyih-dannyih-00016429). – 2015. – 25.02).***

***

В последнее время пользователи Facebook становились жертвами массивной спам-кампании, в рамках которой жертве предлагается узнать, как

она будет выглядеть через 20 лет. Для этого им следовало перейти по ссылке, ведущей на якобы официальную страницу приложения, и ввести свои учетные данные.

По данным Online Threat Alerts, к сообщению-приманке была прикреплена фотография с актрисой К. Холмс, состаренной примерно на 20 лет. Оно также содержало ссылку, ведущую на вредоносный ресурс. Сайт имитировал страницу входа в учетную запись Facebook и требовал ввода логина и пароля. Таким образом злоумышленники похищали учетные данные жертв и использовали их страницы для дальнейшей рассылки спама.

В настоящее время сайт, с которого осуществлялось хищение личных данных, был закрыт. Пострадавшим от спам-кампании пользователям следует незамедлительно сменить пароль. Если это невозможно, жертва может уведомить администрацию Facebook о взломе своей страницы ***(Поддельное приложение для Facebook похищает учетные записи пользователей // InternetUA (http://internetua.com/poddelnoe-prilojenie-dlya-Facebook-pohisxaet-ucsetnie-zapisi-polzovatelei). – 2015. – 25.02).***

***

Європол викрив групу кіберзлочинців, яка контролювала мільйони комп’ютерів

Група кіберзлочинців, яка захоплювала сервери та крала банківську інформацію, була зупинена європейською поліцією. До операції долучились і технологічні компанії.

Операцією керував Центр боротьби з кіберзлочинністю Європолу зі своєї штаб-квартири в Гаазі. Таким чином було завдано удару по так званому ботнету Ramnit, мережі комп’ютерів, заражених шкідливими програмами, повідомляє інформаційне агентство Reuters.

Центр працював зі слідчими з Німеччини, Італії, Нідерландів та Великобританії. В операції також взяли участь компанії Anubisnetwork, Microsoft і Symantec, які повідомили, що близько 3,2 млн комп’ютерів були зламані.

«Ми працювали разом, щоб вимкнути контрольні сервери мережі в різних країнах Європейського Союзу», – розповів начальник відділу операцій у Центрі боротьби з кіберзлочинністю П. Гіллен. У результаті злочинці втратили контроль над інфраструктурою, яку вони використовували.

Програми шкідники, встановлені через необережне поводження зі спамом або зараженими веб-сайтами, давали змогу хакерам брати під контроль комп’ютери й використовувати їх для злочинної діяльності.

Комп’ютери по всьому світу були заражені цим ботнетом, але більшість припадала на Великобританію. Зараження почалося ще у 2012 р.

Слідство триває, тому П. Гіллен сказав, що він не може прокоментувати можливі арешти підозрюваних, оскільки це може зашкодити поліцейським операціям ***(Європол викрив групу кіберзлочинців, яка контролювала мільйони комп’ютерів // InternetUA***

(http://internetua.com/vropol-vikriv-grupu-k-berzlocsinc-v--yaka-kontroluavala-m-lioni-komp-uater-v). – 2015. – 26.02).

***

Увечері 23 лютого одеське інтернет-видання «Таймер» зазнало потужної DDoS-атаки. Про це з посиланням на головного редактора сайту Ю. Ткачова повідомляє Інститут масової інформації (ІМІ).

Видання відновило роботу тільки наступного дня після інциденту. За словами Ю. Ткачова, унаслідок кібератаки на «Таймері» тимчасово неможливо прочитати окремі матеріали. Їх планують відновити з резервних копій.

«Дізнатися, звідки йшла атака неможливо в принципі: при таких атаках запити відправляють комп'ютери з усього світу, в тому числі, часто і без відома своїх власників. Атаки на нас відбуваються досить часто, дуже потужна була восени, більш дрібна – у грудні. Але наша система безпеки побудована так, що менш потужних атак ні ми, ні читачі просто не помічають», – прокоментував головний редактор.

ІМІ зазначає, що редакційна політика сайту «Таймер» відрізняється від загальнодержавних поглядів на політику та події у країні. Зокрема, представників «ДНР» та «ЛНР» на «Таймері» називають «повстанцями», а українські війська – «урядовими».

Наприклад, 25 лютого видання пише про продуктову паніку в Одесі, критикує «поліцейську державу», яка виникла після Революції Гідності. Видання також повідомляє, що «опозиційні ЗМІ України були закриті, а журналісти неугодних каналів побиті, вигнані і позбавлені акредитації». Як «закриті ЗМІ», «побиті» і «позбавлені акредитації» наводяться справи Р. Коцаби і А. Захарчука. Видання також пише про зростання членських рядів партії С. Тігіпка «Сильна Україна». Тих мешканців області, які пропонують визнати Росію країною-агресором, видання називає глузливо «патріотами» в лапках.

Нагадаємо, у моніторингаї сайту MediaSapiens «Таймер» згадувався в переліку ЗМІ, що контролювалися проросійськими бізнесменами й політиками та однозначно висловили підтримку ідеям федералізму та сепаратизму, засуджували «війну проти власного народу» та давали схвальну оцінку діям Росії. Одеський «Таймер», луганські канал ЛОТ, видання «Схід. Інфо», «XXI Век» і «0642», газета Донецької обласної ради «Жизнь» та інтернет-сайт «Комитет» найбільш явно транслювали міфи й стереотипи російської пропаганди ***(Одеське антиурядове і проросійське видання «Таймер» зазнало DDoS-атаки // Телекритика (http://www.telekritika.ua/kontekst/2015-02-25/104206). – 2015. – 25.02).***

***

Европейский регулятор обвинил Facebook в нарушении положений Евросоюза о защите данных, следует из опубликованного по заказу

Бельгийского управления по защите информации доклада «От социальных медиа до рекламной сети».

Доклад посвящен критическому анализу последних обновлений политики Facebook и условий для пользователей. Бельгийские эксперты утверждают, что функции личных настроек в соцсети слишком сложны для пользователей.

Доклад под названием «От социальных медиа до рекламной сети» был опубликован в понедельник, 23 февраля, по заказу Бельгийского управления по защите информации и посвящен критическому анализу последних обновлений политики Facebook и условий для пользователей.

В исследовании приняли участие специалисты Католического университета в Левене и Свободного университета Брюсселя. Его результаты будут использованы при расследовании, которое в январе 2015 г. начала Бельгийская комиссия по защите личных данных. Если комиссия сочтет, что имели место нарушения законодательства, то она отправит материалы в прокуратуру, которая примет решение о возбуждении дела.

В докладе рассматриваются изменения в функциях личных настроек Facebook, а также в условиях предоставления услуг, которые вступили в силу с 31 января 2015 г. Представитель комиссии заявила, что основную озабоченность регулятора вызывают программные дополнения к браузерам, реклама и обмен фотографиями через приложения WhatsApp и Instagram, принадлежащие Facebook, пишет The Wall Street Journal.

В документе говорится, что мощности соцсети по обработке информации «используются для создания масштабной рекламной сети, которая использует данные, собранные как в Facebook, так и вне его, чтобы обращаться и к пользователям Facebook, и к остальным лицам». Исследователи отметили, что компания увечила способность отслеживать поведение пользователей вне соцсети, главным образом через кнопки «нравится» и с помощью функций локализации владельцев мобильных телефонов. Теперь Facebook собирает информацию через эти плагины, независимо от частоты их использования, отмечается в докладе.

В итоге, полагают исследователи, любая информация, добавляемая в Facebook, в конечном счете может быть использована в рекламных целях. «Любой like может привести к тому, что пользователь будет упомянут в материалах, опубликованных на правах рекламы, или в социальной рекламе. Если от упоминания в последней можно отказаться, то единственный способ избежать упоминания в рекламных материалах – это прекратить вообще отмечать понравившиеся публикации. Пользователи оказываются еще более бесправными, потому что они не знают, как именно их данные используются в рекламных целях», – говорится в докладе.

Авторы доклада обращают внимание, что в личных настройках Facebook не дает четких определений в отношении сбора и использовании информации самой соцсетью или сторонними организациями, что дает пользователю ошибочное чувство контроля над своими личными данными.

По словам представителя Facebook, компания недавно обновила пользовательское соглашение, чтобы сделать его более ясным и четким, отразить появление новых функций и показать, как пользователи могут контролировать рекламы. В отношении опубликованного доклада представитель компании заявил, что все обновления соответствуют действующему законодательству.

Как рассказал WSJ источник, знакомый с существом дела, несколько европейских стран ведут переговоры с Facebook по поводу того, что функции личных настроек и пользовательское соглашение не отвечают европейским стандартам защиты информации. В Брюсселе надеются обновить к концу 2015 г. законодательство о защите информации в Евросоюзе. Действующие законы были приняты еще в 1995 г., тогда как Facebook была основана только в феврале 2004 г. ***(Facebook обвинили в нарушении положений Евросоюза о защите персональных данных // Четверта Влада (http://4vlada.net/mass-media/facebook-obvinili-v-narushenii-polozhenii-evrosoyuza-o-zashchite-personalnykh-dannykh). – 2015. – 24.02).***

***

Злоумышленники продолжают использовать «старые» методы для взлома вычислительных систем и проникновения в корпоративные сети. Почти половина (44 %) произошедших в прошлом году инцидентов информационной безопасности были связаны с уязвимостями, которым уже 2–4 года. Об этом свидетельствуют результаты исследования Cyber Risk Report, проведенного сотрудниками подразделения Security Research компании HP.

В опубликованном HP отчете, в частности, отмечается, что самые крупные атаки 2014 г. были проведены с использованием уязвимостей в коде, написанном несколько лет или даже десятилетий назад. При этом далеко не во всех предприятиях внедрена комплексная стратегия применения исправлений в программном обеспечении и поддержания систем в актуальном состоянии. Немаловажным является тот факт, что успешной организации атак злоумышленникам во многом способствовали неверные конфигурации серверов. Согласно результатам исследования, основной проблемой, связанной с неверной конфигурацией, является предоставление слишком широких прав доступа к файлам и папкам. Информация, которую получают злоумышленники, затем используется для совершения других атак.

В 2014 г. киберпреступники активно использовали новые каналы для совершения атак, например, физические устройства, подключенные к сети через «Интернет вещей». Кроме того, наблюдался рост числа вредоносных программ для мобильных устройств. Расширение вычислительной экосистемы играет на руку злоумышленникам, поскольку создает для них еще больше «точек входа» в системы, говорится в отчете.

«Технологии киберзащиты непрерывно совершенствуются, однако мы не должны “терять из виду” старые уязвимости, – говорит А. Гиллиланд,

старший вице-президент и руководитель подразделения Enterprise Security Products, HP. – Мы обнаружили, что самые серьезные риски для безопасности связаны с уязвимостями, о которых мы уже давно знаем. И мы не можем двигаться вперед, забыв об этих проблемах» ***(«Старые» уязвимости по-прежнему представляют собой угрозу кибербезопасности // InternetUA (http://internetua.com/starie--uyazvimosti-po-prejnemu-predstavlyauat-soboi-ugrozu-kiberbezopasnosti). – 2015. – 26.02).***

***

Более миллиона веб-сайтов (хотя представители WordPress говорят о 100 тыс. сайтов) на основе системы управления контентом WordPress оказались подвержены риску атак злоумышленников по причине критической уязвимости плагина под названием WP-Slimstat. Slimstat является инструментом аналитики, скачанным около 1,3 млн раз.

Все версии до недавно выпущенной Slimstat 3.9.6 содержат легко расшифровываемый ключ, используемый для подписи данных, оправляемых и получаемых с компьютеров пользователей. Уязвимость была обнаружена компанией Sucuri.

Результатом уязвимости является возможность SQL-инъекций, которые дают доступ к паролям и ключам шифрования, используемым для удалённого администрирования веб-сайтов. Атаки типа Blind SQL Injection дают доступ к базе данных с логинами, паролями и иногда к файлам WordPress Secret Keys, зачастую дающим полный контроль над сайтом.

Ключ для Slimstat представляет собой всего лишь временную отметку момента установки плагина, зашифрованную алгоритмом MD5. При помощи доступных сервисов можно узнать, когда любой сайт появился в Интернете. Узнав год, нужно протестировать примерно 30 млн числовых вариантов, что займёт всего около 10 мин.

Данная уязвимость WordPress является не первой, подвергающей опасности веб-сайты. Только в конце прошлого года было обнаружено ещё две уязвимости: одна связанная с приложением SoakSoak, другая затрагивала 86 % сайтов на WordPress ***(Множество сайтов на WordPress подвержены уязвимости из-за плагина // InternetUA (http://internetua.com/mnojestvo-saitov-na-WordPress-podverjeni-uyazvimosti-iz-za-plagina). – 2015. – 26.02).***

***

OS X и iOS названы самыми уязвимыми операционными системами

Американская компания GFI Software, которая специализируется на разработке систем защиты от киберугроз, проанализировала данные Национальной базы уязвимостей (NDV) и пришла к интересному заключению: в 2014 г. Windows была более безопасной системой, чем OS X.

Согласно отчету GFI Software, самой уязвимой ОС в 2014 г. стала Mac OS X, втрое место досталось еще одному продукту Apple – iOS, третье место в списке занимают платформы на базе ядра Linux.

По данным NDV за 2014 г., Mac OS X содержала в себе 147 уязвимостей, из которых 64 – повышенной опасности. В iOS было обнаружено 127 уязвимостей, из которых 32 носили критический характер. В системах на базе ядра Linux экспертами было обнаружено 119 брешей, в том числе 24 повышенной опасности.

Windows оказалась более безопасной, хотя и она содержала немало угроз, сообщают авторы отчета. Самая «проблемная» версия ОС от Microsoft – Windows Server 2008 включала в себя 38 уязвимостей, 26 из которых представляли повышенную опасность. Самой безопасной ОС является Windows RT, которая содержала всего 30 уязвимостей, правда 22 из них особо опасные.

Впрочем, Microsoft рано праздновать победу на фронте информационной безопасности. Самым уязвимым приложением по итогам 2014 г. остался Internet Explorer, неизменно лидирующий в подобных списках. 242 уязвимости, 220 повышенной опасности и огромный отрыв от преследователей – результат IE в прошлом году.

Вторую строчку небезопасных приложений занимает Google Chrome со 124 уязвимостями, из которых 85 представляли высокую опасность. Третье место занял еще один браузер – Mozilla Firefox. В нем обнаружено 117 уязвимостей, среди них 57 особо опасных. Adobe Flash Player и Java занимают четвертую и пятую строчки соответственно.

Эксперты GFI Software отмечают, что 2014 г. был непростым с точки зрения информационной безопасности. За прошедший год в базу данных NDV было добавлено 7038 новых уязвимостей, в то время как в 2013 г. эта цифра составляла 4794. 24 % уязвимостей оцениваются как высоко опасные. На долю приложений приходится около 80 % уязвимостей, за 13 % ответственны ОС, 7 % – вклад аппаратной составляющей ***(OS X и iOS названы самыми уязвимыми операционными системами // Ultramir.net (http://ultramir.net/techno/6989-os-x-i-ios-nazvany-samymi-uyazvimymi-operacionnymi-sistemami.html). – 2015. – 27.02).***