СОЦІАЛЬНІ МЕРЕЖІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Огляд інтернет-ресурсів
(16–29.12)

2013 № 24

Соціальні мережі
як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(16–29.12)
№ 24

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

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

Редакційна колегія:
Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Сервис микроблогов Twitter начал тестирование функции Nearby, позволяющей в мобильном приложении сервиса просматривать сообщения других пользователей с привязкой к карте, говорится в блоге издания The Wall Street Journal.

Как сообщает IT Expert со ссылкой на РИА Новости, лента Nearby представлена в виде карты, на которой отображается текущее месторасположение пользователя и отдельными точками помечаются сообщения, отправляемые другими людьми. При этом для просмотра этих твитов не обязательно быть подписанным на отправителя.

Официальный представитель Twitter, к которому обратилось издание, отказался комментировать введение функции Nearby, но эксперты аналитической компании Pivotal Research положительно оценивают ее появление и считают, что она может быть интересной для рекламодателей.

Как сообщает WSJ, возможность добавлять геометку к своим сообщениям появилась в Twitter еще в 2010 г., но эта функция по умолчанию выключена. Введение нового функционала может быть попыткой Twitter привлечь больше пользователей к использованию геолокации, что сделает поиск по микроблогам более удобным, а также позволит компании делать более точные рассылки рекламы ***(Twitter начал показывать сообщения с привязкой к карте // IT Expert (http://itexpert.in.ua/rubrikator/item/32753-twitter-nachal-pokazyvat-soobshcheniya-s-privyazkoj-k-karte.html). – 2013. – 16.12).***

***

Кнопка «Пожертвовать» появилась в социальной сети Facebook. Новая опция будет представлена на страницах благотворительных организаций и в их постах, пишет «Обозреватель» (http://tech.obozrevatel.com/news/69035-v-facebook-poyavilas-knopka-pozhertvovat.htm).

В настоящее время кнопку «Пожертвовать» получили Красный Крест, Американское онкологическое общество и Water.org.

Желающие присоединиться к проекту благотворительные организации должны заполнить заявку на сайте Facebook.

С помощью новой кнопки пользователи могут пожертвовать 10, 25, 100 или 250 дол. В Facebook утверждают, что 100 % полученных таким образом средств будет передано на благотворительность ***(В Facebook появилась кнопка «пожертвовать» // Обозреватель (http://tech.obozrevatel.com/news/69035-v-facebook-poyavilas-knopka-pozhertvovat.htm). – 2013. – 17.12).***

***

Гіперлокальна соціальна мережа «Твоє місто» об’єднає вінничан для спілкування і спільних ініціатив. Ідеологи проекту стверджують, що це перший подібний майданчик в Україні.

Про це йшлося на презентації проекту, передає Укрінформ.

«Є три причини створення цього проекту. Перша – знайомство сусідів: сьогодні люди, живучи в будинках, зовсім не уявляють, хто є їх сусіди. Друга – можливість дізнатися інформацію по будинку: хто старший по будинку, хто є ваш депутат і коли до нього можна звернутися. І третя причина – можливість дізнатися, що є поблизу вашого будинку: дитячі садочки, школи, лікарні», – каже співавтор проекту О. Вірник.

За словами ідеолога проекту, директора муніципально-громадського центру електронного урядування Т. Науменко, проект також допоможе включити активних користувачів соціальних мереж у практичне життя громади, виявити нових лідерів громади, стимулювати прояв та реалізацію місцевих ініціатив.

У майбутньому на цьому сайті також буде реалізовано ряд додаткових інструментів – дошка оголошень, обмін ідеями, музей візуальної історії (будинку, району, міста); музей усної історії будинку (району, міста); історія родини, родинне дерево тощо. Долучитися до віртуальної спільноти міста можливо вже сьогодні, заповнивши реєстраційну форму на сайті.

Довідково. Гіперлокальна соціальна мережа «Твоє місто» створена в рамках проекту ГО «Подільська агенція регіонального розвитку» в партнерстві з інтернет-виданням «Моя Вінниця» та Вінницькою міською радою за підтримки представництва ПРООН в Україні ***(Вінницю об'єднає «власна» соцмережа // RegioNews (http://regionews.ua/node/123364). – 2013. – 16.12).***

***

Разработчики Twitter готовятся внедрить новый сервис, который позволит пользователям редактировать уже опубликованные записи. Об этом сообщает The Desk. Автору твита позволят изменить его только один раз.

Разработчики не сообщают, какой временной промежуток будет предоставляться для редактирования. Запись невозможно будет переписать полностью, будет разрешено лишь исправление опечаток, замена или добавление одного-двух слов.

Если автор исправит свое сообщение, то его действия отобразятся в лентах всех тех, кто «ретвитнул», а также в собственной ленте пользователя.

Завершить разработку нового сервиса планируется за несколько недель. Изначально функция будет доступна для публичных лиц, использующих Twitter. Разработчики объяснили нововведение необходимостью облегчить работу СМИ и других производителей контента.

Ранее в Twitter заявили, что сервис микроблогов будет проверять возраст подписчиков алкогольных брендов. Всех пользователей обяжут указывать возраст перед заходом на страницу ***(Twitter разрешит редактировать опубликованные записи // Полит.Ру (http://www.polit.ru/news/2013/12/17/twitteredit/). – 2013. – 17.12).***

***

Социальная сеть Pinterest, предназначенная для публикации фотографий и видеороликов, запустила русскоязычный интерфейс веб-версии и мобильных приложений, сообщает IT Expert со ссылкой на РИА Новости.

Pinterest, запущенная в 2009 г., позволяет собирать визуальные идеи для разных сфер жизни – например, сделать подборку идей для свадебного торта или подписаться на составляемую другим пользователем коллекцию идей для оформления загородного дома.

Русскоязычные пользователи Pinterest получили доступ к переведенной на русский язык версии сайта, а также приложениям для iOS и Android. В частности, предложены русские версии терминов сайта – сохраненные объекты или закладки называются «пинами», «пользователи-пиннеры» могут сохранить их на собственных «досках». Компании могут использовать Pinterest, чтобы делиться контентом с сообществом соцсети и тем самым увеличивать переходы на свой сайт.

«Идея Pinterest состоит в планировании будущего путем сохранения визуальных ссылок на информацию о путешествиях, дизайнерских решениях и будущих покупках. Россияне демонстрируют живой интерес к познанию нового. Русскоязычная версия Pinterest – это важный для нас шаг: мы стараемся сделать процесс использования Pinterest еще более удобным для российских пиннеров», – говорит директор по международному развитию Pinterest М. Кристал.

Аудитория Pinterest, по данным comScore, превышает 50 млн пользователей. Соцсеть доступна на более чем 20 языках и планирует выпуск новых локализованных версий в 2014 г. ***(Соцсеть Pinterest запустила русскоязычную версию // IT Expert (http://itexpert.in.ua/rubrikator/item/32898-sotsset-pinterest-zapustila-russkoyazychnuyu-versiyu.html). – 2013. – 20.12).***

***

Почему главная проблема Facebook – это ньюсфид

В 2008 г. М. Цукерберг признался, что, по его прикидкам, в ближайшее время количество контента, которым люди делятся на Facebook, будет ежегодно удваиваться (шутники из The New York Times назвали это «Законом Цукерберга», по аналогии с законом Мура). В 2011 г. он еще раз сказал, что количество контента, который генерируют пользователи соцсети, продолжает расти по экспоненте, пишет Marketing Media Review (http://mmr.ua/news/id/pochemu-glavnaja-problema-fejsbuka-eto-njusfid-37685/).

В этом М. Цукерберг абсолютно прав, но с каждым годом становится все очевиднее, что такой бурный рост количества контента никак не помогает Facebook.

Главной целью Facebook всегда было создание сервиса, в котором пользователи могли бы обмениваться любыми типами контента и получать всю необходимую информацию без перехода на другие сайты. То есть

социальная сеть, в идеале, должна была стать для людей синонимом слова «Интернет».

В итоге правильная организация «ньюсфида» стала для Facebook настоящей проблемой. Так, к примеру, считает независимый аналитик Б. Эванс.

В августовском сообщении Facebook была такая фраза: «Каждый раз, когда пользователь открывает свою ленту, для показа ему существует в среднем 1,500 потенциальных историй от друзей, людей и страниц, на которых он подписан, – и у большинства, конечно, нет времени на просмотр всего этого контента. Под историями здесь понимается все от свадебных фотографий лучшего друга, до чекина знакомого в ресторане.

Допустим, пользователь соцсети бодрствует 17 часов в день. Значит, чтобы охватить весь этот контент, ему надо просматривать 88 постов в час или 1,5 поста в минуту. Естественно, это совершенно нереально.

И Facebook осознает наличие проблемы. Соцсеть запланировала грандиозный редизайн, который, по идее, должен был дать пользователям больше контроля над лентой. Увы, тесты на ограниченной группе пользователей показали, что при новом дизайне уменьшается вовлеченность.

С этим надо что-то делать, так что соцсеть вовсю работает над тем, чтобы вычленить из всего многообразия контента самый лучший – и показать пользователю именно его. Результаты этих действий, кстати, многих не радуют (и нас в том числе)».

Все проблемы в ленте новостей. С этим согласен и Б. Эванс, который считает, что главная фича Facebook – его «ньюсфид» – это просто провальный продукт. Они столкнулись с проблемой слишком большого количества контента, с законом М. Цукерберга. «Ньюсфид» стал слишком огромным и рухнул под собственным весом.

Facebook начался как сервис, помогающий уследить за тем, что происходит в жизни друзей, но из-за огромного объема контента в теперешнем «ньюсфиде» пропустить какое-то важное событие из их жизни стало проще простого. Сегодня вы можете запостить фото со своей свадьбы, но благодаря инновационным алгоритмам фильтрации ее увидит половина друзей в лучшем случае.

Конечно, можно улучшить алгоритмы для отбора наилучшего контента, но Б. Эванс считает, что это лишь небольшой хак, который кардинально не изменит ситуацию.

Проблема в продукте. В «ньюсфиде» чересчур много «шума», они просто угробили продукт. И дело не в алгоритмах – все куда серьезнее. Если бы вы получали по полторы тысячи имейлов в день, то не говорили бы, что вам просто нужны алгоритмы получше.

Согласно «закону М. Цукерберга», количество контента продолжит расти. Через год 1,500 постов в ленте запросто могут превратиться в 3,000. И если соцсеть уже сегодня не может переварить весь контент, то что же будет дальше?

Проблемы с «ньюсфидом» особенно заметны в мобильной среде. При использовании смартфона человек не так привязан к соцсети, как на десктопе, где Facebook просто монополизирует внимание пользователя – можно запросто открыть те же WhatsApp, Snapchat или Instagram.

И Б. Эванс считает, что из-за плохой работы «ньюсфида» Facebook такие приложения, помогающие осуществлять какие-то конкретные функции, могут представлять серьезную угрозу для социальной сети. Если пользователь хочет просто посмотреть фотографии друзей, то он пойдет в Instagram или Snapchat. Захочет просто початиться – поможет тот же Snapchat или WhatsApp. Для развлечений можно установить кучу игр, вроде Angry Birds, Candy Crush или QuizUp. Еще пару лет назад все это предполагалось делать именно через Facebook. В настоящее время все перечисленные функции поселились в смартфоне в виде соответствующих приложений, сделав его настоящей социальной платформой.

Возникает вопрос, а как должна работать лента новостей в мобильном приложении Facebook? Должна ли она быть заточена на посты от близких друзей, или стоит реализовать в ней все лучшие функции отдельных приложений? Facebook пока еще не нашел ответ.

Тем не менее, Б. Эванс уверен, что соцсеть останется номером один на десктопах. Однако в мобильной среде все не так просто, и стать единственным победителем будет куда сложнее. И есть еще кое-что, чего компании следует опасаться.

Для Facebook есть опасность превратиться в Yahoo. Миллиарды людей пользуются их продуктом, но всем на него наплевать ***(Почему главная проблема Facebook – это ньюсфид // Marketing Media Review (http://mmr.ua/news/id/pochemu-glavnaja-problema-fejsbuka-eto-njusfid-37685/). – 2013. – 23.12).***

***

В Рунете появилась новая общероссийская социально-информационная сеть «Рустория», ориентированная как на профессиональных журналистов, так и на талантливых любителей и экспертов в различных областях, а также просто на неравнодушных людей, которым есть что сказать.

Инициаторы проекта предлагают авторам вести личные блоги или объединяться в так называемые виртуальные редакции по географическому или тематическому принципу. Они имеют возможность настройки функциональных ролей их участников: главного редактора или журналиста, корреспондента или фотографа.

«Мы придумали виртуальные редакции – такая новая сущность на сайте. В два клика человек может стать главным редактором – писать интересные новости на сайт», – рассказал РИА «Новости» главный редактор «Рустории» Д. Фимин.

При этом в структуре проекта существует и центральная редакция, в задачу которой входит поиск талантливых авторов, привлечение их к участию в проекте, обучение, организация, помощь и поддержка. Отметим,

что основополагающим принципом работы сети, которая задумана как СМИ, ее авторы объявили плюрализм мнений.

Авторы проекта заявили, что не намерены повторять многочисленные новостные ресурсы, чье содержание разнится лишь деталями и временем публикации новостей, и хотят сделать акцент на происходящем в регионах. «В субъектах современной России происходит множество интересных событий и протекает огромное количество важных процессов, которые незаслуженно отодвигаются на второй план», – уверен Д. Фимин.

За свою работу авторы будут получать вознаграждение – за самые интересные, эксклюзивные и популярные новости и репортажи со всей России будут ежемесячно выплачиваться гонорары на сумму 15 млн р.

В открытом доступе соцсеть существует уже около двух месяцев. На самоокупаемость проект должен выйти к концу 2015 г. Как рассказал агентству Е. Храмов, вице-президент финансово-инвестиционной группы «Мортон», на деньги которой создается «Рустория», общий объем инвестиций в проект должен составить около 3 млрд р. А на привлечение аудитории с помощью рекламы, пиар-акций и прочего компания готова ежемесячно выделять еще 25 млн р.

Руководит проектом генеральный директор коммуникационной группы «МедиаШторм» А. Исаев. Он отмечает, что читателям «Рустории» предлагается очень высокий уровень персонализации содержания – учитывается регион проживания пользователя, явные и эмпирически вычисленные интересы, рекомендации и интересы его друзей. На сегодняшний день на такой уровень кастомизации неспособно ни одно российское СМИ.

В течение последних полутора месяцев проект функционировал в тестовом режиме. И к моменту официального объявления о его запуске в «Рустории» уже работают свыше 150 авторов, которые за это время создали больше 15 тыс. материалов ***(В России появилась новая социальная сеть «Рустория», выплачивающая авторам гонорары // InternetUA (http://internetua.com/v-rossii-poyavilas-novaya-socialnaya-set--rustoriya---viplacsivauasxaya-avtoram-gonorari). – 2013. – 22.12).***

***

После смерти человека его электронная почта и аккаунты в социальных сетях не прекращают свое существование: туда продолжают поступать сообщения, письма, комментарии к фотографиям и записям. Часто никто из близких не знает пароля скончавшегося и не может ни закрыть его аккаунт, ни что-то там изменить. Как показывает практика, сегодня в абсолютном большинстве стран эта сфера никак не регулируется. В редких случаях особо сознательные люди заранее оформляют завещание, в котором указывают, что именно необходимо сделать с их электронным архивом, пишет NashaGazeta.ch.

Первыми на проблему обратили внимание американцы. В 2004 г. родители погибшего в Ираке солдата Д. Эллсуорса потребовали, чтобы

Yahoo предоставила им доступ к его электронной почте, чтобы они могли ее удалить. Компания отказалась, заявив, что почтовый аккаунт является ее частной собственностью. Также Yahoo мотивировала свое решение желанием сохранить конфиденциальность частной переписки. Дело дошло до суда, который принял решение в пользу родителей солдата.

Однако частный случай не привел к изменениям в законодательстве. В мире до сих пор нет четкого представления о том, что делать с электронным наследием человека. Почти всегда доступ к нему остается закрытым для родных – наследников во всех других ситуациях.

Электронное наследие – это условный термин, который включает не только личную и деловую переписку, но также фотографии, аудиозаписи, видеофрагменты, дневниковые записи и комментарии. Все это обычно привязано к одному аккаунту и составляет целый пакет данных. Сюда также стоит отнести электронный кошелек и прочие банковские данные.

Родные могут получить доступ к аккаунту умершего или добиться его закрытия или полного удаления данных, но эта процедура занимает несколько лет и стоит очень дорого, отмечает в своем исследовании Э. Брукле-Клей из Цюрихского университета прикладных наук. Пока идут разбирательства, другие пользователи могут оставлять на странице умершего свои комментарии и сообщения, при этом никто не будет проводить модерацию.

Существующие решения

Google на сегодняшний день остается единственной крупной компанией, которая задумалась о возможностях регуляции процесса передачи или уничтожения данных после смерти человека. Пользователи могут заранее указать, как именно следует распорядиться содержимым их аккаунтов. Через Account Manager вы можете назвать имя человека, который получит доступ к данным в случае вашей смерти, при этом уточнив, какие письма или фотографии стоит удалить навсегда, никому их не показывая.

Пока проблема еще не приняла глобальные масштабы, но с ростом числа пользователей естественным образом увеличится и количество неактивных учетных записей. Понимая это, некоторые частные компании уже начали предлагать альтернативные решения. Например, в Швейцарии есть фирмы, которые предлагают услуги по хранению всех данных пользователя на собственном сервере. Таким образом создается резервная копия всех аккаунтов. Пользователь также заранее указывает, что с ними делать после смерти, и все они поступают в распоряжение доверенных лиц ***(Как позаботиться о судьбе своего аккаунта в соцсети после смерти: пока вариантов мало // InternetUA (http://internetua.com/kak-pozabotitsya-o-sudbe-svoego-akkaunta-v-socseti-posle-smerti--poka-variantov-malo). – 2013. – 20.12).***

***

Сотрудники Управления транспортной безопасности США (TSA) разрешили забывшему документы пассажиру зарегистрироваться на рейс по

своему профилю в социальной сети Facebook. Этим пассажиром оказался создатель видеохостинга Vimeo З. Клейн, 22 декабря сообщивший о произошедшем в своем Twitter.

«Добрался до аэропорта и понял, что оставил документы дома. TSA, однако, разрешило мне использовать аккаунт в Facebook», – написал в твите З. Клейн.

Как позднее пояснил разработчик, его случай не является нарушением существующего порядка авиаперевозок. По словам З. Клейна, в правилах, опубликованных на сайте Управления транспортной безопасности, содержится пункт, согласно которому вместо традиционного удостоверения личности при регистрации на рейс может быть использована «информация из открытых баз данных». По всей видимости, к таким базам представители TSA отнесли и Facebook.

Указанный З. Клейном пункт действительно содержится в тексте правил на официальном сайте TSA. Тем не менее, в ответ на просьбу интернет-издания Mashable прокомментировать возможность использования профиля Facebook вместо обычных документов, сотрудники ведомства заявили, что не используют соцсети для идентификации пассажиров. «Мы оперируем только базами данных», – подчеркнули в TSA.

С другой стороны, как пишет Mashable, теоретически аккаунт в Facebook может ничем не отличаться от обычных документов. В соцсети существует механизм верификации, позволяющий пользователям подтверждать аутентичность своих страниц. Получить верификацию профиля пользователь может, предоставив администрации ресурса цифровые копии одного из удостоверяющих личность документов (например, свидетельства о рождении, водительских прав, паспорта или страхового полиса) ***(Забывший документы американец смог зарегистрироваться на авиарейс через Facebook // Подробности.UA (http://podrobnosti.ua/internet/2013/12/23/949677.html). – 2013. – 23.12).***

***

Соцсеть «Одноклассники» добавила возможность сопровождения виртуальных подарков легальной музыкой, сообщил пресс-секретарь соцсети И. Грабовский.

В настоящее время, по словам И. Грабовского, в целях легализации музыки «Одноклассники» сотрудничают с шестью крупными студиями, в том числе с «Первым музыкальным издательством», Gala Records и Warner Brothers. В пользу правообладателей будет отчисляться определенный процент с каждого приобретенного музыкального подарка, в котором используется их музыка. Распределение дохода между соцсетью и правообладателями не уточняется.

Музыкальное сопровождение, как показало тестирование Digit.ru, можно прикрепить почти к любому подарку. При этом к обычной цене подарка, которая во внутренней валюте составляет 20 ОК, прибавляется цена музыки – 10 ОК. 1 ОК равен 1 рублю.

В дальнейшем, по данным соцсети, планируется расширение каталога музыкальных треков. В настоящее время ведутся переговоры с крупным правообладателем зарубежной музыки ***(Соцсеть «Одноклассники» добавила к подаркам легальную музыку // IT Expert (http://itexpert.in.ua/rubrikator/item/32943-sotsset-odnoklassniki-dobavila-k-podarkam-legalnuyu-muzyku.html). – 2013. – 24.12).***

***

Руководство «ВКонтакте» ведет переговоры с западными правообладателями об исключении из списка пиратских сайтов, пишут «Ведомости». Соцсеть хочет добиться исключения из списка уже в следующем году.

Переговоры ведутся с Американской ассоциацией кинокомпаний (MPA). В организации подтвердили, что «ВКонтакте» удается успешно бороться с пиратским контентом, поэтому решение об исключении его из «черного списка» может быть принято через год.

Так называемый «список 301» составляет торговое представительство США. С 2010–2011 гг. в реестр стали попадать российские интернет-ресурсы. В результате, в списке оказались сайты «ВКонтакте», «Одноклассники» и Rutracker.org.

Ранее Facebook заблокировал трансляцию видеозаписей из «ВКонтакте» ***(«ВКонтакте» договорится об исключении из «пиратского» списка США // Полит.Ру (http://www.polit.ru/news/2013/12/26/dialog/). – 2013. – 26.12).***

***

Блог-сервис «Живой журнал» (LiveJournal) обновил мобильную версию сайта, сообщила компания «Афиша-Рамблер-Sup».

Как передает IT Expert со ссылкой на Digit.ru, в новой версии m.livejournal.com значительно изменился дизайн страниц, в первую очередь, расположение и вид элементов интерфейса.

«Новая мобильная версия понятнее с точки зрения интерфейса, ей стало удобнее пользоваться – особенно тем, у кого установлена Opera Mini», – прокомментировал Digit.ru руководитель департамента развития продуктов LiveJournal Д. Пилипенко. По его словам, это первый шаг в развитии мобильных продуктов LiveJournal, в начале следующего года сервис готовит к выпуску приложение LiveJournal для платформ Android и iOS.

Как и ранее, в мобильной версии доступно чтение ленты друзей, своего журналов, написание комментариев к записям, просмотр рейтингов и самых популярных тем дня ***(«Живой журнал» обновил мобильную версию сайта // InternetUA (http://internetua.com/jivoi-jurnal--obnovil-mobilnuua-versiua-saita). – 2013. – 27.12).***

***

В декабре этого года Facebook обновил свой алгоритм ранжирования публикаций в ленте новостей с целью предоставления более соответствующего содержания для интересов пользователей. Согласно Facebook, данное изменение позволяет видеть больше новостей: что читали другие пользователи, что им понравилось, что прокомментировали, а также «высококачественный» материал, опубликованный авторитетными веб-сайтами. Но, по последним сообщениям, это новое изменение алгоритма в Facebook нанесло урон многочисленным страницам Facebook.

Всякий раз, когда Facebook вносит изменения, люди с нетерпением ждут положительного результата. Иногда пользователи остаются довольны, но иногда – нет.

Согласно исследованию социальной маркетинговой компании Komfo, новые изменения алгоритма Facebook оказали негативное влияние на органический охват многих страниц Facebook. Компания изучила вовлеченность аудитории 5000 страниц Facebook и получила следующие результаты исследования:

– 28-процентное увеличение кликов к показам;

– 42-процентное снижение органического охвата страниц;

– 31-процентное увеличение виральности.

Приведенные выше данные показывают, что существует немалое процентное снижение в органическом охвате страниц Facebook (42 %). С другой стороны, кажется, что изменение алгоритма в Facebook оказало и положительное влияние: соотношение количества кликов к показам и виральность. Данные намекают, что в настоящее время нужно сосредоточиться на создании интересного контента, начать активно взаимодействовать и делиться ***(Новый алгоритм Facebook снизил популярность страниц // Uinny.ru (http://uinny.ru/index.php?id=1152). – 2013. – 28.12).***

***

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Сервіс мікроблогів оприлюднив найпопулярніші теми, новини й події, що висвітлювалися на Twitter протягом 2013 р. Серед термінових новин – барикади на майдані Незалежності після штурму спецслужб.

Підсумки розбиті на підрозділи #2013, #news, #entertainment, #sports, #showcase.

Під хештегом #news у розділ «Термінові новини» увійшло повідомлення з майдану Незалежності після спроб міліцейських підрозділів силою ліквідувати наметове містечко. Проте найпопулярнішою новиною року на Twitter стало народження принца в родині герцогів Кембриджських.

Найобговорюванішими подіями 2013 р. стали аварія гелікоптера в центрі Лондона, друга інавгурація президента США Б. Обами, нагородження «Оскар», вибухи під час Бостонського марафону, легалізація шлюбів «для всіх» у Франції, «Євробачення», протести в Бразилії, звільнення французького міністра через Twitter, підняття Costa Concordia, вибір Токіо в конкурсі на проведення літньої Олімпіади-2020, призупинення роботи уряду в США, тайфун на Філіппінах, Олімпіада в Сочі, смерть Мандели.

«Золотими твітами», тобто такими, що набрали найбільшу кількість ретвітів, став пост актриси Л. Мишель з подякою фанам щодо підтримки після загибелі її партнера К. Монтейта – отримав понад 400 тис. поширень, а також смерть в автокатастрофі актора П. Уокера ***(У підсумки 2013 року на Twitter увійшов київський Майдан з барикадами // MediaSapiens (http://osvita.mediasapiens.ua/material/25849). – 2013. – 13.12).***

***

В декабре 2013 г. Институт политической информации проанализировал, каким образом политические партии, принявшие участие в последних выборах в парламент, используют Интернет и социальные сети в своей деятельности. Также анализировались официальные сайты партий.

Исследовались наиболее популярные в Украине социальные сети: «ВКонтакте», Facebook и Twitter. Как и ожидалось, наибольшую активность проявляют движения, прошедшие в Верховную Раду, говорится в отчете экспертов, с результатами которого делится ЛІГАБізнесІнформ.

Самой активной партией в социальных сетях оказалось Всеукраинское объединение «Свобода». Второе место – у «Батькивщины».

«Следует отметить, что “Батькивщина”, в отличие от “Свободы” и других политических движений, уделяет большее внимание Facebook, которым, очевидно, пользуется более зрелое население. УДАР В. Кличко, как и “Свобода” более активен в социальной сети «ВКонтакте». Учитывая, что эта сеть пользуется популярность у более молодых пользователей, можно сделать вывод о том, на кого именно направлена деятельность трех оппозиционных партий в Интернете», – отмечается в сообщении.

По данным экспертов, менее активно проявляет себя в сети Партия регионов. В отличие от оппозиции, «регионалы» вяло используют Twitter. Однако сравнение количества подписчиков в Facebook и «ВКонтакте» (вторая социальная сеть отстает практически в три раза) говорит о более зрелой аудитории и у ПР.

«Коммунистическая партия в Интернете представлена достаточно формально. Страницы в социальных сетях функционируют, однако, особой популярностью не пользуются... Большинство политических движений, не попавших в парламент, ведут пассивную работу в своих представительствах в Интернете. Некоторые партии перестали обновлять свои страницы в социальных сетях после окончания предвыборной кампании», – заключили эксперты.

В Институте политической информации также отметили, что большинство сайтов партий, участвующих в выборах 2012 г., не отвечают современным требованиям. «В них отсутствуют ссылки на официальные страницы в социальных сетях, возможность оценить новость и принять участие в обсуждении», – резюмировали исследователи ***(Веб-мониторинг: названы самые активные украинские партии и их социальная база в сети // NEWSru.ua (http://www.rus.newsru.ua/ukraine/28dec2013/virtual.html). – 2013. – 28.12).***

***

Чернівецька облдержадміністрація створила свою сторінку в мережі Facebook. Про це на брифінгу повідомив голова ОДА М. Папієв.

«Там ми зможемо спілкуватися в режимі діалогу, кожен відвідувач зможе розміщувати свої коментарі, – розповів губернатор. – Також буде можливість спілкування з головою ОДА, я зможу в режимі онлайн прокоментувати важливі для Буковини події. Будемо висвітлювати і ті події, у яких не беремо безпосередньо участь», пише molbuk.ua ***(Чернівецька облдержадміністрація створила свою сторінку у мережі Facebook // Буковинська правда (http://bukpravda.cv.ua/news/suspilstvo/item/12939-z-golovoyu-oda-teper-mozhna-bude-spilkuvatis-u-facebook.html#.UrAhIeXLrWQ). – 2013. – 16.12).***

***

А. Шевченко та Л. Оробець подолали позначку у 20 тис. фоловерів у Twitter. Наразі вони є лідерами серед українських політиків у цій соціальній мережі, якщо не враховувати Ю. Тимошенко, останній запис якої датований ще серпнем 2011 р.

Особливо багато фоловерів А. Шевченко та Л. Оробець набрали за останні два тижні. Наприкінці листопада їх чисельність була близько 10 тис.

Істотно зросла кількість фоловерів в останні дні також у В. Кличка – 17 тис. та А. Гриценка – 12 тис. Найбільша кількість фоловерів серед представників влади наразі у С. Тігіпка – 10 тис.

Найпопулярнішим українським користувачем Twitter залишається С. Вакарчук, у якого чверть мільйона фоловерів ***(За останні 2 тижні депутати опозиції А. Шевченко та Л. Оробець набрали по 10 тис. фоловерів у Twitter // UkrainianWatcher (http://watcher.com.ua/2013/12/16/za-ostanni-2-tyzhni-deputaty-opozytsiyi-andriy-shevchenko-ta-lesya-orobets-nabraly-po-10-tysyach-foloveriv-u-tviteri/). – 2013. – 16.12).***

***

Политики и чиновники Днепропетровска в социальных сетях

В последние месяцы днепропетровские чиновники и политики стали активными пользователями социальных сетей Facebook и «ВКонтакте». Но на своих страницах они говорят преимущественно о своей работе. На отдых, судя по всему, у них времени не остается. Во всяком случае, о своих

поездках за рубеж или отдыхе в гламурных заведениях днепропетровские власть имущие предпочитают умалчивать, пишет «Сегодня» (http://www.segodnya.ua/regions/dnepr/politiki-i-chinovniki-dnepropetrovska-v-socialnyh-setyah-483724.html).

Пожалуй, единственным исключением является депутат Днепропетровского городского совета С. Епифанцева. Она делится со своими друзьями фотографиями отдыха на курортах и ночных клубах. Однако, после прошлогоднего скандала, когда журналисты обнародовали ее фотографии в нижнем белье, С. Епифанцева если и не стала пуританкой, то, во всяком случае, предпочитает появляться на публике в дорогих нарядах. А не демонстрировать свои прелести.

Депутаты и чиновники не смогли обойти стороной последние события в стране. Однако восхищения Евромайдан в Киеве вызвал у немногих. Так, глава областной Федерации футбола и народный депутат А. Павелко опубликовал в Facebook свое фото с сыном на майдане Незалежности.

«Всю прошлую неделю провел в бесконечных встречах-дискуссиях “Пути выхода из кризиса”. С самыми разными людьми – партийцами-соратниками из разных областей, фб-сообществом “План действий”, общественными активистами, представителями культуры и искусства, последние, кстати, вопреки стереотипу оказались очень даже политически активны и осведомлены. Общий вывод – стратегический план выхода страны из кризиса должно предложить именно общество. Ведь именно общество вышло на Майдан, а политики лишь подтянулись. Эта безумно интересная работа продолжится. Но сегодня я был на Евромайдане с сыном – он уже тоже не может быть в стороне и я этим горжусь», – написал А. Павелко.

В то же время бывший первый заместитель губернатора, а ныне – народный депутат-«регионал» В. Задорожный побывал на субботнем Антимайдане. «Совместно с коллегами народными депутатами и единомышленниками, приехавшими в столицу с разных регионов страны, участвую в многотысячном митинге на Европейской площади Киева в поддержку Президента Украины В. Януковича и действующей власти», – пишет на Facebook В. Задорожный.

А вот председатель Днепропетровского областного совета Е. Удод на киевские площади в последнее время не ездил. Но ситуацию в стране комментирует активно. Так, «Сегодня» писали о его словах, где он сравнил митингующих с нацистами: «Киевский Майдан сейчас – это бомба замедленного действия. Которая в любой момент может просто взорваться. Крайне важно не поддаваться эмоциям и трезво смотреть на вещи. Кричать в толпе “Слава Украине” это конечно весело.

Но после лозунгов пойдут призывы. Так уже было в Германии в начале 30-х годов прошлого века. Тоже люди стояли, кричали вполне понятные лозунги и совсем не заметили, как к власти пришли нацисты», – писал Е. Удод.

Но публикация главе облсовета не понравилась. «На своей странице в социальной сети Facebook Е. Удод сравнил митингующих с немецкими

нацистами» – пишет одно из “независимых” интернет-изданий. У меня по этому поводу слов нет, но есть хорошая картинка», – написал Е. Удод и прикрепил картинку лживого журналиста.

А вот мэр Днепропетровска И. Куличенко «активничал» в соцсетях лишь в ноябре. Но публикует лишь официальные заявления пресс-службы городского совета.

Еще есть категория днепропетровских чиновников, которые вплоть до парламентских выборов-2012 чуть ли не каждый постили свои фото в соцсетях. Но после проигрыша, как в случае с нынешним первым заместителем губернатора А. Крупским или экс-главой бюджетного комитета Верховной Рады Н. Деркачем, предпочли не светиться в Facebook или «ВКонтакте» ***(Политики и чиновники Днепропетровска в социальных сетях // «Сегодня» (http://www.segodnya.ua/regions/dnepr/politiki-i-chinovniki-dnepropetrovska-v-socialnyh-setyah-483724.html). – 2013. – 19.12).***

***

Учитель из Донецка собрал в социальных сетях деньги на бесплатный клуб робототехники. Бесплатный клуб робототехники был организован для школьников Донецка простым учителем И. Шихат-Саркисовым.

Клуб открылся на базе донецкого Лицея информационных технологий. Деньги на покупку программируемых роботов Mindstorms EV3 от Lego было решено собрать в социальных сетях.

Отметим, что средняя стоимость одного робота в интернет-магазине составляет примерно 500 дол., а за отдельные датчики приходится доплачивать ещё от 30 до 50 дол.

Инициативный преподаватель сначала хотел собрать средства на украинском сайте коллективного финансирования, но, поскольку клуб планировалось запустить до Нового года, было решено создать страничку клуба в соцсети Facebook, где и началась кампания по сбору средств.

С помощью социальных сетей 25 % от необходимой суммы было собрано всего за два дня. Впоследствии Roboclub умудрился собрать даже сверх требующейся суммы – 11 тыс. грн. Средства перечисляли как знакомые И. Шихат-Саркисова, так и случайные люди.

16 декабря 2013 г. клуб купил первого робота и набор дополнительных ресурсов для конструирования. На сегодняшний день в распоряжении клуба есть два робота и два набора к ним.

В свою очередь первые ученики уже начали работать над программированием роботов. Отметим, что у клуба есть свой сайт, а полноценные курсы стартуют после школьных каникул ***(Учитель из Донецка собрал в социальных сетях деньги на бесплатный клуб робототехники // InternetUA (http://internetua.com/ucsitel-iz-donecka-sobral-v-socialnih-setyah-dengi-na-besplatnii-klub-robototehniki). – 2013. – 29.12).***

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Топ-5 уроков социальных сетей 2013 года

Это был важный год для социальных медиа. Twitter успешно дебютировал на биржевой площадке, в то время как Facebook оправился от беспокойного IPO годом ранее. Мы также увидели запуск Vine, подъем Snapchat и принятие социальных медиа SEC, это означает, что публичные компании могут использовать эти сайты для разглашения информации, пишет Marketing Media Review (http://mmr.ua/news/id/5-samyh-glavnyh-urokov-socialnyh-setej-2013-37649/).

И это было только в США.

В Китае, где самая большая аудитория интернет-пользователей, гигант интернет-коммерции Alibaba потратил 586 млн дол. на создание Weibo, самого крупного микроблоггинг-сервиса (аналог Twitter) и конкурента популярного мессенджера WeChat, созданного телекоммуникационной компанией Tencent. Тем временем в Украине операторы мобильной связи ожидали рост траффика данных, поскольку протесты против власти действующего Президента активно проявлялись в социальных сетях, подобное можно было наблюдать Арабской весной 2011 г.

Конечно, как и в предыдущие годы, были оплошности в социальных сетях, наряду с многочисленными проявлениями звездности и тверкинга. Однако из 2013 г. можно вынести несколько важных уроков.

Социальные медиа могут влиять на рынки

23 апреля аккаунт Associated Press в Twitter был взломан, с него отправили фейковый твит о том, что «в Белом доме были заложены две бомбы, и Б. Обама пострадал». За считаные секунды индекс Доу-Джонса упал на 150 пунктов. Позже в июне инвестор-миллиардер К. Икан завел аккаунт в Twitter, сначала используя его как рупор в своей борьбе с Dell, а потом, чтобы анонсировать свои доли в компаниях, прежде всего в Apple. 13 августа К. Икан опубликовал пост в Twitter о том, что он занимает «крупную позицию» в производстве iPhone, это сообщение вызвало рост котировок компании болем чем на 5 %.

Наблюдая за тем, как всего лишь один твит может раскачать маятник рынка, можно смело утверждать, что социальные сети также важны для трейдеров, как и для ньюсмейкеров.

Социальные медиа всё больше становятся визуальными

Конечно, можно сказать многое в 140 символах, но изображение всё равно лучше тысячи слов. В январе Twitter приобрел Vine, в качестве мобильного сервиса для загрузки 6-секундных видеороликов. Далее, в июне, Facebook отреагировал вставкой видео в Instagram.

Мы также наблюдали рост Snapchat, сервиса, который позволяет пользователям делиться фото и видео, без подключения к социальным сетям. Сам пользователь может контролировать, как долго (1–10 секунд) получатели смогут видеть его «Снэпы». Когда время закончится, фото или

видео исчезнет. Сервис стал настолько популярным среди более юного поколения, что, по имеющимся сведениям, Facebook решили купить его за 3 млрд дол. Snapchat отказались.

За несколько дней до своего IPO Twitter запустил обновление, в котором появился предпросмотр Twitter-фото или Vine-видео. С таким внешним обновлением Twitter стал больше визуальной, чем текстовой площадкой.

Социальные медиа предназначены не только для детей

Начиная с У. Баффета, который присоединился к Twitter, заканчивая Д. Даймоном, который присоединился к программе LinkedIn Influencer, 2013 г. показал нам, что мировые лидеры тоже пользуются социальными сетями. Однако, как показали твиты Р. Мердока, иногда влияние бизнеса может быть непредсказуемым.

Реклама в социальных медиа растет и развивается

Во время Суперкубка больше всего разговоров было не о 30-секундном ролике, а о твите. Из-за сильных перебоев в электричестве пришлось прекратить игру на 34-й минуте, Oreo быстро опубликовали твит «Нет света? Не проблема» и прикрепили изображение Oreo с текстом «Можно забрасывать мяч в корзину в темноте». Этот твит привлек сильное внимание прессы и изменил отношение к возможностям рекламы в социальных медиа.

2013 г. также показал, как много денег можно заработать на рекламе в социальных медиа. В III квартале Facebook предоставили отчет о том, что их доходы возросли на 60 %, по сравнению с предыдущим годом, значительно благодаря мобильной рекламе. Примерно в то же время Facebook анонсировали в Instagram спонсорские посты, которые появились в ленте у пользователей из США.

Социальные сети могут стать лучшим союзником телевидения

В октябре рейтинг Nielsen опубликовал анализ, в котором показал взаимосвязь между публикациями твитов во время просмотра ТВ и более масштабной и вовлеченной аудиторией. Данные показали, что 19 млн пользователей в США создали 263 млн твитов во время тв-трансляций во II квартале 2013 г.

Социальное ТВ еще только на этапе начального развития, но, с телевидением, как источником традиционной тв-рекламой и социальными сетями, как с площадкой роста аудитории и вовлечения, оно может быть началом длительных и хороших взаимоотношений ***(Галушка А. Топ-5 уроков социальных сетей 2013 года // Marketing Media Review (http://mmr.ua/news/id/5-samyh-glavnyh-urokov-socialnyh-setej-2013-37649/). – 2013. – 19.12).***

***

Facebook ввел ряд изменений в своей контент-политике и принципах продвижения контента. В Pando.com попытались разобраться, как эти нововведения повлияют на дальнейшие позиции брендов и проектов, использующих Facebook.

Facebook не только объявил об изменениях, благодаря которым возрастает роль пользовательского контента в новостной ленте, но и заявил, что одни публикации будут продвигаться, а другие – наоборот, терять позиции. И за этим будет следить некий алгоритм.

Еще в Facebook решили понизить влияние внешнего контента, это повлечет за собой целый ряд изменений. Кто выиграет от этого?

Те, кто в выигрыше

Наибольшую выгоду получат агрегаторы вроде Buzzfeed, Upworthy и аналогичных. В отличие от печального опыта компании Zynga, с агрегаторами контента такого не случится: полного отказа от них не будет, возможно небольшое падение трафика, но в ближайшие два года агрегаторы контента точно не пострадают.

Дополнительный фактор влияния – потенциальная монетизация контента, на которой сам Facebook может заработать. К примеру, тот же BuzzFeed уже тратит много денег на продвижение контента через механизм платных постов и рекламы.

И даже если в Facebook решат больше брать денег за медиа-контент, те, кто будет готов привлекать качественно отфильтрованную аудиторию из социальной сети, продолжат платить. Почему бы BuzzFeed не продолжить платить, чтобы остаться на вершине «пищевой пирамиды» и обойти конкурентов, для которых плата за посты в ленте покажется высокой? 1 млрд пользователей, которые читают этот агрегатор, с лихвой окупят затраты.

От новой модели, по которой выше в выдаче новостей оказывается тот, кто платит, есть и другие бренды, которые окажутся в выигрыше. К примеру, выиграют крупные издания и журналы вроде Time Magazine и The Atlantic. Для печатной прессы, у которой есть онлайн-версия, Facebook может стать своего рода спасением. Но не все собираются изменить свою рекламную стратегию в этом ключе. К примеру, вряд ли стоит ждать подобного от BusinessWeek, Better Homes и Gardens.

Такие издания, как Time и The Atlantic, выиграют, потому что старые механизмы дистрибуции не работают. Они стали осваивать новые каналы доставки контента. Но при этом, по оценкам Comscore, аудитория не слишком велика у этого издания именно в Интернете.

Третий победитель – это AdTech и подобные им компании, работающие с таргетированием рекламы и коммерческой информации. Лет 10 эта индустрия напоминала собой Диснейленд, в котором полно детей, которые шумят и спрашивают, ну когда же уже карусели. В роли каруселей выступает прибыль и монетизация как таковая. После целой череды IPO разных интернет-проектов неуверенность в прибыльности таргетирования только растет. Изменения в контент-правилах Facebook могут сыграть на руку таким платформам таргетирования.

И больше всего выиграют бренды с широкой демографией аудитории. Чтобы работа оффлайн-брендов в соцсетях была эффективной в плане таргетирования и показа платных постов именно для ЦА, стоит объединяться таким брендам с онлайн-платформами таргетирования.

А кто проиграет?

Как ни странно, но тактика продвижения платных постов и ранжирования контента не лучшим образом скажется на газетах и журналистах, которые занимаются расследованиями.

Формат срочных, «горячих» новостей не слишком подходит для ленты и хроник Facebook. Даже если кто-то вроде Washington Post публикует историю, собравшую много лайков, то не ясно, получают ли они оттуда какой-то качественный трафик. Публикация на сайте, где кнопки социального шэринга сделали покрасивее, а работа контент-менеджера получше, может собрать больше лайков, чем серьезная значимая новость на сайте, где такого нет.

Пользователи, которые публикуют контент, вообще не вникают, кто именно «запостил» историю в общую ленту. Объективность не всегда в почете, а социальная сеть любит громкие заголовки и яркие вбросы. К тому же традиционные медиа, пришедшие в Интернет, не умеют составлять заголовки, которые оптимизированы для Facebook. Пулитцеровская премия – не залог успеха в социальных сетях.

Вирусность публикаций в соцсети тоже представляет сложность для использования хроники и новостной ленты классическими медиа. История держится на пике максимум сутки, но еще несколько дней подряд образует «хвост», который генерирует дополнительный мощный трафик. Люди приходят почитать смысловой и «долгоиграющий» контент, а горячие новости живут недолго и потому не интересны.

Проиграет от нововведения Facebook и Twitter. Уже сегодня он не дает столько трафика, сколько дает сеть М. Цукерберга (по крайней мере, так полагают авторы исследования в Pando). У Twitter скорее образовалось сообщество внутри собственной экосистемы, из которой никуда не надо переходить для ведения дискуссий. Facebook же активно курирует внешний контент, расположенный за пределами соцсети и ее экосистемы.

И немного неопределенности

Не ясно, что будет с нишевыми контент-проектами и с теми, кто не входит в категорию лидеров по гаджет-новостям (вроде TheVerge, PopSugar, Business Insider). Крупные проекты смогут договориться и с агрегаторами, и с Facebook. А вот что будут делать мелкие, у которых не найдется бюджета, в несколько раз большего, для продвижения? При всём этом рекламодатели по-прежнему ценят нишевые проекты с качественной целевой аудиторией. И только время покажет, как нововведения контент-стратегии в Facebook может повлиять на взаимоотношения небольших проектов и рекламодателей.

Надеемся, что нам в ЦП не придется отказаться от макбуков и бросить все деньги на платные лайки, а то как-то нехорошо получится ***(Кто выиграет в контент-битве за Facebook? // InternetUA (http://internetua.com/kto-viigraet-v-kontent-bitve-za-Facebook). – 2013. – 15.12).***

***

Руководство социальной сети «ВКонтакте» подписало соглашение с компанией StarPro, которая предоставляет легальный доступ к видеоклипам шести крупных российских музыкальных студий, включая «Союз», «Арс-рекордз» и «Национальное музыкальное издательство». Об этом заместитель генерального директора «ВКонтакте» И. Перекопский заявил порталу TJournal.

«ВКонтакте» будет предотвращать загрузку пиратских копий клипов, права на которые принадлежат музыкальным студиям. Кроме того, социальная сеть будет делиться с правообладателями доходами от видеорекламы, которая будет размещена перед клипами во внутреннем плеере «ВКонтакте». Среди исполнителей, чьи ролики будут легально размещаться во «ВКонтакте», – Ф. Киркоров, С. Михайлов, Тимати, И. Дорн, Д. Билан, «Океан Ельзи» и др.

И. Перекопский объяснил TJournal, что данное соглашение – первый случай, когда «ВКонтакте» удалось договориться с музыкальными правообладателями «на взаимовыгодных партнерских условиях». Кроме того, он выразил надежду, что соцсети удастся договориться и с другими правообладателями.

Руководство социальной сети «ВКонтакте» начало переговоры с крупными правообладателями о размещении легального контента накануне вступления в силу антипиратского закона. В сентябре социальная сеть достигла соглашения с медиахолдингом ВГТРК о показе видеоконтента компании. «ВКонтакте» и ВГТРК договорились поровну делить доходы от видеорекламы.

«ВКонтакте», крупнейшая социальная сеть России с посещаемостью около 46 млн человек в сутки, разрешает пользователям загружать самим аудио- и видеоконтент. При этом на сайте уже несколько лет существует механизм, который позволяет правообладателям добиваться удаления своих материалов. Накануне и после вступления в силу антипиратского закона правообладатели ужесточили борьбу с нелегальным контентом: в итоге из социальной сети практически исчезли музыкальные произведения некоторых исполнителей ***(«ВКонтакте» заработает на легальных клипах Киркорова и Тимати // Версии.com (http://www.versii.com.ua/news/293483). – 2013. – 16.12).***

***

Крупнейшая в мире социальная сеть Facebook создаст алгоритм, который соберет подробную информацию о пользователях для улучшения показателей целевой рекламы, пишет The Daily Mail.

По информации издания, социальная сеть будет собирать всю информацию о пользователях по фотографиям, лайкам, местам, которые посещают пользователи, для того чтобы добиться лучших результатов от продаж целевой рекламы.

Издание отмечает, что социальная сеть объединилась с Нью-Йоркским университетом для создания исследовательской лаборатории по изучению

искусственного интеллекта. Лаборатория должна стать крупнейшим в мире научно-исследовательским центром такого рода, ее подразделения будут работать в Нью-Йорке, Лондоне и Калифорнии, отмечает газета ***(Facebook будет собирать подробную информацию о пользователях // InternetUA (http://internetua.com/Facebook-budet-sobirat-podrobnuua-informaciua-o-polzovatelyah). – 2013. – 16.12).***

***

«Билайн» использует этот инструмент для популяризации мобильного Интернета, другие бренды могут найти свои точки соприкосновения.

В последние годы операторы сфокусированы на развитии мобильного Интернета. За этой услугой – будущее бизнеса и база для дальнейшего улучшения бизнес-показателей. Социальные сети как одни из наиболее популярных интернет-площадок стимулируют спрос на мобильный Интернет. Если человек ежедневно выходит в социальную сеть с компьютера, он наверняка станет просматривать ленту и с мобильного телефона.

Одна из возможных совместных акций, направленных на продвижение мобильного Интернета, – предоставление бесплатного доступа к социальной сети. Такая услуга положительно воспринимается клиентами – растет как количество новых, так и активность действующих пользователей, для которых мобильный телефон становится привычным средством выхода в сеть.

Впервые мы опробовали эту акцию с Facebook. Учитывая успешный опыт, создали «нулевые зоны» с бесплатным доступом совместно со многими популярными интернет-ресурсами – «ВКонтакте», Wikipedia, LiveJornal, новостным сайтом «Газета.ру», а также целым рядом популярных региональных сайтов.

Бесплатный доступ к социальным сетям интересен преимущественно двум категориям абонентов: тем, кто уже пользуется мобильным Интернетом, но по различным причинам не подключает безлимитные тарифы и опции, и тем, кто только начинает опробовать услугу и вообще незнаком с тарифами. В совместной акции с Facebook нам удалось вовлечь обе категории пользователей и получить хорошие результаты.

Абоненты, которые начинали выходить в социальную сеть через «нулевую зону», расходовали в 1,5 раза больше трафика. Только в период рекламной кампании количество абонентов, которые выходили в Facebook со смартфона, возросло более чем на 500 тыс. человек. В этот же период 17 % лайков на странице «Билайн» были сделаны с мобильных устройств.

В то же время очень важна имиджевая составляющая. Благодаря совместным активностям с социальными сетями сообщества бренда становятся популярнее. Количество подписчиков нашей страницы «ВКонтакте» на сегодняшний день превышает 800 тыс. Страница в Facebook уже стала первым по количеству пользователей сообществом среди российских брендов, она объединила более 300 тыс. человек.

«Билайн» также участвует в трехсторонних партнерствах. В качестве примера можно привести реализованный совместно с Facebook и «Мультимедиа арт музеем» (Москва) проект «Музей современного момента». Через специальное приложение в Facebook была создана виртуальная галерея, где наши абоненты ежедневно выкладывали снимки моментов из своей жизни и голосовали за лучшие работы.

Около трех лет назад мы начали предоставлять услугу SMS-уведомлений и SMS-ответов из Facebook, «ВКонтакте», «Одноклассников», Twitter и LiveJournal. Она помогает оставаться онлайн без выхода в Интернет и по-прежнему сохраняет актуальность. Присутствие в социальных сетях – это еще и возможность прямого диалога, а для абонентов – альтернатива звонкам в call-центр при разрешении вопросов.

Компании заинтересованы в росте популярности услуг и брендов, как и социальные сети заинтересованы в росте своей аудитории. Это очевидная точка соприкосновения для создания успешных совместных проектов ***(Почему бренды не должны игнорировать социальные сети // InternetUA (http://internetua.com/pocsemu-brendi-ne-doljni-ignorirovat-socialnie-seti). – 2013. – 18.12).***

***

В социальной сети Facebook с 19 декабря появится видеореклама. Пользователи будут видеть рекламные ролики в своей ленте новостей, причем прокручиваться они будут без звука. При нажатии на изображение владелец страницы сможет просмотреть сюжет полностью. Представители Facebook уверяют, что такое видео после прокручивания сегмента новостной ленты с роликом будет исчезать.

По данным аналитиков, доход от предоставления места для размещения 15-секундных роликов в перспективе составит порядка 1 млн дол. в день. В настоящее время в США лидером рынка рекламы на цифровых носителях является канал YouTube, прибыль которого в 2013 г. в этой стране составила 850 млн дол. ***(В Facebook появится видеореклама // Четверта Влада (http://4vlada.net/smi/v-facebook-poyavitsya-videoreklama). – 2013. – 18.12).***

***

Facebook мог вводить в заблуждение инвесторов перед IPO, говорится в сообщении агентства Reuters со ссылкой на заявление судебных органов США, пишет «Обозреватель» (http://finance.obozrevatel.com/economy/51406-facebook-zapodozrili-vo-vvedenii-v-zabluzhdenie-investorov-pered-ipo.htm).

Как отмечается в заявлении, глава компании М. Цукерберг в сговоре с банками, занимавшимися размещением акций Facebook, давали искаженную информацию инвесторам о финансовом состоянии интернет-гиганта. В этой связи инвесторы могут предъявить иски к компании.

У инвесторов также есть претензии к тому, что компания недостаточно раскрыла информацию о росте использования мобильных продуктов и

решений. Это, по мнению инвесторов, может привести в перспективе к снижению доходов компании ***(Facebook заподозрили во введении в заблуждение инвесторов перед IPO // Обозреватель (http://finance.obozrevatel.com/economy/51406-facebook-zapodozrili-vo-vvedenii-v-zabluzhdenie-investorov-pered-ipo.htm). – 2013. – 19.12).***

***

Основатель и исполнительный директор Facebook М. Цукерберг продает 41,4 млн акций своей компании, чтобы выручить средства на оплату налогового счета, выставленного ему в связи с исполнением опциона на покупку 60 млн акций Facebook, пишет «Обозреватель» (http://finance.obozrevatel.com/economy/86142-tsukerberg-prodaet-414-mln-aktsij-facebook.htm). О нетривиальной комбинации сделок стало известно из документа компании, поданного в Комиссию по ценным бумагам и биржам США, передает «РБК-Украина».

Как сообщается в материалах Facebook, М. Цукерберг полностью исполнит опцион на покупку 60 млн акций класса «В» и затем предложит 41 млн 350 тыс. акций класса «А» (будут автоматически конвертированы из акций класса «В») в рамках объявленного вторичного размещения. «Мы ожидаем, что большинство средств, которые М. Цукерберг получит от продажи (41,35 млн акций), будут использованы для исполнения налоговых обязательств, возникших в связи с реализацией опциона», – указывает компания.

Кроме того, в материалах Facebook сказано, что в декабре 2013 г. М. Цукерберг пожертвует 18 млн акций класса «В» (оцениваются в 1 млрд дол.) на некие цели, о которых не сообщается.

После вторичного размещения М. Цукерберг будет контролировать 56,1 % голосующих прав в Facebook (до размещения – 58,8 %).

После 20 декабря 2013 г. акции класса «А» Facebook будут включены в расчетную базу индекса S&P 500. С начала 2013 г. акции социальной сети на бирже Nasdaq подорожали почти на 100 % ***(Цукерберг продает 41,4 млн акций Facebook // Обозреватель (http://finance.obozrevatel.com/economy/86142-tsukerberg-prodaet-414-mln-aktsij-facebook.htm). – 2013. – 20.12).***

***

Социальная сеть Facebook приобрела стартап SportStream, специализирующийся на сборе спортивных данных из социальных сетей и последующем анализе этой информации. В Facebook говорят, что поглощение SportSteam позволяет им получить технологии сбора, фильтрации и отображения в реальном времени больших объемов спортивной информации, генерируемой пользователями соцсетей.

Одновременно с этим данное поглощение позволит Facebook расширить возможности по поиску медиа-партнеров из области спортивного контента и более эффективно анализировать спортивный контент. Напомним,

что ранее ряд похожих поглощений сделала и компания Twitter, которая также делает ставку на контентный анализ в реальном времени. «Через последнее поглощение мы надеемся качественно улучшить возможности для всех наших партнеров по доступу к информации и использованию этих данных», – говорится в блоге Facebook.

Финансовые условия сделки не разглашаются ***(Facebook покупает стартап Sportstream // Минфин (http://minfin.com.ua/2013/12/18/849583). – 2013. – 18.12).***

***

Вторая по популярности соцсеть России «Одноклассники» приносит партнерам-разработчикам приложений (игр, утилит в соцсети) вдвое больше денег, чем лидер рынка «ВКонтакте». Обе соцсети отдают партнерам примерно половину полученных от пользователей денег – значит, соцсеть № 2 зарабатывает на посетителях больше, чем № 1. Эксперты отрасли подтверждают: «ВКонтакте» зарабатывает прежде всего на рекламе. Но борьба с пиратством может уменьшить количество интересного пользователям контента в крупнейшей соцсети. Бизнес-модели соцсетей начинают меняться.

Как выяснили «Известия», социальная сеть «Одноклассники» (на 100 % принадлежит Mail.Ru Group) в 2013 г. выплатила разработчикам приложений 3,3 млрд р. Соцсеть «ВКонтакте» ранее сообщала, что потратила на эти цели 1,3 млрд. При этом, по данным TNS, в октябре у «Одноклассников» было 38,9 млн уникальных пользователей, а у «ВКонтакте» – 51,2 млн.

Как отмечает основатель портала liveinternet.ru Г. Клименко, у двух соцсетей изначально отличались модели ведения бизнеса. «“ВКонтакте” всегда делала акцент на бесплатность. Модель бизнеса для “Одноклассников” строил рекламный отдел Mail.Ru Group, он приучал пользователей платить, монетизацию контента они всегда ставили на первое место, – рассказывает Г. Клименко. – Просить же деньги у людей, привыкших бесплатно получать контент, сложно».

По опыту разработчика проекта Flypoker Д. Твердохлеба, при размещении одинакового приложения в «Одноклассниках» и «ВКонтакте», заработок в первой соцсети бывает вдвое больше. Д. Твердохлеб объясняет это тем, что в «Одноклассниках» активна платежеспособная аудитория 35–45 лет.

У «ВКонтакте» всегда было много бесплатного контента, к которому постоянно возникали претензии у правообладателей, напоминает аналитик «Финам» Л. Делицын.

В условиях ужесточения борьбы с пиратством крупнейшая российская соцсеть занялась легализацией аудио и видео. Параллельно администрация «ВКонтакте» стала уделять больше внимания приложениям, позволяющим получать деньги от пользователей. «Год назад обе соцсети делили заработок с разработчиками 50:50, но потом “ВКонтакте” стала выплачивать создателям приложений больше», – сообщил Д. Твердохлеб. По словам

представителя «ВКонтакте» Г. Лобушкина, на сегодняшний день соотношение составляет 45:55.

Кроме того, крупнейшая российская соцсеть стала размещать ссылки на приложения в лентах новостей всех пользователей.

Тем временем в развитии рынка легального видео в Интернете решили поучаствовать и «Одноклассники». В середине декабря эта соцсеть объявила об открытии онлайн-кинотеатра. По словам главы компании И. Широкова, теперь соцсеть будет получать доход от рекламных роликов, которые будут показывать перед началом воспроизведения фильма. В любом случае, рассказывает Д. Твердохлебов, разработчики приложений обычно делают их сразу для многих соцсетей. «Главное – сделать игру, а заточить ее под любую соцсеть – вопрос двух-трьох дней, – поясняет разработчик. – Делать акцент для одной платформы, игнорируя другую, никто не будет. Ведь это потеря части аудитории».

Глава компании «Русские интернет-решения» С. Кравцов приводит аналогию из рынка пищевых продуктов. «Если в одном магазине сок продается хорошо, а в другом плохо, это не значит, что его вовсе перестанут продавать там, откуда поступает меньше денег», – заявил он ***(«Одноклассники» заработали на посетителях вдвое больше «ВКонтакте» // InternetUA (http://internetua.com/odnoklassniki--zarabotali-na-posetitelyah-vdvoe-bolshe--vkontakte). – 2013. – 23.12).***

***

Социальная сеть «Одноклассники» подписала партнерское соглашение с музыкальным лейблом Warner Music. Об этом «Ленте.ру» 23 декабря сообщил пресс-секретарь соцсети И. Грабовский.

По условиям контракта Warner Music будет получать денежные отчисления от использования принадлежащих ей фонограмм в музыкальных подарках, которые отправляют друг другу пользователи «Одноклассников» (возможность прикреплять к виртуальным подаркам музыкальные треки появилась в соцсети 23 декабря).

По словам И. Грабовского, Warner Music стал вторым лейблом из числа участников Национальной федерации музыкальной индустрии, начавшим сотрудничество с социальной сетью. Раньше соглашение с «Одноклассниками» также подписала звукозаписывающая компания Gala Records, а также такие компании, как «Юнайтед мьюзик групп» и Megaliner Records.

Кроме того, как сообщили «Ленте.ру» источники на рынке, в настоящее время «Одноклассники» ведут переговоры еще с одним крупным международным лейблом Universal (также входит в Национальную федерацию музыкальной индустрии). Каких-либо подробностей относительно того, как проходят эти переговоры и когда может быть подписано соглашение, не уточняется.

Лицензионный музыкальный контент впервые появился в «Одноклассниках» летом 2012 г. Первым лейблами, подписавшими

соглашения об использовании своей музыки в соцсети стали Nikitin MDC («Никитин медиа диджитал контент»), «Первое музыкальное издательство», «СБА продакшн» и ИП «Лешкевич» (компании принадлежат права на творчество группы «Каста»). Рядом с треками, права на которые принадлежат перечисленным компаниям, в соцсети появилась специальная зеленая стрелочка, нажав на которую, можно совершенно легально скачать выбранный музыкальный контент, с которого правообладатели также получают отчисления ***(Warner Music заработает на легальной музыке в «Одноклассниках» // Лента.Ру (http://lenta.ru/news/2013/12/23/okmuzlo). – 2013. – 23.12).***

***

Facebook в настоящее время является лидером по продаже рекламы в Интернете. Крупнейшая социальная сеть пока что уступает только гиганту Google, сообщает EMarketer Inc., пишет Marketing Media Review (http://mmr.ua/news/id/facebook-okazalsja-liderom-po-prodazhe-internet-reklamy-37699).

Крупнейшая социальная сеть может получить 3,17 млрд дол., или 7,4 % от общего объема цифровой рекламы в США в этом году, в то время как на долю Google приходится 17 млрд дол., или 40 %, заявили 24 декабря в своем блоге EMarketer Inc. В 2012 г. Facebook был четвертым после Google, Yahoo! Inc и Microsoft.

Facebook наращивает свои рекламные мощности, генерируя половину своих доходов от мобильных и видеоакций, которые автоматически проигрываются в новостной ленте пользователей. Instagram, который Facebook купил за 700 млн дол. в прошлом году, также транслирует объявления на своем сервисе обмена фотографиями. Facebook и его конкуренты борются за долю на рынке цифровой рекламы, который, по прогнозам, возрастет на 25 % и достигнет 53,4 млрд дол. в США в 2015 г. «Facebook и Google являются основными движущими силами этого растущего рынка, как на уровне страны, так и в мире», – пишет EMarketer Inc. Обе компании также являются крупнейшими мировыми рекламодателями.

Расходы на мобильную рекламу составят 23 % от всего объема расходов на цифровую рекламу. Для сравнения: в 2012 г. этот показатель составлял всего лишь 12 %, по данным EMarketer Inc.

Первые четыре рекламные кампании, запущенные в Instagram, охватили значительную аудиторию, сообщает представитель Facebook в своем блоге. Реклама Levi Strauss & Ко была показана 7,4 млн человек в США за девять дней, а Ben & Jerry»s Homemade Inc. – 9,8 млн человек, в течение восьми дней. Среди тех, кто увидел акцию мороженного Scotchy Scotch, 17 % заинтересовались продуктом и связались с компанией, согласно статистике Instagram ***(Facebook оказался лидером по продаже интернет-рекламы // Marketing Media Review (http://mmr.ua/news/id/facebook-okazalsja-liderom-po-prodazhe-internet-reklamy-37699). – 2013. – 24.12).***

***

Цена акций сервиса микроблогов Twitter практически утроилась с момента первичного публичного размещения – на закрытии Нью-Йоркской фондовой биржи (NYSE) в 26 декабря их стоимость составляла 73,31 дол., однако рост пока основан на вере в будущие перспективы сервиса.

Как сообщал Digit.ru, цена акций Twitter в рамках IPO была определена в начале ноября на уровне 26 дол. за бумагу – выше ранее установленного ценового диапазона в 23–25 дол. Однако в первый же день торгов их стоимость взлетела выше 45 дол., что свидетельствует о консервативной стратегии IPO со стороны руководства Twitter и андеррайтеров.

Накануне акции Twitter обновили исторический рекорд в 74,73 дол., прежде чем закрыться на отметке 73,31 дол. – на 4,8 % выше предыдущего дня и на 182 % выше уровня IPO. Объем торгов составил около 82,76 млн акций при среднедневном показателе в 15,25 млн. Причины роста не связаны с какими-либо крупными анонсами, которые могли бы подстегнуть котировки. Более того, 19 из 26 опрошенных агентством Рейтер аналитиков рекомендуют «придерживать» или «продавать» акции Twitter.

В то же время Twitter активно обновляет продукты, в частности включил фотографии и видеоролики в ленту новостей пользователя, а также представил ряд инструментов, позволяющих лучше таргетировать и эффективнее оценивать рекламу. Это заставляет рынок верить в перспективы более активной монетизации Twitter, в том числе за счет мобильной рекламы.

Именно рост мобильной рекламы «подогрел» акции Facebook летом 2013 г., когда они впервые поднялись выше цены IPO. С конца прошлой недели, когда Facebook вошла в индекс S&P, ее акции возросли на 4,9 % – до 57,73 дол., с начала года они поднялись почти на 117 %.

По рыночной капитализации в 40,7 млрд дол. Twitter теперь почти вдвое опережает соцсеть LinkedIn и идет вровень с интернет-компанией Yahoo. Если бы акции Twitter были включены в индекс S&P 500, то сервис вошел бы в 20 % крупнейших компаний в нем. Это позволяет назвать IPO Twitter одним из самых успешных в США в этом году, отмечает The Wall Street Journal ***(Цена акций Twitter практически утроилась с момента IPO // InternetUA (http://internetua.com/cena-akcii-Twitter-prakticseski-utroilas-s-momenta-IPO). – 2013. – 27.12).***

***

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Как бы мы не сопротивлялись, но социальные сети – это уже сегодняшняя реальность, и с каждым днем они будут все сильнее набирать обороты, занимая в нашей жизни все больше и больше места. Ни для кого уже не секрет, что чрезмерное увлечение соцсетями наносит не только ощутимый вред вашей продуктивности, но и психическому состоянию. Ограничив свои коммуникации виртуальными рамками Facebook, Twitter или Google+, человек теряет способность к нормальным живому общению, теряет настоящих друзей, заменяя их совершенно чужими электронными собеседниками.

Но и это еще не все. Согласно последним исследованиям, чрезмерное времяпровождение в социальных сетях приводит и к более глубоким изменениям в психике, в том числе к появлению нарциссизма, который врачи рассматривают как серьезную личностную дисфункцию ***(Соцсети «прививают» пользователям нарциссизм // InternetUA (http://internetua.com/socseti--privivauat--polzovatelyam-narcissizm). – 2013. – 23.12).***

***

Социальные сети: что происходит в головах пользователей

Целостность историй

Нам и уж точно поколению Z становится присуще расстройство структуры информации и причинно-следственных связей. Мы все больше потребляем информацию не целостными блоками, а несвязными обрывками, перемешанными во времени и логике. Социальные сети, как правило, доносят до нашего внимания истории сильно дробленными, в разных форматах (фото/видео/текст/ссылка), без хронологической структуры. На соединение отдельных клочков историй в единое целое мозг тратит дополнительную энергию. Если ресурса на структуризацию фрагментированной истории не хватает, то человек впадает в информационный транс.

Отсюда вывод: человек подвержен ежедневному сильному стрессу, вызванному отсутствием логики и структуры информации, получаемой из соцсетей. Снять это напряжение мы можем, только упорядочив весь тот поток, который воспринимаем. С точки зрения коммуникации мозгу нужно предоставить целостные истории с сюжетом и логикой, а также с тем, что называется «когезией», или «связностью». Это и есть рассказывание историй.

Я-сериал

Раньше истории создавал некто: издательства, бренды, СМИ. В настоящее время их создает каждый, причем у всех есть возможность сделать контент высокого качества, снять видео, которое станет топовым в YouTube, и для этого уже не нужны бренды, как раньше. Человек сам по себе – медиа. Но почему только некоторые истории набирают популярность, почему не всех слушают?

Если посмотреть несколько дней подряд историю среднестатистического человека, которая формирует, предположим, хронику о нем в Facebook, то увидим ту же модель квантовой подачи информации: отдельные фрагменты истории его жизни без какого-либо порядка, в разных форматах, вне единого контекста. Хотите, чтобы вас читали, тогда создавайте целостную историю.

Бренд-персонажи

Подача информации брендами зачастую безлика, она не вызывает личностного контакта и эмоциональной привязки. Наиболее простой способ сделать присутствие бренда увлекательным – создать сериал. По сути это хронологически и логически целостная история. Здесь многое зависит от сюжета: проще всего создать сериал с ярким героем, историю которого можно будет легко проследить. Такие персонажи брендов уже начинают появляться и говорить от своего имени («Лукашівська Курка», Капитан, он же Морган и др.). Коммуникация от первого лица, внедрение личных историй и опыта выстраивают более доверительное отношение аудитории.

Интеграция вместо 360

Еще один долгоиграющий тренд, касающийся всех каналов. Для человека связь 24/7 на 360 – это удобство и безопасность, для брендов – возможность увлечь в свою целостную историю без ограничения в площадках. С точки зрения площадок выживут те, кто лучше справится с полнотой функционала и форматов проявления.

Раньше все говорили о коммуникации на 360. Что это значит: берем один слоган, один ключевой образ и забиваем ими все каналы. Но больше нет коммуникации на 360, она не эффективна. Каждому каналу присуща своя динамика, свой контент, манера подачи информации, время потребления, функционал. Задача заключается в том, чтобы грамотно интегрировать все возможные каналы, чтобы они не дублировали, а дополняли друг друга. Наружная реклама, реклама на радио и ТВ такой же инструмент, как и социалка, забывать про него не стоит.

Личный подход

У человека всегда была и остается потребность в идентификации себя: через науку, бога, искусство, окружающих. Нам с вами свойственно выражать себя и отстраиваться от остальных через вещи, поэтому большое значение для многих играет «не надеть платье, как у Маши».

При личном обращении человек переживает глубинное удовлетворение, потому что это относится лишь к нему. Поэтому мы обращаем внимание на адресованное нам сообщение, и так много сил тратят

Google и социальные сети на оптимизацию таргетинга рекламы и выдачи контента.

Кроме кастомизации информации, персонализируются продукты и сервисы: сам смоделируй себе штаны, выбери ткань и фасон – получи готовые домой или на работу. Адрес доставки и даже твой рабочий график соцсети и так знают, можно не утруждаться заполнением анкет.

Лень и безопасность

Еще два мотива предоставления информации о себе и внедрения соцсетей в каждый предмет быта: от футболок до автомобилей. Будучи унифицированной и полной базой персональных данных, социальные сети упрощают жизнь пользователя: не нужно каждый раз прописывать одно и то же для регистраций, верификаций и прочих «-ций». Что заставляет нас делиться личной информацией со всем миром? Потребность в безопасности. При высоком уровне кастомизации сервисов уровень риска (будь то врезаться с соседнюю машину, потерять кошелек или пропасть без вести) снижается.

Целесообразность, целостность информации и личный подход – не так уж и много нужно современному человеку. Бренды могут это обеспечить в том случае, если в центре коммуникации будет человек с его личными графиком, потребностями и привычками ***(Социальные сети: что происходит в головах пользователей // Южный федеральный (http://u-f.ru/Article/u1/2013/12/27/667427). – 2013. – 27.12).***

***

Маніпулятивні технології

У Facebook створили «фейкову» сторінку волинського УДАРу, на якій написали, ніби відомий журналіст – гей і педофіл. Повідомлення про це з'явилося на офіційній сторінці партії в соцмережі. На несправжній сторінці опублікували інформацію про журналіста В. Портнікова, якого звинуватили в гомосексуалізмі й педофілії.

Також на сторінці була заява про те, що волинський осередок УДАРу виходить з партії, а причиною виходу є те, що В. Портніков – активіст Євромайдану. Зауважимо, цю інформацію розтиражували кілька сайтів.

«Офіційно заявляємо: Волинська обласна організація ПП "УДАР Віталія Кличка" продовжує свою діяльність у тому ж руслі, що й дотер! Ми маємо лише ПО ОДНІЙ офіційній сторінці в кожній із соцмереж, у яких поширюється ПРАВДИВА інформація!» – ідеться в заяві, опублікованій на офіційній сторінці осередку. «Інформація, яка розміщається на будь-яких інших сторінках, не відповідає дійсності та не є такою, у яку можна вірити», – додають у партії ***(У Facebook з'явилась «фейкова» сторінка УДАРу Волині // ВолиньІнфо (http://news.volyninfo.com/volyn/246701-u-facebook-zyavilas-feykova-storinka-udaru-volini.html). – 2013. – 20.12).***

***

На акцію «Ми за мир» і просування блогів проти Євромайдану витратили понад 1 млн грн в Інтернеті, зовнішній рекламі й на радіо, пише Insider.

У перших числах грудня в Інтернеті стартувала активна кампанія з просування сайту «Ми за мир» та однойменних сторінок у соціальних мережах, де користувачів закликали утриматися від протестів на Євромайдані. Приблизно тоді ж з'явилася кампанія з просування блогів і статей, де стверджувалося, що протести зрежисовані олігархами, які борються за владу, штурм на Банковій – справа рук демонстрантів, а на Майдані легко підхопити туберкульоз. Банери розміщувалися на багатьох новинних сайтах, включаючи korrespondent.net і Vlasti.net.

Кампанія «Ми за мир» виявилася настільки масштабною, що увійшла до топ-10 в українському Інтернеті. За підрахунками дослідної компанії Factum Group Ukraine, її охоплення досягло 4,8 млн користувачів, а на її частку прийшлося 0,76 % всієї реклами в українській мережі. Просування блогів і статей було трохи менш помітним, але також досить масштабним. Аудиторія цієї кампанії могла досягти приблизно 3,2 млн українців, стверджує І. Дубинський, гендиректор Factum Group Ukraine.

У результаті бюджет кампанії «Ми за мир» становив близько 800 тис. грн за два тижні, підрахували в агентствах. Вартість просування блогів – ще близько 100 тис. грн, стверджує на правах анонімності менеджер одного з найбільших рекламних холдингів. При цьому обидві рекламні кампанії проводилися за цінами в кілька разів дорожче від середньоринкових – від двох до трьох гривень за клік, тоді як зазвичай це коштує близько однієї гривні за клік, каже гендиректор агентства інтернет-реклами UaMaster Є. Шевченко.

Чому так дорого?

Схоже організаторам кампанії було вкрай важливо зробити її масовою і провести її в той момент, коли користувачі активно обговорюють протести на Євромайдані, припускає керівник порталу Work.ua А. Міхно. «Впадає у вічі нераціональне використання бюджету. Виконавці виставили максимальну ціну за клік. Схоже, стояло завдання дати максимальне охоплення і гроші не мали значення», – вважає керівник одного з агентств.

Для порівняння: зазвичай онлайн-кампанії навіть топових брендів обходяться у 100–200 тис. грн на тиждень. Наприклад, нещодавня кампанія Comfy мала схоже охоплення аудиторії, кажуть у Factum Group Ukraine. Вартість кліка в ній становила близько 1 грн, а вся кампанія обійшлася бренду мінімум у чотири рази дешевше, стверджують в одному з агентств.

Кампанія «Ми за мир» вирішила не обмежуватися Інтернетом. Цю рекламу розміщували також у пресі, на радіо й зовнішніх носіях. «За своїм розмахом кампанія дуже схожа на активність руху "Український вибір" В. Медведчука», – зазначає керівник Асоціації зовнішньої реклами А. Біденко.

У Києві зовнішня реклама «Ми за мир» з'явилася 5 грудня і включала від 100 до 150 достатньо якісних площ. «Масштаб кампанії як мінімум у два рази перевищує активність будь-якого з топових комерційних брендів. Гадаю, загальний бюджет міг становити від 350 тис. грн на місяць», – каже А. Біденко. Таким чином, загальний медіабюджет цих компаній за два тижні становив понад 1 млн грн.

Нагадаємо, що на початку грудня середня вартість кліка за день у Google Adsense зросла майже у два рази, приблизно з 11–12 до 22 центів. Такий різкий стрибок цін експерти пояснили активізацією антимайданівської PR-кампанії ***(Базак О. На просування блогів проти Євромайдану витратили близько мільйона гривень // Гречка (http://gre4ka.info/suspilstvo/7654-na-prosuvannia-blohiv-proty-yevromaidanu-vytratyly-blyzko-miliona-hryven). – 2013. – 24.12).***

***

Группа хакеров заявила о взломе доступа к Единому государственному реестру избирателей Украины, а также ряду почтовых ящиков региональных госадминистраций по заказу заместителя Председателя Верховной Рады Украины. Однако гонорара от депутата за «проделанную работу» хакеры не получили – заказчик исчез, когда в Украине развернулись акции протеста на Майдане.

Как передает корреспондент «Одесса. Комментарии», пароли к почтовым ящикам на домене @gov.ua, а также инструкции для получения доступа к госреестру избирателей хакеры выложили в сеть. По их словам, этот жест следует расценивать как сообщение для других «недобросовестных заказчиков».

Как сообщили взломщики, они не имеют отношения к группировке Anonymous. «Мы, в принципе, никто и никак себя не проявляли. Мы не Anonymous, мы – лохи. Лохи потому, что нас кинул уважаемый в Украине человек – Первый заместитель Председателя Верховной Рады Украины И. Калетник, тот самый который был председателем ГТСУ», – пишет AIN со ссылкой на CyberGuerrilla

В ноябре 2012 г. к хакерам якобы обратился М. Герасимчук (доверенное лицо заместителя председателя Верховной Рады Украины И. Калетника) с заказом на взлом Госреестра избирателей. За это он заплатил залог, сумма которого не разглашается, однако хакеры называют ее «приличной».

Когда исполнители выполнили заказ, поступила новая задача – получить контроль над более чем сотней государственных почтовых ящиков госадминистраций Волынской, Тернопольской, Ровенской, Львовской и других областей. Однако за этот подряд хакерам не заплатили – с того момента, как в Киеве стартовали акции протеста против срыва евроинтеграции, И. Калетник, как утверждают взломщики, просто исчез.

Кроме почтовых ящиков госадминистраций, депутат якобы «заказал» взлом личной почты и мобильных устройств Председателя Верховной Рады

В. Рыбака, министра внутренних дел В. Захарченко и доступ к переписке С. Речинского. Но до «подряда» на почту журналиста исполнители не добрались, поскольку не получили гонорары за предыдущие ***(Депутат «кинул» хакеров, которые по его заказу взломали доступ к госреестру // Комментарии: Одесса (http://odessa.comments.ua/news/2013/12/25/144214.html). – 2013. – 25.12).***

***

Нужны ли бизнесу профессиональные тролли?

Тролли-фрилансеры вовсю предлагают свои услуги компаниям, однако устойчивого рынка подобных услуг пока не сформировалось.

Одно из таких писем пришло в редакцию «Ведомостей», в котором автор предлагал за деньги отстаивать любые идеи, услуги и взгляды на форумах и в социальных сетях.

Руководитель пресс-службы портала Rabota.ru И. Деречей в комментариях изданию заявила, что специалистов подобного профиля по объявлениям не набирают. Глава отдела аналитики рекрутингового портала Superjob.ru В. Чернецова также отметила, что профессиональных троллей среди соискателей крайне мало. По ее словам, за все время в резюме соискателей фраза типа «имею опыт использования троллинга как инструмента продвижения» встречалась раза три. Причем каждый раз таким резюме в публикации было отказано. Не пользуются спросом подобные услуги и среди работодателей.

Руководитель пресс-службы HeadHunter И. Тютюнджи отметил, что необходимо определиться с терминологией, кого считать троллем? Многие компании активно используют социальные сети для собственного продвижения: продаж, техподдержки, привлечения трафика или просто общения с аудиторией. Именно для этих целей компании и нанимают специалистов по соцсетям. Часто агентства берут на работу «агентов влияния», которые будут скрытым образом лоббировать интересы их заказчиков в тех же соцсетях. И в шутливой форме таких людей также можно назвать троллями. Впрочем, вакансии со словом «тролль» чаще от этого не встречаются.

Чаще всего людей берут на позицию SMM-специалиста, однако далее уже сложно проверить, чем именно они занимаются: это может быть как «белая» активность в социальных медиа, так и различные сомнительные вещи типа «партизанского маркетинга». И чаще всего подобный маркетинг проявляется в явно заказных комментариях касательно конкретных брендов, товаров или услуг. К слову, на Западе подобные вещи уже выходят из моды. Так, в этических кодексах многих компаний установлены запреты на такие методы конкурентной борьбы.

Специалисты уверены, что в России в настоящее время куда более востребованы «белые» SMM-специалисты с опытом работы в агентствах, либо на биржах фриланса. Платят им от 40 до 100 тыс. р. Тем же, кто специализируется лишь на комментариях, могут платить от нескольких

тысяч до 25 тыс. р. – все зависит от конкретной задачи и таланта исполнителя ***(Нужны ли бизнесу профессиональные тролли? // Oborot.ru (http://oborot.ru/news/13739/24). – 2013. – 26.12).***

Зарубіжні спецслужби і технології «соціального контролю»

Владельцев мобильных телефонов, желающих установить приложение Facebook Messenger, просят согласиться с тем, что гигантская социальная сеть сможет использовать микрофон их телефона для записи аудио в любое время без разрешения пользователя.

Пользователей вынуждают принять соглашение, которое позволяет Facebook «записывать аудио с помощью микрофона ….в любое время без вашего подтверждения».

Условия предоставления услуги также разрешает Facebook снимать видео и делать фотографии с использованием камеры мобильного телефона в любое время без разрешения, а также напрямую звонить по телефонным номерам, опять-таки без разрешения, за которые потом придётся платить.

Но погодите, там есть что-то ещё! Facebook также может «читать ваш журнал звонков» и «данные о ваших контактах, хранящихся в телефоне, в том числе как часто вы звонили, отправляли электронную почту или связывались иным образом с отдельными лицами».

Хотя в большинстве приложений на устройствах Android и Apple имеются такие же условия обслуживания, Facebook представляет собой на сегодняшний день наиболее откровенные требования, которые нарушают приватность.

Поскольку подавляющее большинство людей соглашаются с этими условиями, никогда их даже не прочитывая, пользователи мобильных телефонов соглашаются позволить Facebook вести за ними слежку 24 часа 7 дней в неделю, предоставляя такую прослушку, которой позавидовала бы Служба национальной безопасности.

Другие компании, выпускающие приложения, также требуют, чтобы вы позволили им определять ваше местонахождение, посылать с вашего телефона SMS, за которые придется платить, учитывать ваши контакты, статус телефона и личность, иметь «полный доступ сети» к вашему общению (иными словами, прослушивать ваши телефонные звонки), изменять или стирать содержимое, хранящееся в памяти USB, а также отключать ваш код (код из четырех цифр, который блокирует экран телефона).

Как мы подчеркивали ранее, встроенные микрофоны во всех устройствах от консолей Xbox Kinect до современных фонарей уличного освещения могут записывать личные беседы в реальном времени, что является последним гвоздём в гроб приватности по мере того, как обычный Интернет становится частью нашей жизни ***(Фейсбук хочет прослушивать ваш телефон // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/12/16/fb-spy.html). – 2013. – 16.12).***

***

Представители социальной сети Facebook признались, что имеют доступ даже к неопубликованным записям, после того как двое исследователей соцсети сообщили о том, что отслеживали активность около 5 млн пользователей из США и Великобритании. Об этом пишет издание The Los Angeles Times, которое цитирует «Обозреватель» (http://tech.obozrevatel.com/news/49320-facebook-vidit-dazhe-neotpravlennyie-zapisi.htm).

Исследователи выясняли, как часто пользователи занимаются самоцензурой во время набора текстов сообщений и комментариев. Содержание записей можно было отслеживать, когда пользователи набирали более пяти символов. Если записи не отправлялись в течение 10 минут после окончания набора, это считалось самоцензурой. При этом исследователи отмечают, что не читали содержание записей, а лишь отслеживали сам факт набора текста.

В Facebook подчеркнули, что исследование проводилось в соответствии с соглашением пользователя, которое принимает каждый регистрирующийся в соцсети.

Чтобы не позволить Facebook следить за собой пользователем предложили выбрать один из двух путей: выключить JavaScript или отказаться от соцсети. В первом случае многие веб-страницы будут отображаться некорректно ***(Facebook видит даже неотправленные записи // Обозреватель (http://tech.obozrevatel.com/news/49320-facebook-vidit-dazhe-neotpravlennyie-zapisi.htm). – 2013. – 18.12).***

***

Документи з архіву Е. Сноудена говорять про те, що американські й британські розвідники не обмежуються земними справами – вони впровадилися у віртуальні світи World of Warcraft і Second Life, збираючи розвіддані у світі онлайн-ігор, який нараховує мільйони гравців. Про це інформує The New York Times.

Побоюючись, що терористичні й злочинні організації скористаються іграми для таємного обміну повідомленнями, переказу грошей і підготовки змов, співробітники розвідслужб ступили на територію, населену цифровими персонажами, серед яких зустрічаються ельфи, гноми й супермоделі, ідеться в статті.

Розвідники створювали вигаданих персонажів, щоб вести стеження і вербувати інформаторів, не забуваючи збирати інформацію про спілкування геймерів між собою.

Онлайн-ігри здаються невинними, пише один з надсекретних документів Агентства національної безпеки (АНБ) США, що опинився в руках журналістів, але в майбутньому вони можуть перетворитися на «систему комунікації, насичену цілями», що дасть змогу підозрюваним «зникнути, будучи в усіх на очах».

Водночас працівники ігрових компаній і незалежні експерти зазначають, що не спостерігали ознак активного використання ігор терористичними організаціями. «Терористичні групи мають значно ефективніші й простіші способи зберігати канали зв'язку в секреті, ніж поставити троля на аватар», – розповів експерт П. Зінгер з Brookings Institution.

Наразі не зрозуміло, як саме розвід служби отримали доступ до особистих даних користувачів і скільки геймерів були завербовані.

Розробник гри World of Warcraft, студія Blizzard Entertainment, заявляє, що ні АНБ, ні Центр урядового зв'язку Великобританії (GCHQ) не отримували згоди компанії на збір даних за допомогою їхнього продукту. «Нам невідомо про будь-яке стеження, – повідомили представники студії. – Якщо воно ведеться, то без нашого дозволу».

В одному з документів АНБ ідеться, що ведення розвідки у World of Warcraft «продовжує розкривати свою потенційну важливість для радіоелектронної розвідки, виявляючи облікові записи, персонажів і співтовариства, пов'язані з ісламськими радикальними групами, поширенням ОМП і торгівлею зброєю».

Ще до того, як американський уряд почав стежити за віртуальними світами, важливість відеоігор для збирання даних зрозуміли в Пентагоні, повідомляється в публікації. У 2006–2007 рр. командування спеціальних операцій Міноборони США разом з рядом закордонних компаній розробляли ігрові додатки для мобільних телефонів. За словами учасників цього проекту, ігри не позиціонувалися як продукт Пентагона і використовувалися для збирання інформації про користувачів ***(Спецслужби вербують геймерів для стеження за користувачами онлайн-ігор // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/12/19/spetssluzhby_verbuyut_geymeriv_dlya_stezhennya_za_korystuvachamy_onlaynigor_448354). – 2013. – 19.12).***

***

Компания Google, с самого своего появления, опровергла все аксиомы предпринимательства, умудрившись построить процветающий бизнес на бесплатных продуктах. Самый лучший поиск, почта, множество других сервисов предоставляются пользователям совершенно бесплатно, но одновременно приносят компании хороший доход. Так значит Google, вместо денег, берет с нас что-то другое?

Именно так. Мы оплачиваем пользование продуктами компании своим вниманием и своей приватной информацией. Как-то я уже писал о том, как Google собирает данные о нас в сети. А сегодня мы остановимся на другом аспекте этого вопроса, как мобильные устройства с Android на борту шпионят за своими хозяевами.

История ваших перемещений

Android по умолчанию отслеживает местоположение вашего телефона. Он использует эту информацию, чтобы сделать вашу жизнь проще, например

Google Now покажет вам погоду, достопримечательности и маршруты, связанные с вашим местоположением. Он также может использовать эти данные, чтобы позволить вам отслеживать в Интернете потерянный телефон с помощью функции Android Device Manager.

Одновременно это значит, что Google известно, где и когда вы были вместе с вашим телефоном. И будьте уверены, что эти данные аккуратно аккумулируются и сохраняются. И даже если вы отключите GPS, все равно ваше местоположение будет довольно точно определено с помощью близлежащих Wi-Fi сетей и вышек сотовой связи.

Кстати, вы ведь придумали достаточно сложный пароль к своей сеточке? Зря старались. Всего одна галочка в настройках резервного копирования ваших данных отправила ваш суперсложный пароль в Google. Эта компания знает пароли ко всем беспроводным сетям в мире, не плохо, правда?

Письма, контакты и события

Android предоставляет действительно удобную услугу по синхронизации вашей электронной почты, событий календаря и записей в адресной книге между разными устройствами. Однако это само собой подразумевает, что все эти данные хранятся на серверах компании. Уничтожаются ли они после того, как стали вам не нужны, или сберегаются бесконечно, образуя цифровой отпечаток вашей жизни? Очевидно, последнее.

Пароли, история сайтов, поисковых запросов

Мобильная версия Chrome представляет собой хороший браузер, который с удовольствием используют очень многие. А если вы используете еще и десктопную версию программы, то получаете возможность практически бесшовного перехода между разными устройствами, ведь все ваши данные автоматически подтягиваются и синхронизируются. Да, с помощью серверов Google, разумеется. А это значит, что вы, по доброте душевной, поделились всеми своими паролями, интересами и увлечениями с одной очень любопытной компанией.

Фотографии

Компания прилагает чрезвычайно большие усилия по продвижению своего социального сервиса Google+. Постепенно все больше продуктов и сервисов интегрируется в Google+, и не за горами то время, когда вам будет уже не отвертеться от установки соответствующего клиента. А значит, все ваши фоточки будут автоматически подгружаться на серверы Google, связаны с вашим именем и сохранены.

А что насчет СМС и звонков?

Вот с этим пока все в порядке. При использовании стандартных программ, никакие данные о вашей переписке и разговорах никуда не отправляются. Однако в последней версии системы Android 4.4 Kit Kat, на место привычной системы сообщений, пришел Google Hangouts, так что опция резервного копирования истории вашего общения уже, думаю, не за

горами. Исключительно для удобства и безопасности пользователей, само собой.

Стоит ли нам опасаться и что делать?

Если посмотреть объективно и назвать вещи своими именами, то надо признать, что Google успешно строит самую совершенную глобальную систему слежения за своими пользователями. И если при использовании обычного компьютера мы можем хоть как-то регулировать поток собираемых о нас данных, то с мобильным гаджетом, который всегда с нами, справиться гораздо труднее. Хотя большинство людей успокаивает себя привычной мантрой: «я маленький человек, до меня никому нет дела» и «мне нечего скрывать», никто не знает, кто и когда вашими данными воспользуется. И с какой целью.

Так что лучше все-таки держать этот процесс под контролем и следовать нескольким простым правилам.

1. Четко осознайте, что никакой приватности ни в сети, ни в жизни нет. Каждый ваш шаг может быть зафиксирован, просчитан и отправлен на хранение до подходящего случая.

2. Старайтесь не пользоваться продуктами одной компании. Если есть выбор, то отдавайте предпочтение сторонним решениям.

3. Пользуясь продуктами Google, не ленитесь пройтись по настройкам и отключить слишком навязчивые опции, нарушающие вашу приватность.

При написании этой статьи я совсем не хотел бросить тень на компанию Google, многими услугами которой сам с удовольствием пользуюсь. Точно такую же статью можно было бы написать про iPhone или Windows Phone. Но так уж получилось, что именно сервисы Google приобрели глобальный размах, и отеческая опека именно этой компании становится все более напрягающей. А вы что скажете по этому поводу? ***(Android – маленький шпион в вашем кармане // InternetUA (http://internetua.com/Android---malenkii-shpion-v-vashem-karmane). – 2013. – 28.12).***

***

Независимые эксперты говорят, что доверие к отрасли коммерческой ИТ-защиты сильно подорвано после скандала с компанией RSA, которая, как утверждает Э. Сноуден, была подкуплена АНБ США с целью размещения дефектного алгоритма генерации псевдо-случайных последовательностей, который бы позволял взламывать зашифрованные данные.

RSA отрицает подобные сведения, тогда как в документах Э. Сноудена сказано, что компания получила от АНБ 10 млн дол. за использование алгоритма с искусственной уязвимостью. Речь здесь идет об алгоритме Dual EC DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), используемого в продукте RSA Bsafe.

Независимые специалисты говорят, что отчет оказал серьезное влияние на секьюрити-отрасль, так как RSA здесь считается очень влиятельной компанией. 23 декабря М. Хиппонен, известный специалист по ИТ-

безопасности и технический специалист компании F-Secure, направил в RSA письмо о том, что он не поедет на конференцию RSA Conference 2014 из-за отношений RSA с американской разведкой. «Не думаю, что ваша конференция от этого сильно пострадает. Большинство заявленных спикеров – американцы, зачем им беспокоиться о том, что слежка направлена не на них, а на пользователей из других стран. Однако я – иностранец и я отказываюсь от участия в конференции», – пишет М. Хиппонен в письме для Д. Такки, генерального директора компании EMC, которой принадлежит RSA.

К. Ливитт, управляющий партнер консалтинговой компании Bishop Fox, говорит, что хотя RSA и опубликовала опровержение, сам его текст написан очень обтекаемо и в нем компания напрямую не утверждает, что никогда не работала с АНБ и не использовала кодов этого ведомства, вместо этого компания позиционирует себя как жертву. «Ответ RSA, конечно, есть, но он очень банальный и многие важные вопросы по существу не снимает», – говорит он.

М. Грин, специалист по криптографии из Университета Джона Хопкинса, говорит, что как вся эта история, так и невнятные оправдания RSA наводят большую тень на всю ИТ-индустрию. «В своем оправдании RSA утверждает, что использовала общепринятые решения, но не стоит забывать, что эта компания – поставщик коммерческих решений и она должна сама создавать полностью защищенные системы, а не прятаться за чужими спинами», – говорит он.

Напомним, что в документах Э. Сноудена сказано, что RSA работало с АНБ как минимум с 2004 г. ***(Скандал с RSA бросает тень на всю ИТ-отрасль // InternetUA (http://internetua.com/skandal-s-RSA-brosaet-ten-na-vsua-it-otrasl). – 2013. – 27.12).***

***

В чем заключается «Эффект Сноудена»?

Э. Сноуден для кого-то стал героем, а для кого-то предателем, продавшим свою родину ради личной славы. Кто-то думает, что бывший или, как считает сам Э. Сноуден, нынешний, сотрудник АНБ всего лишь пешка в чьей-то большой игре, а кто-то видит в нем одиночку, бросившего вызов системе.

Как бы там ни было на самом деле, публикация секретной информации о слежке американских спецслужб практически за всем миром вызвала массу событий, конечный итог которых оценить пока довольно сложно. «Эффект Сноудена» – явление глобальное, то, что сделал этот человек, известно во всем мире. Так в чем же заключается этот эффект?

Во-первых, доверие людей к ИТ-компаниям было серьезно подорвано. Как бы Google, Apple, Yahoo и другие теперь не оправдывались, вряд ли кто-то поверит, что в следующий раз, когда скандал утихнет, технологические гиганты не предоставят доступ к личной информации пользователей по первому же требованию властей.

Во-вторых, после публикации некоторых документов из огромной коллекции Э. Сноудена и бурной общественной реакции на вскрывшиеся факты шпионажа, технологические компании оперативно ввели шифрование практически всех информационных потоков, с которыми работают. Теперь Google и Yahoo шифрует не только внешний трафик, но даже данные, которые перемещаются между собственными серверами компаний. Особое внимание стало уделяться защите информации, хранящейся в мобильных устройствах. Не исключено, что iPhone 6 и Samsung Galaxy S5 будут по умолчанию шифровать все данные пользователя, и именно эту функцию производители будут выделять особо.

В-третьих, облачные технологии, которые стали трендом в 2013 г., также оказались под ударом. Если простых пользователей это касается несильно, то компании, которых Microsoft и Google плавно подводили к работе «в облаке», теперь вряд ли захотят хранить информацию, представляющую собой коммерческую тайну, фактически у всех на виду. Конечно, в 2014 г. облачные технологии продолжат также активно развиваться, однако главными станут именно вопросы безопасности и доверия к поставщикам услуг.

В-четвертых, международный имидж США стал еще хуже. Как выяснилось, АНБ шпионило не только за простыми гражданами, но и за действующими и даже бывшими главами государств. Например, прослушивали нынешнего президента Бразилии и канцлера Германии. Также без внимания АНБ не остались главы крупнейших компаний, нефтяных гигантов и так далее.

В-пятых, как утверждает сам Э. Сноуден, публикация секретных материалов – это послание самой АНБ, которая должна вспомнить, что же она защищает. В данном случае ставится вопрос о том, может ли правительство вторгаться в частную жизнь своих и чужих граждан, даже если их цели самые светлые и добрые, в чем, в общем-то, тоже есть большие сомнения.

И, наконец, «Эффект Сноудена» – это философский посыл людям. Согласны ли мы на то, чтобы государство вторгалось в нашу частную жизнь, чтобы все наши действия записывались и анализировались, пусть даже ради нашего собственного блага. Сам Э. Сноуден сравнил происходящее в настоящее время с романом Дж. Оруэлла «1984». И, кажется, будущее, когда государство будет полностью контролировать человека, его действия и мысли, а личной жизни не будет в принципе, наступит уже скоро.

Причем люди уже сегодня не против этого – АНБ работает в штатном режиме, никто не удалил свои аккаунты из социальных сетей и электронной почты. Можно сказать, что мы сами приближаем такое будущее, транслируя в сеть свои мысли и действия посредством Twitter, Instagram, Facebook и «ВКонтакте». Однако когда мы сами что-то показываем, и когда кто-то подглядывает без нашего разрешения – это далеко не одно и то же.

«Все, чего я хотел – чтобы общественность могла высказать свое мнение по поводу того, как ею управляют», – сказал в разговоре с

журналистами The Washington Post Э. Сноуден ***(В чем заключается «Эффект Сноудена»? // InternetUA (http://internetua.com/v-csem-zakluacsaetsya--effekt-snoudena). – 2013. – 27.12).***

***

АНБ не справляется с объёмами трафика

Благодаря документам от Э. Сноудена стало известно о программах Агентства национальной безопасности США (АНБ) по тотальной прослушке интернет-трафика, в том числе о программе MUSCULAR по съёму трафика между дата-цетрами компаний Google и Yahoo по всему миру непосредственно через кабели оптоволоконной связи.

Как теперь выяснилось, АНБ не справляется с обработкой слишком больших объёмов трафика, которые поступают в её систему, и в 2013 г. агентство попросило уменьшить масштабы слежки по программе MUSCULAR.

«Их нынешняя деятельность уменьшает работоспособность системы, когда они обрабатывают все эти данные», – сказал У. Бинни, разработчик программного обеспечения, которое используется в АНБ, в интервью WSJ. По его словам, АНБ погрязло в массиве ненужной информации, которая мешает агентству осуществлять полезную работу по поиску потенциальных террористов.

Неудивительно, что некоторые эксперты выражают мнение, что тотальная слежка за гражданами, в том числе сбор всех метаданных и анализ интернет-трафика, не помогла предотвратить ни единого террористического акта.

У. Бинни практически неизвестен общественности, в отличие от Э. Сноудена. Тем не менее, он проработал в АНБ более 30 лет и его нынешние показания имеют не меньший вес, чем документы, опубликованные Э. Сноуденом.

Так или иначе, но АНБ решает проблему по-своему. Они считают, что для обработки возрастающих объёмов трафика нужно увеличивать вычислительные мощности и строить новые дата-центры. Например, в настоящее время в Юте заканчивается строительство гигантского дата-центра АНБ. Но вряд ли это сможет решить проблему, потому что трафик в Интернете растёт слишком быстрыми темпами. Документы, опубликованные Э. Сноуденом и датированные 2012 г., тоже свидетельствуют о том, что представители АНБ жалуются, что сбор метаданных с иностранных мобильных телефонов «превосходит наши возможности по его обработке и хранению».

Как сказал У. Бинни, в ответ на жалобы о недостатке технических средств для обработки данных АНБ получило указание уменьшить объём слежки, не собирать информацию о всех гражданах, а сконцентрироваться на слежке за теми, кто «может представлять угрозу государству и его союзникам». Агентству рекомендовали разработать программное

обеспечение для более «интеллектуальной» фильтрации собранных метаданных.

Э. Сноуден и многие правозащитники говорили, что АНБ собирает слишком много информации, большая часть которой не нужна. Оказывается, что эта точка зрения подтверждается техническими ограничениями в самом АНБ ***(АНБ не справляется с объёмами трафика // InternetUA (http://internetua.com/anb-ne-spravlyaetsya-s-ob--mami-trafika). – 2013. – 28.12).***

Проблема захисту даних. DOS та вірусні атаки

Большинство вредоносных электронных писем можно отнести к одной из двух категорий – массовым сообщениям, ориентированным на широкий круг пользователей, или фишинговым письмам, предназначенным для конкретных пользователей. Между этими двумя группами можно выделить еще одну, более «продвинутую» – персонализированные электронные сообщения, якобы отправленные друзьями из Facebook, либо использующие информацию из соцсетей для приманки.

Для того чтобы заставить пользователя установить на свою систему вредоносное ПО, злоумышленники проделывают огромную работу, собирая информацию о пользователе и делая электронное письмо более персонализированным.

Как сообщил в своем блоге эксперт Й. Уллрих, одним из таких фишинговых писем является письмо о якобы новом полученном сообщении в сервисе WhatsApp, которое выглядит совсем как настоящее. Кроме того, кнопка Play наводит на мысль о том, что сообщение действительно голосовое. Загружаемое пользователем письмо является ZIP-файлом. При этом имя исполняемого файла варьируется в зависимости от телефонного номера, соответствующего местоположению IP-адреса, с которого был загружен файл.

Так, если файл загружен на домашний компьютер в Джексонвилле, США, имя исполняемого файла будет VoiceMail_Jacksonville_(904)458abcd.exe, если в Уэйне, Пенсильвания, – VoiceMail_Wayne_(610)458abcd.exe. При этом последние четыре цифры являются числами телефонного номера ***(Фишинговые письма становятся более персонализированными // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/12/16/targeted-phishing.html). – 2013. – 16.12).***

***

Эксперты проанализировали киберугрозы, с которыми сталкивались жители Украины в 2013 г. По степени риска, которому подвергаются в киберпространстве интернет-пользователи, а также по среднему количеству обнаруженного вредоносного ПО на компьютерах, самым безопасным

городом страны оказался Львов. Верхние же строчки нерадостных рейтингов киберинцидентов занимает столичный Киев. Об этом свидетельствуют данные «Лаборатории Касперского», на которые ссылается ЛІГАБізнесІнформ.

На одного киевского пользователя в 2013 г. приходилась в среднем 21 атака с использованием вредоносного ПО. А в киберспокойном Львове, к примеру, этот показатель оказался в три раза меньше – семь атак на пользователя. На втором месте – Одесса, в которой на одного интернет-пользователя пришлось 16 веб-атак. Замыкает тройку лидеров Харьков с показателем 12 зловредов на одного пользователя.

«Лидерство» Киева продолжается и с точки зрения показателя обнаруженных вредоносных объектов на компьютерах пользователей. В среднем житель этого города 13 раз за год сталкивался с так называемыми локальными угрозами: вредоносными программами, содержащимися на флэш-носителях или попавшими на компьютер иным способом. Следующая за столицей Одесса не сильно отстает: здесь на одного пользователя пришлось 11 локальных угроз. В других же крупных городах – Харькове, Донецке и Львове – этот показатель несколько ниже и варьируется от пяти до семи.

По количеству переходов по небезопасным ссылкам, ведущим на фишинговые или вредоносные сайты, жители Киева разделяют первенство с Одессой: в среднем в 2013 г. у каждого пользователя в этих городах было заблокировано пять переходов. Показатели других городов отличаются от них почти в два раза: в Харькове и Донецке каждый пользователь пытался пройти по опасным ссылкам в среднем три раза, а в Львове – два.

Примечательно при этом, что два самых «киберопасных» города – Киев и Одесса – предпочитают старую операционную систему, безопасность которой вызывает сомнения многих экспертов: Windows XP. Здесь эта система установлена почти на трети компьютеров: 32 % и 29 % соответственно. В более безопасных Донецке и Харькове, к примеру, любителей этой устаревшей ОС заметно меньше – здесь почти та же треть пользователей работает на более современной Windows 7 ***(Эксперты назвали города Украины, которые чаще всего подвержены кібератакам // Подробности.UA (http://podrobnosti.ua/internet/2013/12/17/948661.html). – 2013. – 17.12).***

***

Согласно исследованию, 40 % мобильных устройств были скомпрометированы во время целевых атак, направленных на кражу корпоративных секретов.

Смартфоны, планшеты и другие мобильные устройства все чаще подвергаются заражению вредоносным ПО, а также используются в целенаправленных атаках. Такие результаты показало исследование среди 676 ИТ-специалистов и безопасников.

Компания Ponemon Institute провела исследование «состояние угроз для конечных устройств в 2014 г.». Примерно 2/3 респондентов указали, что мобильные устройства в их компаниях подвергались заражению вредоносным ПО, а 40 % устройств были скомпрометированы во время целевых атак, направленных на кражу корпоративных секретов. В 63 % организаций сотрудники используют мобильные устройства, а их среднее количество возрастет в течение трех последующих лет с 5 тыс. до 7 тыс. устройств.

Согласно опросу, проспонсированному компанией Lumension, больше половины инцидентов, связанных с целевыми атаками на мобильные устройства, были обнаружены вследствие появления подозрительного трафика внутри корпоративных сетей. В настоящее время для проведения целенаправленных атак злоумышленники используют в большинстве случаев фишинговые email-сообщения, хищение кликов, и подписанные фальшивыми сертификатами приложения.

Только половина опрошенных используют в компаниях политики BYOD, и примерно в половине случаев администраторы полагаются на добровольную установку средств защиты на клиентские устройства. Что касается облачных сервисов, используемых компаниями, показатели по внедрению политик возросли на 14 % по сравнению с прошлым годом – 54 % респондентов указали, что у них есть централизованные политики по обеспечению безопасной работы с облачными сервисами.

К сожалению пока далеко не все компании готовы дополнительно финансировать затраты, связанные с обеспечение безопасности мобильных устройств. Только 44 % опрошенных компаний предусмотрели увеличение бюджета в 2014 г.

Также в следующем году компании планируют приобретать средства контроля за приложениями, DLP-системы, системы управления мобильными устройствами (MDM) и системы контроля за устройствами. Самыми основными требованиями к системам управления мобильными устройствами респонденты назвали возможность определения и защиты от вредоносного ПО, резервное копирование и управление доступом.

Согласно выводам исследования, на сегодняшний день смартфоны и планшеты представляют большую угрозу для корпоративной безопасности, чем офисные ПК и ноутбуки ***(Злоумышленники используют мобильные устройства для осуществления целевых атак // InternetUA (http://internetua.com/zloumishlenniki-ispolzuuat-mobilnie-ustroistva-dlya-osusxestvleniya-celevih-atak). – 2013. – 19.12).***

***

Эксперты «Лаборатории Касперского» обнаружили новый троян, под названием ChewBacca, использующий для связи с командным сервером анонимную сеть Tor.

Сеть Tor позволяет анонимно размещать в сети веб-сайты и предоставлять пользователям доступ к ним на условиях анонимности. В

числе прочих задач она используется для распространения запрещенного контента. Изначально проект финансировался Научно-исследовательской лабораторией ВМС США. Позже он перешел под покровительство некоммерческой организации. В настоящее время затраты на проект на 60 % покрываются различными ведомствами правительства США.

Троян ChewBacca создан с помощью компилятора Free Pascal 2.7.1 и имеет формат исполняемых файлов PE32. Размер файла составляет 5 МБ, в его состав входит клиент Tor 0.2.3.25.

После запуска вредоносное приложение помещает файл spoolsv.exe в папку C:\Documents and Settings\All Users\Start Menu\Programs\Startup\ и запрашивает IP-адрес компьютера жертвы с помощью бесплатного публичного сервиса http://ekiga.net/ip. Файл клиента Tor, tor.exe, помещается в папку Temp. Затем троян начинает регистрировать все нажатия на клавиши компьютера, записывая информацию в файл system.log, размещенный в папке Temp.

Командный сервер злоумышленников представляет собой набор серверного программного обеспечения LAMP, включающий Linux-дистрибутив CentOS, Apache 2.2.15, MySQL и PHP 5.3.3. Сервер размещен по адресу http://5jiXXXXXXXXXgmb.onion. Ссылка ведет на страницу ввода логина и пароля с фоновым изображением, на котором изображен персонаж «Звездных Войн» Чубакка.

Троян ChewBacca заставил экспертов «Лаборатории Касперского» обратить на себя внимание из-за того, что использует сеть Tor. Это очень редкое, но не единичное явление, утверждают аналитики компании. Около недели назад была обнаружена очередная модификация трояна Zeus с такой же функцией.

Однако ChewBacca нельзя найти в открытом доступе, в отличие от Zeus. Эксперты предполагают, что новый троян либо пока находится на стадии разработки, либо находится в руках узкого круга злоумышленников ***(Найден троян, живущий в анонимной сети Tor // InternetUA (http://internetua.com/naiden-troyan--jivusxii-v-anonimnoi-seti-Tor). – 2013. – 18.12).***

***

Практически сразу после появления на игровых рынках новых консолей PlayStation 4 и Xbox One эксперты из «Лаборатории Касперского» обнародовали статистические данные о вирусных тенденциях в геймерской среде.

Как выяснилось, в течение 2013 г. любители видеоигр становились объектом атак порядка 11,7 млн раз. Таким образом, ежедневно в течение года игроки по всему миру ежедневно сталкивались с 34 тыс. нападений. При этом на сегодняшний день антивирусной компанией было зафиксировано более 4,6 млн различных образцов вредоносного ПО, ориентированного на компьютерные игры и их пользователей.

В «Лаборатории Касперского» также предупреждают, что в канун зимних праздников и сопутствующих им подарочных акций, геймерам стоит проявить особую бдительность и принять меры предосторожности.

Отметим, что согласно отчету, чаще всего жертвами «игровых» вирусов и прочих связанных угроз становятся игроки из Испании. В период с января по ноябрь 2013 г. количество инцидентов безопасности, связанных с тамошними геймерами, составило 138,7 тыс. случаев. Далее с небольшим отрывом следует Польша (127,5 тыс. случаев), а на третьем месте расположилась Италия (немногим более 75 тыс. случаев) ***(В 2013 г. геймеры становились объектом хакерских атак более 11 млн раз // InternetUA (http://internetua.com/v-2013-godu-geimeri-stanovilis-ob-ektom-hakerskih-atak-bolee-11-millionov-raz). – 2013. – 18.12).***

***

По данным исследователей из CERT Polska, злоумышленники внедряют в системы Linux и Windows вредоносное ПО, направленное на дальнейшее осуществление DDoS-атак.

В настоящее время наблюдается расширение Linux-версии вируса, которую успешно использовали для осуществления атак по подбору паролей к SSH-серверу. Это значит, что уязвимыми являются только те системы, которые позволяют удаленный SSH-доступ и имеют слабые пароли.

«Нам удалось получить в распоряжение 32-битный бинарный ELF-файл», – сообщили представители CERT Polska в своем блоге. Исполняемый файл работает в режиме демона и подключается к C&C-серверу посредством использования предустановленного IP-адреса и порта. После первого запуска вредоносное ПО отправляет данные об операционной системе и ждет дальнейших команд от злоумышленников.

Благодаря анализу исследователям удалось установить, что вирус позволяет осуществление DDoS-атак четырех типов. Одной из них является атака DNS Amplification, в рамках которой на DNS-сервер отправляется запрос, содержащий 256 случайных или заранее определенных поисковых запросов.

Во время осуществления атаки вирус постоянно общается с подконтрольным злоумышленникам сервером, предоставляя данные о запускаемых процессах, мощности процессора, загрузке системы и скорости сетевого подключения.

Что касается Windows-версии, то вредоносное ПО устанавливается по адресу: «C:\Program Files\DbProtectSupport\svchost.exe» и запускается вместе с системой. Единственным отличием является то, что этот вирус подключается к C&C-серверу через доменное имя, а не IP-адрес. При этом используется один и тот же сервер ***(Системы Windows и Linux атакует новый вирус для DDoS-атак // InternetUA (http://internetua.com/sistemi-Windows-i-Linux-atakuet-novii-virus-dlya-DDoS-atak). – 2013. – 20.12).***

***

Эксперты компании Eset, занимающейся вопросами безопасности, считают, что в следующем году интернет-пользователи по всему миру будут уделять особое внимание безопасности своих данных и анонимности, поэтому особым спросом начнут пользоваться анонимная сеть TOR и технологии шифрования. Отметим, что согласно данным компании ComRes в настоящее время проблемы безопасности волнуют 79 % пользователей.

По словам специалистов из Eset, в ближайшем будущем программное обеспечение, существующее в настоящее время, будет полностью заменено анонимными поисковиками, браузерами, ОС и сервисами для обмена сообщениями. Тем не менее, эксперты отмечают, что анонимность в сети также несет определенную угрозу.

Эксперты также считают, что в 2014 г. для выражения протеста все чаще будут использоваться DDoS-атаки. Особенно это касается граждан, недовольных деятельностью правительств своих стран.

Аналитики прогнозируют, что в следующем году следует ожидать роста активности ПО для вымогательств и блокировщиков экранов. Кроме того, существенно возрастет число вирусов для платформы Android ***(В 2014 г. спросом у пользователей будут пользоваться анонимные сети и шифрование // Центр информационной безопасности (http://www.bezpeka.com/ru/news/2013/12/19/encryption-demand-in-2014.html). – 2013. – 19.12).***

***

Как победить DDoS

Уходящий – 2013 г. был весьма активным в сфере киберпреступности. Несмотря на то что системы защиты современных ресурсов постоянно модернизируются, «любовь» злоумышленников к DDoS-атакам постоянно портит нервы IT специалистам.

Массовый DDoS банков

За текущий год 30 украинских банков пострадало от DDoS. При этом атаки проводились направленно и сразу на все банки.

«В этом году по банковской системе Украины было совершено две целевые, заранее подготовленные, массированные DDoS-атаки, которые коснулись многих крупных игроков. Речь не идет об одном банке – 30 банков подтвердили, что стали целевым объектом таких атак со стороны организованных преступников, при этом в одно и то же время», – прокомментировал руководитель по безопасности технологий розничного бизнеса Альфа-Банка (Украина) С. Досенко для Минфин.

Стоит отметить, что основной целью проведения DDoS-атак на банковские структуры – отвлекающий маневр, в то время как остальные силы хакеров будут направлены на взлом системы и попытках хищения информации или денежных средств.

Полит-DDoS

События, развивающиеся на Евромайдане, не только показали сплоченность украинского народа, но и уязвимость отечественных серверов

перед злодеями. Вместе с украинским народом на свой – виртуальный майдан вышли и DDoS-атакеры, и здесь, как по законам военного времени – пощады не было.

За последнее время несколько ресурсов, принадлежащих центральным украинским СМИ, таких как «Зеркало недели», «Левый берег», LB.ua и «Украинская правда» – подверглись мощным атакам. Среди числа пострадавших от DDoSa СМИ и набирающий популярность интернет-телеканал «Громадське ТБ», все эфирное время которого отводится освещению событий Евромайдана. Так 29 ноября в течение полутора часов интернет-телеканал вынужден был транслировать черный экран. Коллеги из «Громадського ТБ» подтвердили, что причиной сбоя было именно постороннее вмешательство в работу хостинга, обслуживающего их сайт. «Уточнюємо лише те, що, за словами наших технічних партнерів, атака здійснювалась на “сервер, на якому лежить наш сайт”. Тому ми не маємо права стверджувати, що атакували саме нас. Крім того, ми отримали анонімного листа від працівника одного з місцевих провайдерів, у якому він розповідав про “запит наближених до КМДА органів” про надання їм детальної технічної інформації щодо Громадського», – уточняют в пресс-службе канала.

Заслуживает внимания и атака на национальный портал № 1. Как признаются IT-специалисты компании УКР.НЕТ, атаки по своей мощности и подготовленности заставили админов понервничать.

«Готовь сани летом»

Специалисты компании ITbiz которых мы попросили прокомментировать ситуацию, уверены, что проблемы можно было бы избежать, если бы владельцы серверов заранее позаботились о своей безопасности. На примере обучающего видео, с помощью которого компания подготавливает свои кадры для обслуживания аппаратного решения подавляющего DDoS-атаки, ведущий специалист В. Еланин объяснил, что влиять на атаки не только можно, но и нужно и для этого есть серьёзные инструменты. «На видео показаны искусственно смоделированные условия для демонстрации DDoS-атаки. Тут используется приложение LOIK. Данная программа не раз афишировалась организацией Anonymous как программа, которой они пользуются для своих атак, сам софт является бесплатным и доступен для скачивания даже в Google play. Кроме того, каждый пользователь скачавший этот софт добровольно вступает в сеть ботнет, то есть его компьютер будет использоваться в других атаках когда это потребуется», – комментирует ведущий специалист компании ITbiz В. Еланин.

«Подавление на атаки производится с помощью комплекса Peakflow SP от компании Arbor Networks, – продолжает В. Еланин. – Мы увидели возрастание вредного трафика, и то, как специалист запустив устройство – настраивает его для борьбы с атакой. Решение поддерживает большое количество противомер для разных видов атак, настройка некоторых из них показано в видео. Следует отметить, что это демонстрация операторского

решения Peakflow SP. В продуктовой линейке Arbor Networks есть и клиентское решение, это Arbor Pravail APS, конечно, гораздо лучше когда эти два устройства работают в связке, но каждое решение может работать независимо. При этом клиентское решение спроектировано таким образом, чтобы подавлять DDoS прямо из коробки, без дополнительных настроек, и в автоматическом режиме» ***(Воронин Д. Как победить DDoS // InternetUA (http://internetua.com/kak-pobedit-DDoS). – 2013. – 20.12).***

***

Темная сторона WhatsApp

Самый популярный мессенджер WhatsApp – одна из любимейших тем для обсуждения в кругах мобильных пользователей. Однако остались еще темы, не получившие достаточного освещения. Например, условия, права и обязанности, которые возлагает на нас мессенджер и о которых мы чаще всего даже не задумываемся. Так ли все просто с WhatsApp, и какие сюрпризы таит в себе оборотная сторона медали?

Изменения условий

Первое, что стоит сказать о WhatsApp – это то, что данное приложение оставляет за собой право вносить изменения любого характера в условия использования его услуг без предварительного уведомления. Для нас это в первую очередь означает, что приложение автоматически получает разрешение на использование некоторых наших личных данных. Не самая радужная перспектива в свете и без того спорного уровня безопасности, предоставляемого приложением.

Минимальный возраст

Факт из рубрики «Мало кто знает»: минимальный допустимый возраст пользователя WhatsApp составляет 16 лет. Для любителей переписываться, не достигших этого возраста, в приложении реализован родительский контроль.

Гарантии и безопасность

– Первое, о чем стоит упомянуть: нет никаких гарантий того, что история ваших переписок или файлы, которые были отосланы через мессенджер, останутся конфиденциальной информацией. Вообще проблема безопасности личных данных в WhatsApp – притча во языцех, и пока мы не видим никакой тенденции к исправлению этого недочета;

– К тому же, сообщения, которые мы удаляем, на самом деле не стираются безвозвратно – они лишь архивируются и продолжают храниться в памяти устройства;

– Кроме этого, проблема затронула и личную информацию людей в нашем списке контактов. Получается, что мы предоставляем мессенджеру не только номер телефона, но и адрес электронной почты, привязки к профилям в социальных сетях и всю прочую информацию, которая прописывается в полях контакта, когда он создается или связывается с синхронизированными записями. WhatsApp здесь делает предположение, что мы уже получили разрешение от каждого из наших контактов на получение личной

информации, ну а мессенджер получил разрешение от нас. Так сервис попросту умывает руки, фактически перекладывая ответственность на пользователей.

Ограничения

– Запрещено использование WhatsApp в коммерческих целях. Продажи, продвижение, и прочие операции с товаром, направленные на получение выгоды, запрещены в чатах мессенджера;

– запрещено использованием ботов для составляения и рассылки спам-сообщений;

– обмен контентом сексуального характера не запрещен, но для отправки сообщения подобного содержания, нужно для начала выслать предупреждение, например, эмотикон +18 или знак X;

– запрещено использовать код программы WhatsApp для создания приложений-клонов;

– запрещено размещать материалы, которые не являются нашей собственностью, без разрешения владельца. За подобные нарушения интеллуктуальных прав WhatsApp ответственности не несет;

– то же самое касается и ссылок на вредоносные сайты.

Обязательства и последствия

– Если вы потеряли телефон, или у вас его украли, а вы были пользователем WhatsApp, необходимо написать разработчикам электронное письмо и проинформировать их о случившемся. Таким образом, если с аккаунта будет совершено нарушение, с вас ответственность снимается;

– при нарушении какого-либо из пунктов правил WhatsApp, разработчики программы имеют право прекратить обслуживание аккаунта нарушителя без объяснения причин;

– у нас есть 12 месяцев на то, чтобы сообщить об инцидентах внутри приложения: вирусах, кражах, спаме.

Таким образом, WhatsApp – это не просто поделка мобильных дел мастеров, а целая система, которая определяет наши права и обязанности и приписывает некоторые правила, нарушение которых карается исключением из круга пользователей ***(Темная сторона WhatsApp // InternetUA (http://internetua.com/temnaya-storona-WhatsApp). – 2013. – 22.12).***

***

Антивирусная компания Eset сообщила о всплеске активности банковского трояна Qadars, способного обходить механизм двухфакторной аутентификации через вредоносный мобильный компонент. Злоумышленники уже активно используют данный троян для атак на пользователей в Европе, Азии, Австралии и Северной Америке.

По данным экспертов, троян Win32/Qadars применяет различные виды веб-инъекций (внедрение вредоносного кода в код легальной программы или процесса), стремясь похитить у пользователя аутентификационные данные для онлайн-банкинга. Кроме того, киберпреступники обманом принуждают к установке мобильного компонента, который позволяет обойти систему

подтверждения банковских операций. В настоящее время киберпреступники ориентируют троян Qadars на пользователей (и соответствующие банковские учреждения) Голландии, Франции, Италии, Канады, Индии, Австралии и ряда других государств.

Для осуществления мошеннических операций Win32/Qadars использует распространенный у злоумышленников метод «человек в браузере» (Man-in-the-Browser, MiB). В ходе подобной кибератаки вредоносный код внедряется в браузер (Internet Explorer, Firefox и др.) через программную уязвимость, позволяя киберпреступнику менять параметры транзакции или проводить иные мошеннические операции с банковским счетом жертвы.

«Внедряемый в браузер контент может быть чем угодно, – но, как правило, он представляет собой форму авторизации, которая используется злоумышленниками для сбора конфиденциальных данных пользователей. Также это может быть и вредоносный JavaScript, который будет стремиться перевести средства с банковского счета пользователя на счет злоумышленников без его ведома, – говорит Жан-Йен Бутен (Jean-Ian Boutin), исследователь вредоносного ПО в канадском подразделении Eset. – Файл Qadars, содержащий веб-инъекции, меняется достаточно часто и используется злоумышленниками для переориентирования вредоносного кода на нужные банковские сайты. Для достижения максимального эффекта, злоумышленники стремятся заражать пользователей в определенных, заранее выбранных странах» ***(В сети зафиксирован всплеск активности банковского трояна Qadars // InternetUA (http://internetua.com/v-seti-zafiksirovan-vsplesk-aktivnosti-bankovskogo-troyana-Qadars). – 2013. – 23.12).***

***

Компания «Доктор Веб» сообщает об обнаружении новой вредоносной программы, которая нацелена на добычу электронной валюты Bitcoin. Эксперты отмечают, что методы действия трояна несколько отличаются от его предшественников.

Новая вредоносная программа встраивает свой компонент в процесс explorer.exe. Потом троян находит запущенные в системе процессы браузеров и внедряет в них вредоносный код, который был сгенерирован в отдельной динамической библиотеке.

Напомним, что все предыдущие версии трояна встраивали вредоносную библиотеку в процессы браузеров Microsoft Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome, Chromium, Mail.Ru Интернет, Яндекс.Браузер, Рамблер Нихром.

Новый троян также наделен функцией добычи электронной валюты Bitcoin. Именно такой функционал все чаще используют злоумышленники в последнее время в связи с повышением популярности и подорожанием этой электронной валюты ***(Обнаружен новый троян для добычи Bitcoin // InternetUA (http://internetua.com/obnarujen-novii-troyan-dlya-dobicsi-Bitcoin). – 2013. – 25.12).***

***

Поскольку Windows XP больше не будет получать обновления, все уязвимости в ней всегда будут нулевого дня.

Несмотря на то что Windows XP является второй по популярности платформой, под управлением которой работает почти треть компьютеров мира, Microsoft прекратит поддержку своей 12-летней ОС 8 апреля следующего года. В связи с этим, компания неоднократно просила пользователей перейти на более новую версию платформы. Эксперты предупреждают, что после прекращения поддержки сотни миллионов компьютеров и ноутбуков окажутся под угрозой, поскольку хакеры начнут атаковать незащищенные системы.

Ранее Microsoft предупреждала, что хакеры могут использовать патчи для Windows 7 и 8 для обнаружения эксплоитов для XP. «В первый месяц, когда Microsoft выпустит обновления безопасности для поддерживаемых версий ОС, хакеры осуществят реверс-инжиниринг, найдут уязвимости в XP и проверят, подходят ли патчи для нее, – сообщил директор группы Microsoft Trustworthy Computing Т. Рэйнс. – В случае, если патчи подойдут, злоумышленники разработают эксплоиты для этих уязвимостей. Поскольку Windows XP больше не будет получать обновления, все уязвимости в ней всегда будут нулевого дня».

По данным Microsoft, с июля 2012 по июль 2013 г. она исправила 30 уязвимостей в Windows 7 и 8, предоставляя хакерам широкие возможности для реверс-инжиниринга. По словам экспертов, компании рискуют стать жертвами масштабных DDoS-атак, вредоносного ПО и хищения данных. Кроме того, они не смогут устанавливать новое программное обеспечение, которое будет разрабатываться в будущем ***(Патчи для Windows 7 и 8 помогут хакерам разработать эксплоиты для уязвимостей в Windows XP // InternetUA (http://internetua.com/patcsi-dlya-Windows-7-i-8-pomogut-hakeram-razrabotat-eksploiti-dlya-uyazvimostei-v-Windows-XP). – 2013. – 25.12).***

***

Хакеров привлекают не только правительственные сайты или банковские серверы, на которые в последнее время периодически накатывают волны DDoS-атак. Попытки «положить» сайт ощутила на себе фондовая биржа ПФТС, однако сумела их отразить, сообщает информационно-аналитический портал Inpress.ua.

На сайт фондовой биржи ПФТС, а также на один из серверов биржи в течение 20 и 23 декабря было совершено несколько DDoS-атак, сообщили в ПФТС.

В частности, 20 декабря неизвестные совершили несколько попыток атаковать сайт биржи. Так, по информации ПФТС, в течение дня на сайт биржи осуществлялось большое количество запросов, которые временно снижали его производительность. «Оперативное вмешательство IT-специалистов ПФТС, которые блокировали адреса, с которых поступали

неправомерные запросы, позволило быстро восстановить работу сайта биржи в полном объеме», – отметили на бирже.

23 декабря состоялась DDoS-атака на один из серверов ПФТС. Как отметили на бирже, около 10:00 поступило несколько обращений клиентов, которые по техническим причинам не могли соединиться с торговой системой. Как сообщили IT-специалисты ПФТС, причиной стало большое количество запросов, в результате чего канал связи, который вел к одному из серверов доступа биржи, был чрезмерно загружен.

Как сообщили в ПФТС, обслуживание участников торгов, которые столкнулись с этой проблемой, перевели к альтернативным провайдеров, что дало возможность «приобщиться к торгам на бирже без задержек» ***(На украинскую биржу ценных бумаг налетели хакеры // InternetUA (http://internetua.com/na-ukrainskuua-birju-cennih-bumag-naleteli-hakeri). – 2013. – 25.12).***

***

Эксперты «Лаборатории Касперского» проанализировали данные о срабатывании функции «Родительский контроль», полученные с помощью облачной системы мониторинга угроз Kaspersky Security Network (KSN) за 2013 г. в Украине, передает корреспондент proIT со ссылкой на пресс-службу компании.

Как уточняется, срабатывание «Родительского контроля» происходит в тех случаях, когда дети случайно или намеренно переходят на сайты с нежелательным содержанием.

В результате анализа оказалось, что сайты категорий «Социальные сети» и «Почта» лидируют с большим отрывом от остальных – 64 % и 19 % соответственно. Помимо этого, категория «Игры» попала на 3-е место (4,56 %), четвертую позицию занимает категория «Порнография и эротика» (3,74 %), а на пятом месте оказалось нелегальное программное обеспечение.

«Не имея достаточного опыта работы с компьютерами и мобильными устройствами, дети ненамеренно совершают ошибки, за которые часто приходится платить родителям. 18 % опрошенных мам и пап понесли финансовые убытки, либо потеряли важные данные из-за действий ребенка. В основном, дети случайно удаляли важные сведения и без спроса пользовались платежными средствами», – говорит К. Игнатьев, руководитель группы анализа веб-контента «Лаборатории Касперского».

Как уточнили корреспонденту proIT в компании, каждый пятый родитель не предпринимает никаких действий для того, чтобы обезопасить своего ребенка в Интернете. А те взрослые, которые все же решили обезопасить своего ребенка, выбирают различные методы защиты. Так, 38 % родителей ограничивают время, которое дети проводят в Интернете, а 31 % регулярно проверяют историю браузера. При этом лишь 25 % используют защитное ПО с функциями родительского контроля ***(«Родительский контроль» в Украине от Касперского чаще всего срабатывает в соцсетях***

// proIT (http://proit.com.ua/news/internet/2013/12/23/130044.html). – 2013. – 23.12).

***

Новое вредоносное программное обеспечение, функционирующее как модуль для веб-серверов Apache и Nginx, продается на подпольных хакерских форумах, говорят в ИТ-компании IntelCrawler.

Новый вредонос получил название Effusion и согласно описанию он может вставлять код в реальном времени в веб-сайты, размещенные на скомпрометированных веб-серверах. Инъекции кода могут создать условия для переадресации на хакерские сайты, кроме того, атакующие могут встраивать разные социально-инженеринговые тактики для обмана пользователей.

IntelCrawler сообщает, что Effusion работает с сервером Nginx 0.7 и старше, вплоть до текущей версии 1.4.4, а также с 32- или 64-битной версией Apache под Linux или FreeBSD. Маскируется вредонос под модуль, расширяющий базовую функциональность веб-сервера. Сам по себе вредонос может вставлять заданный контент в различные MIME-типы, в частности в JavaScript, HTML или PHP либо вначале страницы, либо по специальным тэгам в разметке. Атакующие могут также обновлять конфигурацию вредоноса и удаленно контролировать модификации кода.

В коде также есть возможность фильтрации, которая ограничивает события при наступлении инъекции кода. Effusion поддерживает фильтрацию по заголовкам, источникам заходов пользователей, пользовательским агентам, IP-адресам или их диапазонам. Одновременно с этим, вредонос также старается заполучить root-доступ к системе, чтобы оператор кода смог проводить другие деструктивные действия с зараженным сервером.

А. Комаров, генеральный директор IntelCrawler, рассказал, что авторы Effusion просят на форумах за скомпилированный вариант вредоноса 2500 дол., что является довольно высокой ценой даже по меркам функциональных вредоносных кодов и может указывать на то, что авторы этой разработки намеренно ограничивают круг пользователей их продукта.

Отметим, что вредоносные модули для Apache появляются не впервые, однако до сих пор серверу Nginx удавалось избежать этой участи. Впрочем, в настоящее время доля Nginx на мировой арене преодолела 14 %, согласно данным Netcraft, и злоумышленники начали обращать внимание в том числе и на этот продукт ***(Новый вредоносный код атакует сервер Nginx // InternetUA (http://internetua.com/novii-vredonosnii-kod-atakuet-server-Nginx). – 2013. – 25.12).***

***

Ресурс Dogewallet, специализирующийся на хранении и обмене электронных денег, подвергся хакерской атаке. Сообщение об этом 26 декабря появилось на сайте Reddit. В результате атаки у пользователей

Dogewallet было похищено более 21 млн так называемых догкоинов (цифровой валюты, созданной на основе популярного интернет-мема).

По словам представителей Dogewallet, хакеру удалось взломать файловую систему сайта и получить доступ к хранившимся в ней онлайн-кошелькам. После атаки ресурс временно приостановил свою работу. «Все инвестированные в валюту средства будут компенсированы. Мы работаем над этим», – говорится в размещенном администрацией Dogewallet сообщении. В пересчете на доллары США сумма похищенных денег составила более 12 тыс.

Первые сведения о том, что Dogewallet был взломан, стали поступать от пользователей сайта ранним утром 26 декабря. Владельцы онлайн-кошельков сообщали о взломе своих аккаунтов и о том, что хранившиеся на них деньги неожиданно пропали. Указывались суммы от 9500 до одного миллиона догкоинов.

Цифровая валюта догкоин (dogecoin) была разработана в конце ноября программистом из США Б. Маркусом и его другом из Австралии Д. Палмером. За основу разработки был взят открытый исходный код цифровой криптовалюты лайткоин (litecoin), усовершенствованного, но более дешевого аналога резко набравших популярность в 2013 г. биткоинов.

Официально догкоины были представлены 8 декабря. С тех пор курс валюты пережил несколько серьезных колебаний. На момент написания этой заметки один догкоин стоил около 0.00000083 биткоина или около двух копеек.

Своим названием валюта обязана распространенному интернет-мему с собакой породы Сиба-ину (мем строится вокруг изображения собаки, окруженного различными фразами, написанными шрифтом Comic Sans). По словам разработчиков догкоинов, цифровая валюта была создана ими «ради смеха» ***(Хакерам впервые удалось взломать кошельки с «собакоденьгами» // InternetUA (http://internetua.com/hakeram-vpervie-udalos-vzlomat-koshelki-s--sobakodengami). – 2013. – 26.12).***

***

Как сообщает эксперт «Лаборатории Касперского» К. Раю в блоге компании, за последние годы использование редких видов вредоносного ПО, схожих по функционалу с вирусом Wiper, резко возросло. В связи с этим исследователь составил перечень самых опасных аналогов данной угрозы.

«За последние годы произошло несколько крупных инцидентов, связанных с деструктивной деятельностью вредоносных программ. Мы решили составить короткий обзор наиболее заметных случаев», – поясняет эксперт. По его данным, после Wiper наибольший ущерб атакованным системам удалось нанести вредоносному приложению Shamoon, с помощью которого была нарушена работа и стерта информация с 30 тыс. компьютеров нефтяной компании Saudi Aramco. Отдельного внимания также заслуживают вирус Groovemonitor/Maya, вредоносная программа Dark Seoul, а также червь Narilam.

Последний вызывает интерес из-за способности портить базы данных определенных компьютерных программ, которые используются прежде всего в Иране. Вносимые Narilam искажения не очевидны, и их довольно сложно обнаружить. Если позволить вирусу «функционировать на компьютере годами, результат может оказаться крайне разрушительным» ***(Обзор наиболее опасных аналогов вируса Wiper // InternetUA (http://internetua.com/obzor-naibolee-opasnih-analogov-virusa-Wiper). – 2013. – 28.12).***

***

Уходящий год запомнился антивирусным экспертам серией кибератак на мировые ИТ-корпорации, социальные сети и ростом числа вирусов, нацеленных на мобильные устройства. Об этом говорится в годовом отчете международной антивирусной компании ESET.

«Эти атаки в той или иной степени привели к утечке персональных данных работников компаний и пользователей сервисов», – уточнили в компании. В разное время атакам подверглись интернет-ресурсы Twitter, Facebook, Apple и Microsoft, миллионы аккаунтов были скомпроментированы. «Так, в феврале эксперты ESET обнаружили вредоносный код PokerAgent, который заражал пользователей приложения Zynga Poker в Facebook. Целью хакеров были личные данные пользователей, а также информация о привязанных к их аккаунтам банковских картах», – напомнили в компании. В итоге «зловред» похитил данные более 16 тыс. аккаунтов в соцсети.

«В 2013 г. под ударом находились не только пользователи соцсетей, но и поклонники общения через интернет-мессенджеры, – отмечают эксперты ESET. – Обнаруженная масштабная спам-кампания в сервисах Skype, gTalk и QIP и ряде других мессенджеров подвергла опасности более полумиллиона пользователей во всем мире, включая 40 тыс. в России». В результате атак злоумышленники получили доступ к персональным данным.

Если говорить о мобильных угрозах, то, по сравнению с аналогичным периодом прошлого года, количество новых семейств вредоносных программ для операционной системы Android в 2013 г. возросло на 43,6 %, причем наибольшие темпы роста угроз продемонстрировали Иран, Китай и Россия. «Аналогичные темпы роста сохранятся и в 2014 г., новые мобильные угрозы продемонстрируют не только количественный, но и качественный рост. В частности, будут все более активно использовать уязвимости мобильных платформ и их компонентов», – предупреждают эксперты.

Активность программ-вымогателей в 2013 г. тоже продемонстрировала значительный рост. По данным ESET, на российских пользователей пришлось более 44 % обнаружений вредоносных программ. «В 2014 г. не стоит ждать снижения активности вымогателей, этому поспособствует популярность виртуальной валюты Bitcoin», – уверены эксперты ***(Уходящий год отличился ростом числа кибератак на ИТ-корпорации и соцсети //***

InternetUA (http://internetua.com/uhodyasxii-god-otlicsilsya-rostom-csisla-kiberatak-na-it-korporacii-i-socseti). – 2013. – 28.12).

***

InternetUA (http://internetua.com/siriiskaya-elektronnaya-armiya--vnov-atakuet-amerikanskie-smi). – 2013. – 27.12).

«Сирийская электронная армия» вновь атакует американские СМИ

ФБР США предупредило крупнейшие американские СМИ о том, что хакерская группировка «Сирийская электронная армия» начала проведение кампании по кибератаке в отношении отрасли средств массовой информации в Штатах. Согласно сообщению ведомства, сейчас ряд журналистов таких изданий, как The New York Times, CNN, The Wall Street Journal и других получили по электронной почте сообщения о событиях в Сирии. Во всех сообщениях содержатся ложные сведения и гиперссылки, при нажатии на которые происходит переадресация через ряд URL, которые в конечном итоги приводят на ресурс с поддельными формами авторизации, выполненными в стиле Google.

Задача данной кампании – похищение личных реквизитов журналистов от почты, социальных сетей, редакционных порталов и других ресурсов, работая с которыми можно было бы получить ту или иную закрытую информацию.

Напомним, что «Сирийская электронная армия» выступает в поддержку президента Б. Ассада, тогда как США традиционно критикуют этот режим. Также следует напомнить, что ранее «Сирийская электронная армия» уже взламывала Facebook- и Twitter-ленты крупных западных СМИ.

***

Исследователи из Стэнфордского университета, США, при помощи анализа метаданных абонентов сотовой связи доказали, что установить имя владельца мобильного устройства, зная номер телефона, очень просто.

Для подтверждения своей теории исследователи собирали номера телефонов, время и продолжительность звонков, информацию о координатах телефона и так далее.

Для исследования на телефоны добровольцев устанавливалась программа Metaphone, которая собирала метаданные АНБ. Программа записывала номера из списка вызовов, текстовые сообщения и другую информацию. На определённом этапе эксперимента учёные осуществили случайную выборку из 5 тыс. номеров добровольцев, и попытались определить их имена. Четверть всех имён удалось установить простым поиском телефонного номера в справочниках Yelp, Facebook и Google Places.

Отметим, что результат был получен без каких-либо особенных усилий, можно сказать, автоматически. Для усложнения задачи исследователи взяли наугад ещё 100 номеров и запустили поиск Google. Менее чем за час они смогли установить владельцев 60 из 100 номеров.

Оставшиеся номера специалисты «прогнали» через агрегатор данных Intelius – процент определения имени повысился до 91 %. До максимально

возможных 100 % точность возросла тогда, когда к делу подключили профессиональное программное обеспечение для анализа данных ***(Узнать имя человека по номеру его телефона оказалось предельно просто // InternetUA (http://internetua.com/uznat-imya-cseloveka-po-nomeru-ego-telefona-okazalos-predelno-prosto). – 2013. – 27.12).***

***

Эксперты Gibson Security сообщили, что обнаружили новую брешь в безопасности социальной сети Snapchat.

Всего несколько секунд необходимо умелым хакерам, чтобы, пользуясь уязвимостью социальной сети, вычислить сотовые номера телефона пользователя и снять все его настройки приватности.

Несмотря на крайне необычную идею и скепсис инвесторов, запуск социальной сети Snapchat вызвал большой интерес среди пользователей Интернета. Смысл нового проекта проста – зарегистрированный пользователь отправляет фотографию своему другу. Тот ее открывает, просматривает, а через несколько секунд она удаляется. Максимальное время просмотра составляет 10 секунд. Пользуясь данной опцией, многие пользователи делились с другими личными фотографиями, надеясь на анонимность (все пользователи использую псевдонимы вместо реальных имен), которую дарит новая социальная сеть.

Уязвимость обнаружена в версиях клиента Snapchat для мобильных платформ Android и iOS. Злоумышленники могут рассекретить имя пользователя, сохранить локально его историю переписки и изменить содержание непрочитанных сообщений.

Несколько месяцев назад представители Gibson Security сообщили разработчикам Snapchat об обнаруженных ошибках, однако не получили ответа. Публикация информации об уязвимости пользователей – это вынужденная мера Gibson Security, которая была предпринята для предупреждения людей о потенциальной опасности ***(Алексеева В. Социальная сеть Snapchat оказалась опасной // Позитайм.ru (http://positime.ru/socialnaya-set-snapchat-okazalas-opasnoj/27970). – 2013. – 28.12).***