

**СОЦІАЛЬНІ МЕРЕЖІ
ЯК ЧИННИК
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

*Огляд інтернет-ресурсів
(4–17.03)*

2013 № 6

Соціальні мережі як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(4–17.03)
№ 6

Засновники:

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

Головний редактор

О. Онищенко, академік НАН України

Редакційна колегія:

В. Горовий (заступник головного редактора, науковий керівник проекту),
В. Касаткін, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

© Національна бібліотека України
імені В. І. Вернадського, 2013

Київ 2013

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ.....	4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА.....	12
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ	19
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ.....	31
Інформаційно-психологічний вплив мережевого спілкування на особистість.....	31
Маніпулятивні технології.....	36
Зарубіжні спецслужби і технології «соціального контролю»	46
Проблема захисту даних. DOS та вірусні атаки	50

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Соціальна сеть «Одноклассники» запускает сервис персональных рекомендаций музыки «Мое радио». Об этом сообщает пресс-служба компании Mail.Ru Group, которой принадлежит соцсеть.

Данный сервис самостоятельно находит и формирует список песен для пользователя, опираясь на его музыкальные вкусы. Рекомендации работают следующим образом. Анализируется максимум активности пользователя, чтобы определить его вкусы, в частности, что человек слушал, в какой последовательности, какое количество раз, что добавлял в собственные списки песен. На основе этой информации сервис и рекомендует песни.

Помимо этого, для каждого формируется список персональных «радиостанций», представляющий собой различные музыкальные направления, которыми интересуется пользователь. Чтобы воспользоваться данным сервисом, необходимо зайти во вкладку «Музыка», выбрать раздел «Мое радио» и начать слушать сразу или сначала выбрать радиостанцию, которая поможет подобрать музыку в определенном стиле.

«Благодаря запуску радио, мы планируем на 10 % увеличить количество пользователей сервиса “Музыка” и на 10–20 % – количество прослушиваемых треков каждым пользователем», – сказал И. Широков, руководитель социальной сети «Одноклассники».

Ранее пользователи «Одноклассников» могли получать рекомендации от социальной сети о похожих песнях для определенного исполнителя.

Сервис «Музыка», запущенный летом 2011 г., позволяет пользователям прослушивать музыку из обширной фонотеки сайта, загружать собственные треки, создавать плейлисты и получать доступ к плейлистам друзей. С недавних пор сервис также позволяет приобрести музыку прямо на «Одноклассниках» и скачать ее на свое устройство.

Напомним, ранее Google приступил к плавному развертыванию в рамках своей сети Google+ нового сервиса для любителей музыки. Новый сервис позволяет создавать музыкальные коллекции, сканируя записи на пользовательском компьютере и копируя некоторые из них в облако, чтобы позже пользователь мог в потоковом режиме прослушивать загруженные мелодии при помощи плеера Google Play Music Manager (*Соцсеть «Одноклассники» запускает персональные «радиостанции» // Газета «Донбасс»* (<http://donbass.ua/news/technology/internet/2013/03/05/socset-odnoklassniki-zapuskaet-personalnye-radiostancii.html>). – 2013. – 5.03).

Gemius Україна оприлюднила ТОП-20 сайтів Уанету за січень 2013 р. Дані базуються на результатах дослідження Gemius Audience (Fusion Panel).

У рейтингу сайтів за охопленням Інтернету соціальна мережа «ВКонтакте» з грудня опустилася на одну позицію і зайняла третє місце в рейтингу. Mail.ru, у свою чергу, піднявся на другу позицію. Четверте місце, як і раніше, займає пошукова система yandex.ua, а п'яте – YouTube. Соціальна мережа «Однокласники» обійшла Facebook і перебуває на 8 позиції у рейтингу з охопленням аудиторії в 33,2 %. Сервіс зберігання інформації ex.ua опустився на 3 позиції, а банк privatbank.ua – піднявся на 6.

Згідно з даними Gemius Audience (Fusion Panel), розмір інтернет-аудиторії в січні 2013 р. становив 15,9 млн осіб (real users, 14+). Всього в грудневій панелі представлені понад 650 сайтів. Звіт складений на основі 8071 анкети software-панелістів і 49 893 анкет cookie-панелістів.

Fusion-панель (змішана панель) у дослідженні gemiusAudience – об'єднує cookie-панель і software-панель.

Охоплення – процентне співвідношення кількості відвідувачів (реальних користувачів), що здійснили принаймні один перегляд сторінки на вибраному сайті за цей часовий інтервал, до загальної кількості інтернет-користувачів за цей часовий інтервал (*«Однокласники» знову стали популярнішими за Facebook в Україні // UkrainianWatcher (<http://watcher.com.ua/2013/03/05/odnoklassnyku-znovu-staly-populyarnishymy-za-facebook-v-ukrayini/>). – 2013. – 5.03*).

В Інтернеті появилась новая соціальная сеть для католиков. Сеть Awestruck, благодаря успешной рекламной кампании, насчитывает тысячи участников по всему миру, пишет Мир Вам!

Н. Сервэйс, креативный директор Awestruck, отмечает: «Католики, хотят общаться друг с другом по-новому. Возникла идея создать нечто новое, похожее на Facebook. В отличии от этой социальной сети, католическая не имеет рекламы, но наполнена содержанием, чтобы каждый католик мог найти для себя много полезного».

Авторы сайта описывают его как своего рода Facebook для католиков. Но на этом портале вы не найдете оскорбительных комментариев или материалов непристойного содержания. Тем не менее, это не означает, что социальная сеть будет лишена возможности для творчества и креатива.

Н. Сервэйс рассказал, что команда разработчиков хотела создать платформу для творческих идей, которая стала новым социальным пространством для общения католиков. Поэтому предложили посмотреть на проблемы в общении и потенциал, который существует сегодня, с учетом новых технологий.

Проект не является повторением известной социальной сети Facebook. Католический проект был разработан в Южной Африке, где католики составляют меньшинство.

«В Южной Африке только 7 % населения составляют католики. Таким образом, мы оказываемся в изоляции, не имея возможности общения через

наши национальные сети. Ведь очень трудно найти католическое содержание в светском общении», – отметил Н. Сервэйс.

Пользователи сайта это люди разных социальных и национальных групп, сферы занятий и деятельности. Это блогеры, домохозяйки, а также церковные приходы и благотворительные организации, средства массовой информации. Посещаемость и наполняемость сети продолжает возрастать (***В Интернете появилась новая социальная сеть для католиков // Власти.нет (http://vlasti.net/news/161514). – 2013. – 5.03).***

Facebook меняет дизайн главной страницы. Новый вид которой будет напоминать теперь то, как она выглядит на мобильных устройствах. Также появляются различные тематические альтернативы у основной новостной ленты соцсети. Реклама будет занимать большее место, чем раньше, становясь более заметной.

Однако ведущий инженер проекта К. Струар отрицает, что это является главной целью предлагаемых новшеств. Он также не согласен с предположением, что новый дизайн нацелен на то, чтобы люди проводили на сайте соцсети больше времени.

К. Струар заявил, что стремился к тому, чтобы ограничить тот объем информации, который показывает новостная лента, делая каждый пост более «цепляющим».

«Мы хотим очистить страницу, привести ее в порядок, сделать более простой, более современной и более удобной для использования», – сказал он.

В дизайн страницы социальной сети внесены три основных изменения:

Сайт переходит от формата с тремя колонками к формату с двумя. Таким образом главная лента новостей становится больше. Это позволяет всем постам, будь это обновления от друзей или реклама, занимать большую часть страницы.

К левой стороне страницы добавляется всплывающая черная панелька. Она содержит закладки приложений, ссылки на отдельных друзей, инструменты для чата и календаря, а также уведомитель об «апдейтах».

Кроме того, помимо стандартной новостной ленты, пользователь сможет выбирать альтернативные ленты. Можно будет получать все обновления от своих друзей, а не только те, которые выбраны по алгоритму Facebook. Может быть также создана специальная лента, посвященная организациям и людям, которые интересны пользователю. Особая страница может касаться также размещенных фотографий или музыкальных материалов: обновлений от музыкантов, которые нравятся пользователю, объявлений о концертах и информации о песнях, которые друзья пользователя слушают с помощью таких сервисов как Spotify и Rdio.

Социальная сеть также изменила свой логотип, отказавшись от facebook в пользу иконки с буквой f.

Еще одно новшество касается автоматического появления карт рядом с постами о месторасположении чего-либо.

Без сомнения, инвесторы и рекламодатели будут теперь заинтересованы в том, чтобы узнать, повлияют ли изменения на то, как будет использоваться платный контент.

В Facebook заявляют, что рекламные объявления из основной новостной ленты пользуются большей популярностью, чем те, которые размещены справа. Эта колонка уже сегодня отсутствует на приложениях для мобильных.

Увеличение новостной ленты делает из рекламного поста самый большой элемент экрана, который будет занимать без малого треть всей страницы (*Facebook меняет дизайн главной страницы // InternetUA (<http://internetua.com/Facebook-menyaet-dizain-glavnoi-stranici>). – 2013. – 7.03*).

Стартап из Одессы запустил бесплатное приложение для пользователей социальной сети «ВКонтакте» – «ВК.Рация». Ранее та же команда запускала похожее по функционалу приложение GroupVox для Facebook. Компания-разработчик появилась в прошлом году, называется GroupVox Inc., главным техническим руководителем ее является А. Макаров, сообщает AIN.UA.

Если пользователь установит приложение на смартфон и войдет под своим аккаунтом «ВКонтакте», он получит возможность голосового общения в чатах с друзьями из этой социальной сети (в личных разговорах, в групповых чатах, в чатах сообществ). Предполагается, что все участники чата слышат пользователя, как только он нажмет кнопку записи сообщения. Сообщения записываются в облаке, их можно прослушать после разговора.

В компании утверждают, что помехи, которые могут возникнуть при записи, не зависят от их технологии, а только от качества микрофона и фонового шума со стороны пользователя. Ограничение по количеству человек в чате – 15 тыс.

Из браузера пока что доступна только функция прослушивания голосового общения участников чата и отправка текстовых сообщений. «Для общения в существующих группах и сообществах “ВКонтакте”, приложение позволяет сгенерировать и отправить на стену сообщества ссылку на веб-страницу, где в прямом эфире в браузере можно читать и слушать все текстовые и голосовые сообщения. Оттуда же можно и отправлять текстовые сообщения. Голосовые сообщения при этом можно отправить только из мобильного клиента “ВК.Рации”», – пояснили в компании (*Одесские разработчики запустили приложение для голосового общения в чатах «ВКонтакте» // AIN.UA (<http://ain.ua/2013/03/07/115716>). – 2013. – 7.03*).

Геолокационная соцсеть Foursquare выпустила обновление для приложения на платформе iOS, существенно облегчающее процесс «чекина» – отметки в каком-то месте. Теперь «зачекиниться» можно будет быстрее и легче.

Некоторые эксперты пророчат Foursquare великое будущее, другие предрекают сервису скорую смерть. Соцсеть постоянно пытается расширить свою функциональность, предоставляя все больше и больше информации об окружающих пользователя локациях. Тем не менее, основой для поддержания проекта на плаву по-прежнему является количество выполненных пользователями «чекинов». Чтобы простимулировать людей «чекиниться» чаще, соцсеть выпустила обновление своего iOS-приложения, упрощающее этот процесс.

Компания утверждает, что теперь «чекины» стали «молниеносно быстрыми». «Когда вы нажмёте на кнопку “зачекиниться” и увидите список локаций, просто удерживайте палец на нужной надписи. Зеленая полоска быстро промелькнет вверху экрана и вуаля! Вы моментально зачекинились», – сообщают разработчики приложения.

После нововведения процесс «чекина» стал как-бы чуть менее официальным. Пользователю уже почти не представляется шанса задуматься о том, хочет ли он рассказать всем о своем местонахождении. Человек просто притрагивается пальцем к записи, и через секунду «чекин» завершен. Удерживание пальца на определенной части экрана, сопровождающееся заполнением индикатора, заставляет вспомнить сервис Vine, в котором подобным образом реализована съемка видео. Раньше пользователям, выбрав локацию, приходилось подтверждать чекин. Выкинув лишний шаг, Foursquare существенно убыстрила всю процедуру.

Тестируя новую функцию, мы нашли небольшой баг – если во время заполнения индикатора «чекина» сделать скриншот экрана, чекин произойдет автоматически, вне зависимости от того, додержал пользователь палец или нет. Стандартное нажатие на необходимую локацию открывает привычный экран, на котором можно добавить к «чекину» текст и изображения.

Нововведение безусловно увеличит количество проходящих через соцсеть «чекинов». Тем не менее, соцсети придется все так же отчаянно бороться за место на рынке, учитывая что собственные геолокационные сервисы появляются у многих конкурентов (***Foursquare ускорила «чекины» // InternetUA (<http://internetua.com/Foursquare-uskorila--csekini>). – 2013. – 11.03).***

Корпорация Google решила отказаться от некогда популярного хранилища фото Picasa Web Albums. Вместо обычного интерфейса пользователей направляют в их профили в соцсети Google+.

Таким образом, Google начала перенаправление посетителей сервиса Picasa Web Albums на социальную сеть Google+. При попытке просмотреть веб-альбомы сервиса, браузер переходит к профилю пользователя в Google+, в котором возникают альбомы из Picasa Web Albums. Это действие можно отменить и вернуться к прежнему виду.

Более того, IT-компания заменила ссылку Picasa Web Albums на Google+ в навигационном меню на своем ресурсе, который служит для доступа к услугам Google. Также на сайте техподдержки Google отмечается, что Google+ является «новым домом для ваших фотографий».

Отметим, что возможности Picasa Web Albums включают ограничение доступа к альбомам и возможность загрузки фото в полном разрешении. Прежде этот сервис был один из немногих, который предоставлял подобную опцию. В дополнение к веб-сайту юзеры могут использовать приложение Picasa, которое позволяет легко загружать фото с локального диска на сервер.

Напомним, что год назад Google решила отказаться от дальнейшего распространения ПО для доступа к Picasa Web Albums с систем на базе Linux и iOS, в рамках очередной фокусировки усилий на более перспективных сферах.

Сообщается, что Picasa Web Albums вскоре станет очередной жертвой оптимизации, которая проводится гендиректором Google Л. Пейджем, занявшим свой пост в апреле 2011 г. С тех пор корпорация закрыла несколько десятков проектов, включая Google Buzz, Google Desktop, Google Labs, Knol и др. (*Google принял решение отказаться от легендарного сервиса // Вечерние Вести (<http://gazetavv.com/news/world/80576-google-prinyal-reshenie-otkazatsya-ot-legendarnogo-servisa.html>). – 2013. – 8.03*).

Запущенная в конце прошлого года в Twitter функция, позволяющая пользователям скачать архив твитов из собственных микроблогов, теперь доступна на 12 языках в дополнение к изначально поддерживавшемуся английскому. Поддержку получили не только весьма распространенные языки, вроде немецкого, французского и испанского, но и ряд довольно экзотических, в том числе малайский и хинди.

Всего, как отмечают создатели Twitter, возможность скачать архивы своих твитов теперь имеют более 70 % пользователей сервиса микроблогов. Однако останавливаться на достигнутом разработчики не намерены и собираются уже «в течение ближайших месяцев» сделать функцию архивации твитов доступной на всех языках, которые поддерживаются в Twitter, включая русский (*Twitter разрешает архивацию твитов для неанглоязычных пользователей // InternetUA (<http://internetua.com/Twitter-razreshaet-arhivaciua-tvitov-dlya-neangloyazicsnih-polzovatelei>). – 2013. – 13.03*).

Facebook вводит тэги, посвященные образу жизни.

Как сообщает Украинский Бизнес Ресурс, после запуска обновленного сервиса ленты новостей компания Facebook объявила о новых способах использования разработчиками сервиса Open Graph для разработки приложений, посвященных образу жизни (lifestyle), подразумевая под этим термином четыре типа содержания: фитнес, книги, фильмы и телевидение.

Facebook вот уже несколько месяцев разрабатывает альтернативу популярной функции Like, позволяя разработчикам добавлять свои собственные функции, но в то же время внедряет «официальные» функции достаточно медленно, чтобы сократить избыточность и продвинуть новые категории в ленте новостей. Дополнительные функции дают разработчикам возможность использовать все больше и больше видов активности, в которые люди хотят быть вовлечены, по крайней мере на это надеется Facebook.

Девять новых «команд», добавленных на сегодняшний день, выглядят следующим образом:

- фитнес: бежать (run), ходить (walk), ездить на велосипеде (bike);
- книги: читать (read), оценить (rate), цитировать (quote), хотеть прочесть (want to read);
- кино и ТВ: оценить (rate), хотеть посмотреть (want to watch).

Для среднестатистического пользователя Facebook появление этих дополнительных команд просто означает, что больше приложений, связанных с образом жизни, появится в его новостной ленте, поскольку этому будет способствовать социальная сеть. Но только при условии, что друзья будут использовать программы, в которые разработчики приложений внедрили перечисленные команды. В конце концов, все сводится к экосистеме Facebook и тому, что она может дать разработчикам.

Всего два месяца назад Facebook запустила Flexible Sentences, функцию, которая позволяет разработчикам настроить синтаксис там, где не хватает контекста и / или текст не встраивается в исходную структуру предложения. Теперь разработчики получили больше команд, с которыми можно работать на начальном этапе, поскольку зачастую невозможно продвинуться дальше, не подобрав глаголу адекватной замены.

На этот раз, очевидно, что Facebook приурочил введение новых команд к запуску обновлений в ленте новостей. Компания хочет, чтобы на главной странице в социальной сети отображались наиболее релевантные истории, и это только первый из многих шагов, которые ожидаются в ближайшие несколько недель.

Facebook: «Согласно вчерашним новостям, мы представили новую Новостную ленту на мобильной и веб-платформах. Мы хотим, чтобы удивить людей, которые используют приложения тем, как их посты отображаются в ленте новостей – делятся ли они таким важным моментом их жизни, как первый марафон, или чем-то менее значимым, таким как книги, которые они сейчас читают».

В действительности Facebook работала с разработчиками приложений, посвященных образу жизни, чтобы адаптировать новые функции и истории в новостных лентах и, таким образом, охватить все случаи повседневного использования. Компания утверждает, что «первичные данные исследований показывают, что среднее количество лайков историй увеличились более чем в два раза» (*Facebook вводит тэги, посвященные образу жизни // Украинский Бизнес Ресурс* (<http://ubr.ua/ukraine-and-world/society/facebook-vvodit-tegi-posviashennye-obrazu-jizni-213432>). – 2013. – 11.03).

Twitter ведет разработку мобильного музыкального приложения, которое позволит воспроизводить музыкальные записи и обмениваться ими на устройствах Apple.

Приложение будет получать музыкальные записи через аудиообменный германский сервис SoundCloud, утверждают источники, близкие к Twitter. Кроме того, в основу приложения лягут разработки ранее купленной Twitter компании We Are Hunted.

Ранее руководство сети неоднократно заявляло, что намерено вывести Twitter из сферы чистого микроблогинга и представить на суд пользователей приложения, которые будут так или иначе дополнять функционал ресурса. Так, в январе этого года Twitter выпустила видеоприложение, позволяющее встраивать короткие ролики в твиты.

Аналитики уверены, что последние медийные инициативы как Twitter, так и Facebook в музыкальной сфере имеют смысл, ведь в противном случае нишу «социальной музыки» займут конкуренты в лице Spotify, Rdio и др. Кроме того, недавно Twitter расширила возможности поиска, чтобы пользователям было проще находить мультимедийный контент.

Сегодня же Twitter выпустила официальное приложение для операционных систем Windows 8 и Windows RT с поддержкой живых иконок на рабочем столе ОС. Согласно сообщению в официальном блоге компании, скачать приложение на 22 языках можно уже сейчас из Windows Store. В компании прогнозируют, что особенно популярным приложение будет для ОС Windows RT, так как пока эта система не слишком избалована социально-ориентированным софтом (*Twitter работает на музыкальном приложении // Media бизнес* (<http://www.mediabusiness.com.ua/content/view/34176/118/lang,ru/>). – 2013. – 14.03).

Разработчики Facebook работают над введением на своих страницах хэштегов, которые активно используются в сервисе микроблогов Twitter. Об этом сообщается на сайте газеты The Wall Street Journal со ссылкой на неназванные источники, знакомые с вопросом.

Благодаря введению хэштегов Facebook сможет быстро индексировать записи, посвященные одной теме, из-за чего пользователи будут больше времени проводить на сайте и увидят больше рекламы, поясняет издание. Когда именно появится нововведение, пока не ясно.

Сервис публикации фотографий Instagram, который Facebook приобрел в 2012 г., уже внедрил систему хэштегов.

Напомним, хэштег – это слово, помеченное знаком # (октоторп), которое используется в Twitter и других родственных сервисах для маркировки сообщений на определенную тему. Американское диалектологическое общество признало «хэштег» главным словом 2012 г. (*Facebook внедряет в записи хэштеги // InternetUA* (<http://internetua.com/Facebook-vnedrit-v-zapisi-heshtegi>). – 2013. – 15.03).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВІЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

В борьбе с неудобными соседями киевляне создают группы в соцсетях, где дают друг другу советы, как «насолить» знакомому, передает newsoboz.org со ссылкой на tsn.ua.

Обитатели скандального дома на Срибнокильской, где жильцам больше года не дает покоя общежитие с гастарбайтерами и бывшими заключенными, создали в Facebook свое сообщество. Здесь они публикуют последние новости о конфликте, обсуждают дальнейшие действия и собирают 26 тыс. грн на ремонт парадного.

«Нам милиция пообещала проверки, но владельцы и постояльцы ночлежки только увереннее стали себя вести. Они нас вообще ни во что не ставят», – сказал житель дома Константин. Кстати, подобный конфликт и на улице Вышгородская, где владелец подвала решил оборудовать сауну и спортзал.

«У нас согласия не спросили, построили крышу и пристройку, которая заслоняет полностью окна на первом этаже. Приходили из мэрии и снесли пристройку, но хозяйка подвала ее вновь отстроили – наверное, заплатили всем чиновникам в районе», – говорят жильцы. Люди страдают от соседей-любителей вокала и бокала, а также тех, кто любит делать ремонты по ночам.

Есть даже «группа для тех, у кого соседи сверху катают железные шарики по паркету». «Я не сплю из-за семьи, которая ночью устраивает оргии: музыка, дикое ржание, лошадиные гонки, прыжки – кто сильнее прыгнет на пол. Милиция даже трубку не берет, а вообще, похоже, у них все схвачено с милицией», – жалуется на форуме киевлянка Ирина.

На форумах люди делятся секретами, как же бороться с соседями. Например, А. Сосницкая решила петь в ответ. «У меня соседка сверху поет постоянно в ванной, где слышимость лучше. Но я не даю ей расслабиться –

тоже люблю петь жутко. Так что мы с ней живем по принципу – кто кого переорет», – пише вона.

В сети также рекомендуют специальные диски со звуками пьяного застолья, скрипучей двери, криков голубей. «Соседи закатывают дискотеки до 3–4-х часов утра?! В милицию жаловаться бесполезно? Установите звук на максимум и спокойно идите гулять или в гости», – сказано в описании к диску.

Еще один способ – спустить пар с помощью компьютера. «Рекомендую игру “Как достать соседа”, представляю перед собой этого с 5-го этажа, бью по клавиатуре – и легче становится», – пише Артем. Ране сообщало, що в последнее время в Украину возвращается мода решать разнообразные проблемы с помощью киллера (*Интернет как инструмент мести соседям // NewsOboz (http://newsoboz.org/obshchestvo/internet-kak-instrument-mesti-sosedyam-04032013110800). – 2013. – 4.03).*

Львівські чиновники – у Facebook.

За останній тиждень у популярній соціальній мережі з'явилися: перший заступник міського голови О. Синютка, начальник управління охорони здоров'я Львівської міської ради В. Зуб та начальник управління капітального будівництва І. Фалюта. А вже міський голова А. Садовий видав розпорядження, згідно з яким усі працівники міськради мають бути зареєстровані у Facebook.

Про це повідомили журналісти телеканалу ZIK.

«Це було прохання мера, щоби ми зареєструвалися. На сьогодні це такий суттєвий комунікативний механізм між людьми. Стосовно мене особисто, то я вже давно був зареєстрований на Facebook і відчуваю ці переваги», – розповів начальник управління «Секретаріат ради» Львівської міської ради Л. Зубач.

Головний медик Львова В. Зуб своєї сторінки не має. Але є сторінка Головного управління охорони здоров'я. Там на головній сторінці зображений В. Зуб. Загалом від такої ідеї він не в захваті.

«Всі соціальні мережі – це приватна територія. Це моя особисто справа спілкуватися з кимось чи не спілкуватися», – зазначив В. Зуб.

Суспільну перевагу в соціальних мережах бачить О. Синютка. «Я думаю, що це буде зручність для людей, які зможуть звернутися. А стосовно особистих речей, то не думаю, що в мене на це вистачатиме часу», – переконаний він (*Львівські чиновники – у Facebook // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/03/04/396782). – 2013. – 4.03).*

Правоохоронці шукатимуть підлітків-утікачів з допомогою соціальних мереж.

Нещодавно на базі тренінгового центру управління боротьби з кіберзлочинністю МВС України відбулися навчальні семінари для працівників територіальних підрозділів управління кримінальної міліції у справах дітей МВС України. Участь у пілотному тренінгу взяли працівники відділень кримінальної міліції у справах дітей районних управлінь столичного Главку міліції.

Темами занять, розглянутих правоохоронцями, стали використання можливостей соціальних мереж у розшуку неповнолітніх, які зникли безвісти, а також встановлення фактичного місцезнаходження користувачів соціальних мереж та VoIP сервісів.

Під час зустрічі представники управління боротьби з кіберзлочинністю обговорили з колегами з підрозділів КМСД питання співпраці, їх потреби у пошуку та фіксації інформації в мережі Інтернет, а також перспективи подальшого співробітництва у сфері протидії кіберзлочинності (*Правоохоронці шукатимуть підлітків-утікачів з допомогою соціальних мереж // Міністерство внутрішніх справ України (http://mvs.gov.ua/mvs/control/main/uk/publish/article/823486;jsessionid=A9E945A6C82BB24FCCE9B07B52C78A9C). – 2013. – 5.03).*

Мэр Одессы А. Костусев будет общаться с горожанами и другими неравнодушными к городу людьми через соцсеть Facebook. Страница мэра появилась в этой соцсети 8 марта.

Правда, сам А. Костусев признался, что аккаунт делал не он – его оформила помощница мэра Н. Мальцева, сообщает «Провокация» со ссылкой на сайт горсовета.

Кстати, Н. Мальцева уже оставила в соцсети ссылку на тему «Ремонт дорог».

Надо полагать, букет цветов на главной странице А. Костусева – лишь элемент отвлечения внимания и временный атрибут. Судя по серьезности темы от Н. Мальцевой и решительности помощницы на этой странице будут обсуждаться совсем не «цветочные» темы (*Одесский мэр посмотрит на горожан через соцсеть // «Провокация» (http://provokator.com.ua/2013/03/08/odesskij-mer-posmotrit-na-gorozhan-cherez-socset-foto/). – 2013. – 8.03).*

Госавтоинспекция завела странички в социальных сетях. Об этом сообщила пресс-служба ГАИ. «Госавтоинспекция Украины информирует об открытии в социальной сети страниц Департамента ГАИ МВД Украины и лично начальника Госавтоинспекции В. Астапковича», – сказано в сообщении.

Ведомство заявило о готовности принимать жалобы, а также предложения от всех участников дорожного движения.

При этом в сообщении не опубликованы ссылки на странички, а также не указывается, в какой именно социальной сети они появились. Примечательно, что в Facebook и Twitter странички ГАИ появились еще в январе, однако пресс-служба сообщила об этом только 7 марта.

Страничка В. Астапковича появилась в Facebook 28 февраля. На момент написания заметки «друзей» у него не было, а комментировать записи было запрещено настройками пользователя.

«Хочу отметить, что главной задачей моей страницы в социальной сети Facebook является прямое общение с гражданами, изучение предложений, касающихся безопасности на дорогах, обеспечения конструктивного диалога между ГАИ и участниками дорожного движения, создание дополнительной возможности оперативного обмена мнениями», – написал 4 марта начальник ГАИ (*ГАИ отчиталась о страничках в соцсетях // Левый берег (http://society.lb.ua/life/2013/03/10/192090_gai_zavela_stranichki_sotssetyah.html). – 2013. – 10.03*).

Twitter обошел традиционные телерадиовещательные средства коммуникации с точки зрения так называемого newsgathering оперативности сбора и распространения новостей. Об этом говорится в докладе о значении современных социальных сетей в журналистике аналитического центра факультета «Медиа и связей с общественностью» Лондонской школы экономики и политических наук (LSE), передает Wallblog.

Принцип Twitter – мгновенная передача коротких сообщений – лидирует и среди других типов социальных сетей. В частности, Facebook намного уступает в оперативности, зато лучше подходит для обсуждения событий.

Авторы доклада при этом отмечают, что социальные сети меняют работу традиционных новостных агентств. От 50 % до 80 % новостей журналисты теперь находят в социальных сетях, тогда как раньше они обращались в информационные агентства. Корреспонденты ведущих телерадиокорпораций признают, что сегодня «невозможно охватить всю историю, если у вас нет Twitter и Facebook».

Кроме того, умение пользоваться социальными сетями становится обязательным условием для успешного поиска работы в журналистике. «Я не беру на работу людей, у которых нет Twitter», – приводятся в отчете слова редактора вечернего выпуска новостей на BBC Д. Карр.

При составлении отчета аналитики из LSE пользовались статистикой BBC, согласно которой, число заходов на сайт телерадиокомпании через социальные СМИ за два года увеличились на 500 %. В конце 2012 г. аккаунт @BBCBreaking получил в Twitter более 4,5 млн фоловеров (читателей). Сейчас это число приблизилось к 5,2 млн (*Twitter обогнал СМИ по скорости*

распространения новостей // InternetUA (<http://internetua.com/twitter-obognal-smi-po-skorosti-rasprostraneniya-novostei>). – 2013. – 10.03).

Количество читателей персональной страницы Ю. Тимошенко в социальной сети Twitter, которую экс-премьер вела лично, превысило 125 тыс. На момент ареста Ю. Тимошенко количество читателей ее твитов составляло 41 тыс.

Как говорится в сообщении редакции сайта Ю. Тимошенко, количество фоловеров продолжает расти, несмотря на то, что 5 августа 2011 г. Ю. Тимошенко сообщила своим интернет-сторонникам об очередном ходатайстве прокуроров о ее аресте.

Редакция Tymoshenko.UA подчеркивает, что на тот момент количество читателей ее твитов составляло 41 тыс., но арест не смог прекратить процесс роста ее личной популярности и популярности ее персональной страницы в Twitter. За время пользования этим ресурсом Ю. Тимошенко написала 501 сообщение.

В то же время редакция напомнила, что Ю. Тимошенко самостоятельно не вела ни одной страницы в Facebook. Многочисленные экаунты поддерживаются или сторонниками лидера «Батькивщины», или информационными службами партии (*Количество сторонников Тимошенко в Twitter превысило 125 тыс. // Главред (<http://glavred.info/politika/kolichestvo-storonnikov-timoshenko-v-twitter-prevysilo-125-tysyach-245088.html>). – 2013. – 9.03).*

Руководитель Чеченской Республики Р. Кадыров подарил квартиры 17 нуждающимся семьям. С просьбой поспособствовать в решении проблем с жильем они написали главе Чечни на его странице на социальном фоторесурсе Instagram.

Р. Кадыров подчеркнул, что обеспечение жильем населения для властей Чечни является одной из главных задач. «Мы делаем особый акцент на жилищную политику. За последние годы тысячи наших жителей стали обладателями квартир и домов. Работа в этом направлении будет продолжена. Я знаю, что вы остро нуждаетесь в жилье. Поэтому с большим удовольствием вручаю вам эти ключи и документы», – отметил он.

Отмечается, что квартиры выделены в новостройках Чеченской Республики: 15 – в Грозном, две – в Гудермесе.

Ранее сообщалось, что стоимость квартиры в Грозном, сходной по размеру с той, что досталась в подарок от Р. Кадырова актеру Ж. Депардьё, может составлять от 3 до 6 млн р. (100–200 тыс. дол.) (*Кадыров подарил 17 квартир через Instagram // Фокус (<http://focus.ua/economy/263930/>). – 2013. – 12.03).*

Ученые использовали Facebook для анализа данных о разрушениях после торнадо.

Если где-нибудь происходит торнадо, то вполне естественно, что видевшие его люди начнут фотографировать и выкладывать в социальные сети фотографии, отображающие последствия стихии. В университете Джорджии исследователи решили воспользоваться этим публичным фотоматериалом для проведения анализа оставленных торнадо разрушений и создания на основе этого исследовательской базы данных. В ход пошли также комментарии пользователей сети Facebook, ставшей источником фотографий и впечатлений очевидцев.

На основе данных из группы «Фотографии и документы, найденные после торнадо 27 апреля 2011 г.» ученые попытались также составить траекторию движения унесенных воронкой предметов из личного имущества пострадавших людей. При этом также использовалось программное обеспечение, показывающее информацию о геоположении объектов, и технологии моделирования траекторий высокого разрешения. При помощи данных систем Facebook и удалось идентифицировать точки подъема в воздух и точки приземления 934 пропавших предметов.

Еще 10 лет назад вряд ли пострадавшие люди после торнадо смогли бы вернуть всё то, что переместилось ветром на неопределенное расстояние. Утерянные вещи направлялись прямиком на свалки или приобретали нового хозяина. Теперь же соцсети и разработки ученых смогут оказать серьезную помощь в воссоединении пропавших из домов или дворов объектов с их хозяевами. Используя тестируемую методику, можно найти даже унесенную за несколько сотен километров дорогу сердцу семейную фотографию.

С научной точки зрения у проведенного исследования также имеется ряд полезных выводов, касающихся устройства и внутренних законов социальных сетей. Также удалось выяснить, что самая далекая траектория, по которой проследовал подхваченный ветром объект, составила 353 км, что превышает самую длинную зафиксированную ранее траекторию полета обломков после торнадо.

Еще ученые обнаружили, что у объектов, отнесенных на далёкие расстояния, траектория сильно изменяется и зависит от присутствующего направления ветров. Поэтому в итоге поднятые воронкой вещи находят в достаточно неожиданных местах, как правило, правее пути, по которому шел торнадо. Эти результаты можно будет в дальнейшем применять в отслеживании траектории движения токсических или радиоактивных веществ, попавших на путь торнадо, и заранее среагировать для предотвращения отравления людей и организовать эвакуацию (***Ученые использовали Facebook для анализа данные о разрушениях после торнадо // Око планеты (<http://oko-planet.su/science/sciencediscussions/171133-uchenye-ispolzovali-facebook-dlya-analiza-dannye-o-razrusheniyah-posle-tornado.html>). – 2013. – 11.03).***

По информации японского информагентства Kyodo News, местные власти вскоре планируют развернуть систему оповещения о чрезвычайных ситуациях через социальную сеть Twitter и другие популярные в Японии сервисы микроблогов. По данным Kyodo News, японское Агентство по чрезвычайным ситуациям начнет тестировать систему Twitter-оповещения этим летом, сообщает cybersecurity.ru

По словам представителей ведомства, новая система должна помочь в тех ситуациях, когда в случаях пожаров или землетрясений повреждаются сотовые вышки и многие жители не могут воспользоваться сотовой связью даже для совершения вызова в службу спасения по экстренному номеру 119. Кроме того, новая система позволит расширить охват распространения предупреждений и предотвратить перегрузки сотовых сетей экстренными предупреждениями *(Япония будет рассылать предупреждения о катастрофах через Twitter // IT Expert (http://itexpert.in.ua/rubrikator/item/23844-yaponiya-budet-rassilat-preduprezhdeniya-o-chs-posredstvom-twitter.html). – 2013. – 13.03).*

Державтоінспекція Вінниччини завела сторінки в соціальній мережі та готова приймати скарги і пропозиції від усіх учасників дорожнього руху.

Про це повідомляє служба профілактичної роботи управління ДАІ УМВС у Вінницькій області.

У соцмережі Facebook уже відкрита сторінка управління ДАІ і особисто начальника Державтоінспекції Вінниччини П. Солоненка. Створення цих сторінок покликані сприяти кращому інформуванню громадян про діяльність ДАІ і спілкуванню з усіма учасниками дорожнього руху.

На сторінці управління ДАІ користувачі всесвітньої мережі зможуть ознайомитися з новинами, дізнатися всі зміни законодавства, які стосуються дорожнього руху і інших нововведень в цій галузі. Також користувачі зможуть залишати свої зауваження і побажання по роботі ДАІ прямо на сторінці начальника цього відомства. Всі повідомлення автомобілістів і пішоходів не залишаться без уваги *(Солоненко відправив вінницьких ДАІ-шників в Facebook // Винниця.info (http://www.vinnitsa.info/news/solonenko-vidpraviv-vinnitskih-dai-shnikov-v-facebook.html). – 2013. – 13.03).*

Как только стало известно об избрании Папы Римского, социальные сети заполнили радостные комментарии. По данным Twitter, за 13 марта – день избрания понтифика – было написано более 7 млн сообщений на эту тему. Сразу после объявления имени нового Папы об этом появлялись 130 тыс. твитов в минуту, передает РИА Новости.

Хэштег #HabemusPapam («У нас есть Папа», традиционная заключительная фраза на выборах понтифика) за день превратился в один из самых популярных и комментируемых в сети.

Следующими по популярности хэштегами стали словосочетания #HumoBlanco и #FumataBlanca («белый дым», извещающий об избрании Папы).

При этом официальный микроблог Папы, созданный еще при предшественнике Хорхе Марио Бергольо и заблокированный после решения Бенедикта XVI оставить папский трон в конце февраля, вновь ожил сразу после избрания нового главы римско-католической церкви.

«Теперь у нас папа Франциск», – говорилось в сообщении, набравшем более 76 тыс. ретвиттов за несколько часов (*Новость о новом Папе взорвала социальные сети // InternetUA (<http://internetua.com/novost-o-novom-pape-vzorvala-socialnie-seti>). – 2013. – 14.03*).

У Facebook пропонуєть асоціюватися з ЄС

Понад 800 підписів, майже 1400 лайків і 350 перепостів уже набрав у Facebook флеш-моб, організований відомим українським блогером Р. Шрайком і політологом, громадським діячем Д. Потехніним. Учасникам акції пропонуєть асоціюватися з ЄС в індивідуальному порядку.

На сторінці Р. Шрайка, зокрема, зазначається:

«флеш-моб!

пропонується асоціюватися з ЄС в індивідуальному порядку))

1) ставте лайк фото.

2) пишіть у коментах свій “підпис”.

Dmytro Potekhin обіцяє відвезти підписний лист у Брюссель))»

У заві ж щодо асоціації з ЄС зазначається: «прошу асоціювати мене з ЄС» і «прошу не асоціювати мене із режимом Януковича» (*У Facebook пропонуєть асоціюватися з ЄС // Новий погляд (<http://www.pohlyad.com/news/n/11463>). – 2013. – 15.03*).

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Что рекламодатели думают о Facebook (исследование AdAge)

В июньском исследовании абсолютное большинство опрошенных маркетологов (85 %) сообщили о том, что чувствуют необходимость своего присутствия в Facebook. Только около половины респондентов заявили, что ощущают необходимость в использовании рекламы в этой соцсети. В начале 2013 г. AdAge провели новое исследование по этой же теме.

Выборка состояла из 701 маркетолога и медиа-руководителя, выяснив их взгляды. Процент тех, кто использует рекламу в Facebook, увеличился – 61 % (против 55 % семью месяцами ранее). Кроме того, выяснилось, что

процент тех, чей рекламный бюджет «умеренно» или «значительно» вырастет, также немного увеличился (58 % против 56 % в ходе прошлого опроса).

В этот раз AdAge задавал конкретные вопросы о продуктах, которые семь месяцев назад только зарождались или вообще еще отсутствовали в природе. Выяснилось, что степень проникновения сервисов sponsored stories и Facebook Ad Exchange очень низка – большинство маркетологов до сих пор даже не пробовали их использовать. Как и предполагалось, умами маркетологов владеет мобильная реклама Facebook: 69 % из них говорят, что мобильная реклама имеет некоторое или очень высокое значение в сравнении с 63 % семью месяцами ранее (*Что рекламодатели думают о Facebook (исследование AdAge) // Marketing Media Review (<http://mmr.ua/news/id/chto-reklamodateli-dumajut-o-facebook-issledovanie-adage-33823/>). – 2013. – 4.03).*

Социальная сеть Facebook начала показывать меньше бесплатных постов в новостной ленте пользователей. По наблюдениям редактора The New York Times Н. Билтона, компания экспериментирует с алгоритмом, который отдает предпочтение проплаченным объявлениям, показывая их выше, а бесплатные посты скрывает или сдвигает вниз.

Журналист напомнил, что в конце 2011 г., когда Facebook разрешила фоловить других юзеров (то есть подписываться на обновления ленты новостей), число его подписчиков быстро возросло до 25 тыс. человек. Сообщения Н. Билтона получали большой отклик. К примеру, его новогодний материал про то, чтобы уделять гаджетам меньше времени, собрал 535 лайков и 53 репоста.

С тех пор количество фоловеров редактора увеличилось до 400 тыс., однако цифры, отражающие взаимодействие с аудиторией, пошли вниз. «Четыре колонки, которыми я поделился в январе, получили в среднем 30 лайков и два репоста, – пишет сейчас Н. Билтон. – Картинки год назад могли собрать под тысячу лайков, а теперь – всего лишь около ста. Я посмотрел на ленты других техноблогеров, включая Э. Сиглера из TechCrunch и репортеров The New York Times, и у них произошел такой же спад».

Затем Н. Билтон заплатил соцсети 7 дол. за спонсорское продвижение его колонки подписчикам. Как показал эксперимент, ссылку увидело намного больше людей: пост получил 130 лайков и 30 репостов всего за несколько часов. «Кажется, что Facebook не только продвигает мои ссылки в новостных лентах, когда я за них плачу, но и игнорирует те, которые я публикую без оплаты», – заключил журналист.

Н. Билтон обратился за разъяснением к Facebook, где ему подтвердили, что компания замещает бесплатный контент платным. «Это действительно не в наших интересах убрать самый интересный материал и заменить его рекламой. Мы хотим убедиться, что показываем нужный контент нужным людям», – сказали сотрудники соцсети.

Алгоритм, решающий, что видят пользователи, может быть правильным для Facebook, которая ищет новые источники прибыли. Однако такой подход может нанести ущерб взаимодействию брендов с потребителем, которые стараются держать клиентов в курсе новостей. Компаниям теперь потребуется тратить деньги не только на то, чтобы набрать подписчиков, но и платить, чтобы их новости показывались в лентах.

Похожей рекламной модели, «спонсорским твитам», придерживается и Twitter. Однако, в противоположность Facebook, в микроблогах показывается весь контент из всех источников, на которые подписан пользователь, в том числе и рекламный (*В ленте новостей Facebook стало больше рекламы // InternetUA (<http://internetua.com/v-lente-novostei-Facebook-stalo-bolshe-reklami>). – 2013. – 5.03).*

Facebook offers: почему соцсеть проигрывает купонным сервисам

В минувшем году Facebook попыталась сыграть в бизнес «горячих предложений» и запустила одноименный сервис Offers («предложения»). Старт был весьма заметный, и соцсети предрекали определенные преимущества перед специализированными купонными сайтами. Время показало, что функционал «предложений» в данном виде не способен составить им конкуренцию.

Суть Offers в том, что пользователи соцсети могут воспользоваться скидками от компаний, разместивших рекламу на сайте. С одной стороны, логика рекламодателей понятна: у Facebook огромная аудитория, следовательно, предложение достигнет большого количества пользователей. Действительно, сервис поначалу вызвал большой интерес и желание экспериментировать. Однако в дальнейшем поведение некоторых клиентов Facebook просигнализировало рынку об изменившихся приоритетах. К примеру, за минувший год такие гиганты, как Gap, J.C. Penney, Nordstrom и GameStop, сначала разместили, а потом отозвали свои предложения из соцсети.

Почему Offers не смог составить конкуренцию купонным сервисам? Во-первых, масштабность, которая на первый взгляд кажется преимуществом, на деле способна обернуться определенными проблемами. Offer – это предложение (купон), которое предлагается огромному числу пользователей, следовательно, возникает ситуация, при которой компания не имеет возможности контролировать количество полученных купонов. Что, если оно превысит ресурсы рекламодателя? Вместо удачной маркетинговой акции мы получаем недовольных клиентов, кризис на производстве и т. д. Адресное предложение, напротив, четко выверяет аудиторию, ее объем и характеристики. Можно заранее спрогнозировать и просчитать максимальное количество купонов, которое целесообразно предложить к реализации так, чтобы это было оптимально выгодно самому бизнесу.

Есть еще один важный момент: безопасность. В любой из наших акций, дабы избежать мошенничества, важным условием является наличие уникального кода купона. Offers не предоставляет такую возможность, присваивая всем воспользовавшимся предложением единый номер.

Уникальный код – необходимый инструмент защиты от мошенничества. Его наличие гарантирует, что конкретный пользователь действительно оплатил конкретный купон. Код, во-первых, присутствует в распечатке самого купона, во-вторых, на платежном чеке, в-третьих, приходит в качестве подтверждения пользователю на мобильный. Представитель компании может сверить уникальный код клиента со списком кодов проданных купонов по акции в своем личном кабинете на купонном сайте.

Так это работает с уникальными кодами. Можно только представить себе, какое пространство для мошенничества порождает система, когда все купоны имеют один и тот же код. Что теоретически мешает множеству пользователей их подделывать, множить и копировать? Разве что лень (*Facebook offers: почему соцсеть проигрывает купонным сервисам // InternetUA (<http://internetua.com/Facebook-offers--pocsemu-socset-proigrivaet-kuponnim-servisam>). – 2013. – 5.03*).

Перевести «Яндекс.Деньги» можно через Twitter

Сотрудники электронной платежной системы «Яндекс.Деньги» запустили экспериментальный проект Twym, который позволяет переводить деньги от одного пользователя другому при помощи сообщения в сервисе микроблогов Twitter.

Как пишет Прайм, для обмена деньгами с помощью Twitter-сообщений у получателя и отправителя должны быть счета в «Яндекс.Деньгах», которые при помощи Twym необходимо связать с соответствующими Twitter-аккаунтами.

Для перевода средств нужно отправить сообщение, содержащее имя получателя в Twitter, сумму и хештег #twym. В дальнейшем деньги с кошелька можно вывести на банковскую карту или получить наличными.

Как утверждают в «Яндекс.Деньгах», проект Twym создавался по инициативе сотрудников компании. При этом авторы проекта использовали стандартные, открытые всем инструменты для разработчиков Twitter и «Яндекс.Денег».

Зарубежные компании уже используют механизм перевода денежных средств при помощи сообщений в Twitter. Такой проект совместно с Twitter уже анонсировала American Express, аналогичный механизм использует и сервис Twitpay (*Перевести Яндекс.Деньги можно через Twitter // IT Expert (<http://itexpert.in.ua/rubrikator/item/23548-perevesti-yandeksdengi-mozhno-chez-twitter.html>). – 2013. – 6.03*).

Сторонним клиентам Twitter приходит конец

Несколько дней назад представители Twitter официально объявили о прекращении поддержки клиента Tweetdeck, которым компания владела в течение последних двух лет. Официальную смерть Tweetdeck констатируют в мае, когда приложение будет удалено из App Store и Google Play. Веб-версия клиента продолжит функционировать. Произошедшее с Tweetdeck вновь напомнило о печальном положении дел в стане сторонних клиентов Twitter.

В прошлом году Twitter опубликовал новые правила работы альтернативных клиентов сервиса. Главное изменение заключалось в ограничении пользовательской базы приложений до 100 тыс. пользователей. Когда порог достигнут, новые пользователи не могут получить доступ к Twitter. Если разработчики хотят увеличить лимит, им нужно связаться с представителями Twitter и решать этот вопрос в особом порядке.

Проблема в том, что не все разработчики альтернативных клиентов получают право на расширение лимита и могут себе это позволить. Виной тому пиратство. В большинстве случаев приложение набирает 100 тыс. пользователей, из которых только 50 % действительно заплатило за него. В итоге, новые покупатели не могут получить стабильный доступ к Twitter, а разработчик не досчитывается прибыли.

Так, например, случилось с клиентом Carbon для Android. Его разработчик объявил о прекращении разработки и поддержки приложения из-за проблем с пиратством и лимитом на пользователей.

Схожие проблемы наблюдаются и у приложения Falcon Pro – только 40 тыс. пользователей заплатили за него. При этом установленный Twitter лимит давно достигнут. Разработчик даже открыл сбор подписей на увеличение пользовательской базы, но достучаться до представителей Twitter таким образом ему вряд ли удастся.

Клиент Tweetro для Windows 8 тоже пал жертвой новых правил – за несколько дней он набрал максимальную базу пользователей, что вынудило разработчиков удалить приложение и выпустить вместо него платную версию, ограничив тем самым спрос.

Таким образом, политика Twitter по борьбе со сторонними клиентами приносит свои плоды – их количество уменьшается с каждым днем. У официального клиента перед ними есть огромное преимущество – разработчики никогда не объявят о прекращении его поддержки и не перекроют доступ к сервису. Жаль только, что о свободе выбора и богатстве функций пользователям скоро придется забыть (***Сторонним клиентам Twitter приходит конец // InternetUA (<http://internetua.com/storonnim-klientam-Twitter-prihodit-konec>). – 2013. – 10.03***).

Что даёт новая «Хроника» Facebook рекламодателям?

Facebook анонсировал новый вид «Хроники» пользователя. За изменениями в интерфейсе социальной сети внимательно следят не только пользователи, но и рекламодатели. Facebook давал много поводов для волнения (и приятного, и не очень) рекламодателей в последнее время. Что же даёт новая новостная лента Facebook маркетологам, проанализировал техноблог Mashable.

В первую очередь, самая большая радость для брендов – это расширение «рабочей поверхности» новостной ленты. Больше места – более крупная реклама. Об этом давно просили Facebook рекламодатели и агентства. Об увеличении пространства как о преимуществе для рекламодателей говорит аналитик eMarketer Д. Вильямсон. Представитель Facebook подтвердил, что спонсорские сообщения (Sponsored Posts) будут появляться в новой ленте, так же как и в текущей версии, только крупнее.

Facebook выделяет фотографии и видеоролики в отдельные новостные ленты. Несмотря на то что о видеорекламе на презентации Facebook не упоминалось, Д. Вильямсон уверена, что возможность показа видео у брендов будет. М. Цукерберг ранее упоминал, что в новой ленте новостей будет больше видеороликов.

Решение о приведении к единой форме новостной ленты на десктопах и мобильных устройствах также положительно воспринимается рекламодателями. Это упрощает реализацию единой рекламной кампании, в то время как ранее контент необходимо было проверять на различных устройствах.

Тем не менее, когда речь идет о разделении новостной ленты на отдельные категории, у маркетологов появляется повод для огорчения. Если в общей новостной ленте реклама могла быть размещена наряду с сообщениями друзей, то теперь у пользователя есть возможность просматривать, например, категорию «Ближних друзей», в которой рекламные объявления, если и появятся, то будут выглядеть «белой вороной». Пользователь сможет более целенаправленно просматривать информацию о брендах, за которыми он следит (в ленте Following), но это не будут его друзья. О возможном увеличении числа пользователей, которые будут читать лишь ленту близких друзей и не видеть рекламу, говорит как об угрозе С. Мэнселл, CEO агентства TBG Digital.

С другой стороны, выделенные категории новостной ленты могут дать рекламодателям возможность продвигать бренды для более таргетированной аудитории. Например, Sony может размещать свою рекламу только в категориях «Музыка» и «Игры», что даст ей намного более активное участие пользователей в кампании.

Старший специалист по социальной стратегии компании Rokkan М. Агуайо считает, что пользователь, получающий больший контроль над тем, что он видит в ленте, будет больше увлекаться интересными ему

продуктами и брендами. М. Агуайо предполагает, что Facebook в дальнейшем будет предлагать рекламодателям размещать рекламные сообщения за пределами ленты Following, но за дополнительную плату (*Что даёт новая «Хроника» Facebook рекламодателям? // InternetUA (<http://internetua.com/cto-da-t-novaya--hronika--Facebook-reklamodatelayam>). – 2013. – 10.03*).

Социальная сеть Facebook получила патент под названием PaidProfilePersonalization. В нем описывается возможность введения платы, которая освободит пользователя от рекламы на сайте социальной сети и позволит самостоятельно изменять дизайн страницы. Об этом сообщают «Вести».

Facebook подала заявку на патент PaidProfilePersonalization еще в середине 2011 г., однако получила этот патент только в январе этого года.

Пользователь сможет выбрать один или несколько объектов социальной сети, чтобы заменить рекламу или другие элементы, которые обычно отображаются посетителям страницы профиля пользователя и которые контролирует система социальной сети. В конкретных случаях пользователь сможет редактировать элементы на странице своего профиля, управлять дизайном и содержимым системы социальной сети.

В качестве авторов патента указаны создатель соцсети М. Цукерберг, а также директор по рекламным объявлениям Г. Раджарам, а также бывший директор по управлению продуктами П. Фулориа.

В патенте не указывается Facebook как конкретное место применения патента – текст говорит лишь об абстрактном функционале некоего ресурса социальной сети, но эскизы дают ясно понять, что однажды патент превратится в еще одну стратегию по монетизации ресурса.

Напомним, что Facebook была яростным противником какой-либо кастомизации своих страниц. Когда она только запустилась, в сети господствовал другой социальный ресурс – MySpace, где пользователи могли сами бесплатно настраивать почти все элементы дизайна по своему вкусу. Свобода дорого стоила: на профили многих пользователей сложно было взглянуть без боли в глазах. Facebook же, наоборот, жестко контролировала унифицированный по всему сайту дизайн.

Теперь компания, похоже, решила чуть ослабить контроль. Один из примеров, описанных в патенте, говорит о том, что платным пользователям доступно замещение рекламных блоков справа от «Хроники» на фото любимой машины или любой другой контент (*Facebook введет платные аккаунты // IT Expert (<http://itexpert.in.ua/rubrikator/item/23858-facebook-vvedet-platnie-akkaunti.html>). – 2013. – 13.03*).

У Швейцарії запроваджують надкомпактний міський транспорт із викликом через соцмережі. Міська мобільність коштуватиме недешево.

Швейцарцям пропонують їздити на роботу на персональних міні-автобусах. Нова розробка розрахована на чотирьох пасажирів, ідеться в сюжеті ТСН.

Новинка зможе проїхати там, де не розміститься звичайний автобус. Транспорт розрахований на тих, кому по дорозі – автобус підбиратиме попутників через замовлення в соціальних мережах.

Комп'ютер, яким оснащений диво-транспорт, прокладатиме зручний для всіх маршрут, а пасажери зможуть згаяти час за чашечкою кави.

Поїздки на персональному автобусі коштуватимуть недешево, адже його вартість становить приблизно 10 тис. дол. ***(У Швейцарії запроваджують надкомпактний міський транспорт із викликом через соцмережі // ТСН (<http://tsn.ua/tsikavinki/u-shveycariyi-zaprovadzhuut-nadkompaktniy-miskiy-transport-iz-viklikom-cherez-socmerezhi-285568.html>). – 2013. – 12.03).***

Блоги більше впливають на поведінку споживачів, ніж Facebook.

Блоги – третє за впливовістю цифрове джерело, яке впливає на поведінку споживачів. На першому місці інтернет-магазини, на другому – сайти брендів. Після блогів за впливовістю Facebook, групи/форуми, YouTube, LinkedIn та ін.

Споживачі вважають огляди у блогах більш відвертими щодо товарів, послуг і брендів, більше їм довіряють. Часто споживачі читають відгуки у блогах перед тим, як прийняти рішення про покупку.

Цікаво, що бренди виділяють близько 10 % рекламних бюджетів на соціальні медіа, але 57 % із них витрачаються на Facebook. За рекламними бюджетами блоги аж на четвертому місці після Facebook, YouTube та Twitter.

Крім того, 54 % споживачів вважають (12 % споживачів не погоджуються з цим твердженням), що менші спільноти є більш впливовими.

Відповідно, автори рекомендують сфокусуватися на цінностях і розбудові сильних взаємозв'язків у середині спільноти, а також пропонувати якісний контент – замість того щоб ганятися за кількістю ***(Блоги більше впливають на поведінку споживачів ніж Facebook // UkrainianWatcher (<http://watcher.com.ua/2013/03/11/blohy-bilshe-vplyvayut-na-povedinku-spozhyvachiv-nizh-facebook/>). – 2013. – 11.03).***

Социальная сеть LinkedIn покупает производителя новостного приложения Pulse и все принадлежащие ему активы и разработки за сумму примерно в 100 млн дол., сообщает интернет-издание AllThingsD. По

неофициальным данным, LinkedIn приобрела компанию Alphonso Labs за 50–100 млн дол., – пишет cybersecurity.ru.

Официальных уведомлений о сделке пока ни одна из сторон не делала.

Приложение Pulse представляет собой визуальный новостной агрегатор, поддерживающий работу на ПК, мобильных устройствах и планшетах. Версии Pulse есть под Android и iOS. При помощи такого актива, как Pulse, соцсеть LinkedIn может значительно расширить собственные мобильные продукты и технологии, а также получить в свой штат группу инженеров, специализирующихся на мобильном программном обеспечении (*Социальная сеть LinkedIn покупает Alphonso Labs // Media бизнес (<http://www.mediabusiness.com.ua/content/view/34151/118/lang,ru/>). – 2013. – 12.03).*

Насколько важно общение в режиме реального времени с вашими потребителями в соцсетях?

Реакция в режиме реального времени – один из отличительных моментов использования социальных сетей для коммуникации. Вы пишете сообщение другу, отправляете фотоснимок коллеге, лайкаете пост знакомого или подписываетесь на участие в профильном мероприятии – и все это «здесь и сейчас». Соцсети приучили потребителя к тому, что не только коллеги, друзья и знакомые должны реагировать чуть ли не мгновенно, едва получив уведомление, но и бренды должны вести себя аналогично. Насколько важна коммуникация в режиме реального времени для бизнеса? Подходит ли она всем сферам деятельности или только определенным?

Согласно отчету от Oracle, только 30 % потребителей ожидают реакции от представителей компании в течение 30 мин. в микроблогах Twitter. И хотя это – вполне значительное количество людей, но вовсе не большинство потребителей. «Реакция в реальном времени» не означает, что надо бросить все силы техподдержки, маркетологов и отдела продаж на социальные сети, забыв об оффлайн-коммуникации и оказании услуг для клиентов по остальным каналам продаж.

Безусловно, реакция в режиме real-time играет важную роль в современной потребительской модели, но нельзя не отметить тот факт, что постоянное нагнетание «важности» привело к несколько неадекватному восприятию проблемы. Если запрос о поломке контрактного оборудования или проблемах с доступом к интернет-банкингу – это вопрос срочный и важный, то многие вопросы, которые задают клиенты, не настолько срочные. Компании должны сами для себя определить круг первоочередных проблем для реагирования, потому что наличие ПО для мониторинга не сделает вас автоматически клиентоориентированным и внимательным бизнесом. Вы просто получите в руки инструмент для мгновенного реагирования на запросы покупателей; а вот как применять этот инструмент, зависит целиком от вас.

Учтите также, что между твитом или комментарием покупателя и ответом на него все равно проходит какое-то время; лучше, чтобы этот промежуток был как можно короче, но это только в тех случаях, когда решение можно предоставить точно также быстро, как это происходит при обращении через оффлайн-канал коммуникации с компанией.

Самый простой способ успокоить клиента – это заранее сообщить ему, сколько времени занимает ответ на запрос через соцсети. Если вы с самого начала открыто говорите клиенту, что на его вопрос в соцсети он получит гарантированный ответ через определенное количество минут или часов, то не будет возникать ненужная паника ни среди клиентов, ни среди ваших сотрудников (что обычно бывает, когда компания взваливает на себя обязанность отвечать всем и каждому едва ли не через секунду или вообще месяцами не отвечает на твиты с вопросами, и клиенту остается только гадать, сколько обычно уходит у компании времени на подготовку ответа).

Важно также знать профиль вашего покупателя: кто эти люди, как интенсивно они используют коммуникации в соцмедиа, на что они готовы и т. д. В этом случае хорошим примером может послужить история коммуникации Dell и создание компанией своей линии сервис-поддержки в Twitter.

Все больше и больше брендов признает тот факт, что клиенты активно делятся в Интернете не только положительными, но и негативными отзывами. Причем большинство таких отзывов попадает на страницы брендов в социальных сетях, а также идет от личных профилей и циркулирует в личных блогах.

Помимо адекватного времени реагирования и точного определения портрета вашего потребителя, нужно не забывать, что иногда подробный ответ на вопрос, совет и решение проблемы клиента занимает больше, чем 140 символов в твите или короткое разъяснение в пару-тройку предложений на странице в Facebook. Именно в таких случаях стоит предложить потребителю дополнительный канал коммуникации, запросить телефон или иные контактные данные для дальнейшего решения проблемы уже за пределами сети.

Подводя итог, можно сказать, что реагирование в режиме реального времени важно, но степень его важности и механизм реализации такого общения на практике зависит сугубо от приоритетов компании и задач, которые компания ставят перед собой. Покупатели голосуют «за» своими сообщениями, лайками, твитами и кошельком. Перед вами стоит задача масштабировать этот новый стиль коммуникации в рамках работы вашего департамента маркетинговой, информационной и технической поддержки ваших клиентов (*Насколько важно общение в режиме реального времени с вашими потребителями в соцсетях? // Marketing Media Review (<http://mmr.ua/news/id/naskolko-vazhno-obschenie-v-rezhime-realnogo-vremeni-s-vashimi-potrebiteljami-v-socsetjah-33912/>). – 2013. – 12.03*).

Р. Скотт сделает сериал для Youtube, Facebook и Twitter.

Как пишет The Next Web, создатель «Чужого», «Прометей», «Бегущего по лезвию бритвы» режиссёр Р. Скотт объединяет усилия с одним из топовых каналов YouTube Machinima для создания 12 коротких фантастических фильмов.

Фильмы будут распространяться на платформе Machinima, а так же в Facebook и Twitter. Ну и чтобы было понятно, почему именно Machinima, несколько фактов:

- ежемесячная аудитория канала – 260 млн человек;
- количество просмотров роликов в месяц – 2,6 млрд;
- основная аудитория – молодые мужчины (они как раз являются самой отзывчивой аудиторией для научной фантастики).

Дата запуска сериала в производство пока не называется (***Ридли Скотт сделает сериал для Youtube, Facebook и Twitter // Media бізнес (http://www.mediabusiness.com.ua/content/view/34147/118/lang,ru/). – 2013. – 12.03).***

Продвижение в социальных сетях – мощный инструмент по привлечению трафика

Ежедневно миллионы пользователей Интернета, или даже десятки миллионов, проводят свое свободное время в социальных сетях. И можно представить себе, сколько людей из этого числа могут оказаться вашими клиентами. Этот большой рост популярности Facebook, «ВКонтакте», Twitter и Instagram породил новый способ продвижения сайтов – продвижение сайтов в социальных сетях.

Смысл раскрутки сайта в социальных сетях состоит в том, что вы размещаете свою рекламу на страничке в социальной сети и человек, который заинтересован данной рекламой, перейдет по ссылке. Большой плюс в том, что заинтересованных людей может оказаться большое количество, так как в социальных сетях в режиме онлайн одновременно находятся огромное количество человек.

Социальные сети могут быть разные. Так, например, занявшись раскруткой в Instagram, можно привлечь людей, заинтересованных фотографией и всякого рода технологичными гаджетами, т. е. потенциальных клиентов в конкретной целевой аудитории. Более того, посетители вашей странички будут не просто случайные люди, а те, кому интересна ваша информация или ваш предлагаемый товар. Посетитель может даже оказаться постоянным читателем или покупателем.

Разместив рекламу страницы в социальных сетях или даже купив фоловеров, есть большой шанс получить огромный трафик, что естественно положительно скажется на вашем сайте. Конечно, нужно стараться

периодически обновлять контент, чтобы он был уникален и интересен, дабы посетители не заскучали и познакомились с какими-либо новинками.

Если информация на вашей страничке полезна и информативна, уникальна и интересна, то пользователи социальных сетей, зашедшие на ваш сайт, могут поделиться ссылкой с друзьями, тем самым, не зная того, они будут выполнять за вас какую-то часть вашей работы. А это популярность и рост трафика, поэтому немаловажно ориентироваться на пользователей определенной социальной сети, которые больше склонны к контенту определенной тематики.

Если вы этого добились, то вы получите желаемый трафик и целевую аудиторию, которая будет постепенно расти. SEO-ссылки начинают переживать себя, и способ продвижения сайта в социальных сетях начинает набирать обороты в своем развитии и становится более актуальным. Поэтому самый быстрый и оптимальный вариант раскрутки вашего сайта – это продвижение в социальных сетях. Но результат, естественно, зависит только от вас, от уникальности и интересности вашего контента на сайте (*Продвижение в социальных сетях – мощный инструмент по привлечению трафика // Reklamaster (http://reklamaster.com/news/id/40100/index.html). – 2013. – 11.03).*

В США установили правила для оплаченных твитов.

Федеральная комиссия по торговле США приняла новый свод рекомендаций для размещения онлайн-рекламы. В нем, в частности, конкретизируются требования к платным объявлениям в микроблогах Twitter и других социальных сетях.

Так, комиссия требует в случае размещения таких объявлений четко и очевидно показывать, что они являются рекламными. В примере, который показывается государственным органом, популярная в Twitter блогерша использует хэштег #spon (sponsored). Однако в правилах отмечается, что для многих других блогеров, особенно новичков сервиса, этот значок может не говорить ничего, поэтому рекомендуется ставить более ясный хэштег – например #ad (реклама).

Как отмечает The Wall Street Journal, неясно, каким образом регулятор будет проводить эту политику в жизнь. Как вариант, преследоваться будут только наиболее крупные нарушители, тогда как тысячи мелких нарушений будут игнорироваться.

Комиссия не заводит уголовных дел, так что нарушители будут попадать под положения гражданского права. Это означает, что им могут грозить штрафы, но не тюремное заключение.

Последний раз правила соблюдения прав потребителей в Интернете публиковались комиссией в 2000 г. С тех пор в сети появилось и развилось множество новых форматов, включая социальные сети и блоги, с чем и связаны изменения (***В США установили правила для оплаченных***

твитов //InternetUA (<http://internetua.com/v-ssha-ustanovili-pravila-dlya-proplacsennih-tvitov>). – 2013. – 13.03).

Треть ведущих брендов через Twitter взаимодействуют с клиентами.

Twitter становится популярным инструментом для маркетинговых коммуникаций с клиентами.

Из числа компаний, которые входят в международный рейтинг брендов Interbrand Top-100, почти каждая третья компания создала отдельный от основного аккаунт в сервисе микроблогов Twitter, специально для поддержания взаимодействия со своими клиентами. Об этом говорится в исследовании компании Simply Measured.

Исследователи выяснили, что крупнейшие мировые бренды признают в качестве популярной платформы для организации взаимодействия с клиентами не только Facebook, но и активно используют возможности Twitter.

Каждый из этих 30-ти брендов получил в среднем только за последний квартал свыше 198 тыс. твитов от пользователей и отправил почти 83 тыс. ответных твитов.

Создание отдельных от основного аккаунтов исследователи объяснили нежеланием компаний выносить негатив в главный профиль компании, что вполне естественно.

Наилучшую работу сервиса поддержки в Twitter продемонстрировали Ford и Nike: оба бренда ответили более чем на 70 % упоминаний в сервисе. Тем не менее, только 10 % аккаунтов, созданных для пользовательской поддержки, откликнулись на обращения на протяжении часа от их поступления (*Треть ведущих брендов через Twitter взаимодействуют с клиентами // InternetUA (<http://internetua.com/tret-vedusxih-brendov-cserez-Twitter-vzaimodeistvuuat-s-klientami>). – 2013. – 15.03).*

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Социальные сети: опасность мнимая или реальная?

Социальные сети, образно говоря, построены образу и подобию нервной системы. Нейроны здесь сплетаются, ветвятся, по ним, словно искры пробегают электрические импульсы. И в социальных сетях каждый человек воспринимается как очередной источник импульса для общих мнений и новых связей, пишет obozrevatel.com.

По большому счету, едва ли не все цифровые современные технологии ориентированы на сближение людей, на то, чтобы упростить общение, ускорить реакции. Как ни парадоксально, при этом сетевую реальность готовы обвинить в противоположном. И это не слишком справедливо?

Могут ли социальные сети вызывать зависимость?

В средствах массовой информации пишут истории о том, как люди готовы сидеть в сети сутками. Они забывают о домочадцах, сне, еде, личной гигиене. Некоторые даже попадают в психиатрическую клинику, ведь их гениальный пост никто так и не залайкал. Не в социальных сетях стоит искать причины появления этих проблем.

В мировой практике известно множество подобных случаев. Если рассмотреть их пристально, наверняка выяснится, что тот или иной человек на самом деле страдал глубинными психическими расстройствами, и это никак не связано с социальной сетью. С возникновением цифровых форм общения данные статистики подобных тяжелых расстройств почти не изменились.

Опасна ли информационная зависимость?

Информационная зависимость, сама по себе, как и масса иных форм зависимости, на самом деле существует. Но когда не случаются отягчающие обстоятельства, такая зависимость не носит фатальный характер. Она не способна вызвать ломку, как, к примеру, наркомания. От нее вряд ли будет выворачивать суставы и сводить мышцы. Данная форма зависимости находится полностью в эмоциональной и волевой сфере, следовательно, носит обратимый характер, причем, без негативных последствий, она не провоцирует распад личности.

Почему появляется информационная зависимость?

Есть мнение, что какая-либо форма зависимости – от социальных сетей, игр, чего-то другого, развивается, когда на это имеются генетические предпосылки. Проявляется это в формировании противоестественного азарта. Родители зачастую этому не придают значения, наивно полагают, что ребенок сможет сам сориентироваться в виртуальной реальности и найти дорогу домой.

Между тем, специалисты уверяют: даже самого увлекающегося и азартного ребенка можно попытаться удержать от погружения в сеть. Для этого нужно немного – живое общение и интересные дела в реальности. Разумеется, разным детям это необходимо в разном объеме. Но, как бы то ни было, зависимость от сетей является только следствием, а не причиной (*Социальные сети: опасность мнимая или реальная? // Обозреватель (<http://life.obozrevatel.com/social/74659-sotsialnyie-seti-opasnost-mnimaya-ili-realnaya.htm>). – 2013. – 4.03).*

Недавно проведенное исследование выявило, что чаще всего люди выходят в социальные сети не в выходные, как предполагалось, а в

понедельник. Самая большая активность пользователей в социальных сетях приходится на разгар рабочего дня – 14:36 понедельника.

На это время приходится пик посещения Интернета. Это совпадает с затишьем на работе после обеда. Исследование обнаружило, что люди в это время выкладывают очень много информации, в том числе видео, сообщения, фотографии.

Самую значительную часть всего объема информации занимают именно снимки. В основном, это фотографии личного содержания, фото животных. Владельцы домашних питомцев, по меньшей мере, один раз в неделю публикуют фото с семьей, друзьями и животными. 51 % опрошенных отмечают, что у них в течение дня появляется желание переписываться с людьми, которые недоступны или находятся далеко. 45 % людей желают выйти в социальную сеть, чтобы заставить других улыбнуться.

Следом идет потребность в близости и общении. 37 % респондентов назвали это причиной посещения соцсети. Четвертая часть опрошенных выкладывают снимки и пишут сообщения, чтобы просто получить ответную реакцию. Каждый пятый пользователь таким образом пытается привлечь к себе внимание.

Экспертам удалось выяснить основные области интересов людей, общающихся в социальных сетях. Первое место заняли личные фото. Второе направление, привлекающие внимание, это различные изображения животных. На третьей позиции – увлекающие предложения. Четвертую ступень рейтинга занимают смешные картинки и вирусы. На пятом – разные новости. Шестыми по заинтересованности пользователей стали шутки. Седьмое место у забавных видеороликов. Восьмой стала музыка (***Чаще всего соцсети посещают в понедельник после обеда // NovostiUA (<http://novostiua.net/obshchestvo/32589-chasche-vsego-socseti-poseschayut-v-ponedelnik-posle-obeda.html>). – 2013. – 6.03).***

Как социальные сети могут влиять на отношения?

Каждый третий развод в мире происходит по вине социальных сетей. Отсутствие каких бы то ни было барьеров и широкий выбор партнеров для общения в соцсетях приводит к всплеску желаний. Количество измен, с момента возникновения такого понятия, как социальная сеть, возросло втрое. Возросло и число внутрисемейных конфликтов, ведь 80 % людей склонны больше доверять онлайн-друзьям, а не мужьям и женам.

Негативно воздействуют социальные сети и на отношения между детьми и родителями. В среднем, дети начинают самостоятельно пользоваться соцсетями с 10 лет. Постепенно время, проведенное подростком в сети, увеличивается. В итоге, 20 % подростков способны находиться онлайн 21 час в сутки. 80 % родителей уверены, что знают, чем их чада занимаются в Интернете, но у детей противоположное мнение – 31 %

детей убеждены, что их родители даже не догадываются, что они делают в сети. 69 % родителей включают своих детей в друзья в соцсетях, а вот дети отвечают взаимностью и «френдят» своих родителей лишь в 32 % случаев. Хуже всего то, что 90 % подростков с доверием относятся к советам ровесников на сайтах и, в первую очередь, обращаются за советом к ним, а не к родителям.

Кроме прочего, излишняя увлеченность электронным общением приводит к снижению иммунитета, сердечно-сосудистым заболеваниям и душевной дисгармонии. Малая подвижность и зачастую пустые мыслительные процессы (обработка скучной и ненужной информации) способствуют развитию заболевания эндокринной системы (*Как социальные сети могут влиять на отношения? // VLASTI.NET (<http://vlasti.net/news/161793>). – 2013. – 9.03).*

Американские исследователи выяснили, что социальная сеть Facebook теряет свою популярность среди молодежи по всему миру, пишет журнал Time.

Представители Facebook признались, что некоторые пользователи соцсети, особенно молодежь, все активнее пользуются другими продуктами и услугами, такими как Instagram, Twitter и Tumblr.

Вместо Facebook подростки все чаще выбирают Instagram для выкладывания фотографий, Twitter – для размещения статусов, а сайт микроблогов Tumblr предлагает молодежи больше возможностей для творческого самовыражения.

При этом опрошенные подростки отметили, что, когда они достигнут 20-летнего возраста, Facebook может стать для них более интересным, нежели другие соцсети, так как сегодня они постоянно видятся с друзьями в школе и знают друг про друга все. А позже, когда все разъедутся по колледжам, Facebook станет источником новостей от друзей.

Однако, несмотря на подобные показатели, аудитория Facebook продолжает расти по всему миру. Так, в 2012 г. количество пользователей соцсети увеличилось на 28 % (*Популярность Facebook значительно падает // InternetUA (<http://internetua.com/populyarnost-Facebook-znacsitelno-padaet>). – 2013. – 12.03).*

Пользователи Facebook недооценивают свою аудиторию.

Почти каждый знает, сколько у него виртуальных друзей в Facebook, однако мало кто действительно представляет, сколько именно человек видят каждую опубликованную в соцсети запись. Количество лайков и комментариев – далеко не достоверный показатель. Проведенное учеными исследование показало, что большинство пользователей сильно недооценивают размер своей аудитории.

Научная работа была проведена информационными аналитиками из Стэнфордского университета – М. Бернштейном, И. Бэкси, М. Бюрке и Б. Кэрриером. Как показало исследование, каждый пост в Facebook попадает на глаза в среднем одному из трех виртуальных друзей пользователя. Ученые получили эти цифры, проанализировав 220 тыс. постов в Facebook, сделанных в течение июня 2012 г., сообщает The New York Times.

Аналитики также опросили пользователей, как они оценивают размер их аудитории. «Люди перманентно недооценивают количество своих читателей», – сделали вывод исследователи. Это связано с тем, что Facebook постоянно изменяет и дорабатывает алгоритм, отвечающий за отображение записей в лентах новостей. Это приводит к тому, что пользователи попросту не успевают привыкнуть к переменам и подстроиться под них (*Пользователи Facebook недооценивают свою аудиторию // InternetUA (<http://internetua.com/polzovateli-Facebook-nedoocenivauat-svoua-auditoriuu>). – 2013. – 11.03).*

«ВКонтакте» оказался самой аддиктивной соцсетью Рунета.

Портал Superjob.ru по просьбе Roem.ru провёл исследование того, сколько времени пользователи социальных сетей могут воздерживаться от того, чтобы не пользоваться ими.

В принципе, все соцсети разделились на два лагеря: с высокой аддиктивностью («ВКонтакте» и «Одноклассники», пользователи которых не могут и двух дней провести в Интернете без того, чтоб не зайти на сайт) и, соответственно, с низкой (Facebook, Twitter и «Мой Мир», где доля пользователей, которые не помнят, когда заходили в соцсеть, составляет 15, 18 и 21 % соответственно) (*«ВКонтакте» оказался самой аддиктивной соцсетью Рунета // Roem.ru (<http://roem.ru/2013/03/07/vkontakte65854/>). – 2013. – 7.03).*

Соцмережа може визначити віросповідання чи політичну приналежність через ваш профіль.

Завдяки комп'ютерним програмам можна дізнатись особисту інформацію про користувачів Facebook, якою вони хоча б раз ділилися в мережі.

Як повідомляє Financial Times, соціологи та програмісти з Кембриджського університету провели дослідження за підтримки Microsoft, у якому використовувались дані 58 тис. випадкових користувачів соціальної мережі Facebook.

Завданням дослідження було зібрати якомога більше інформації, яка не була спочатку вказана користувачами в їхньому соціальному профілі, але так чи інакше стала відома за час користування акаунтом.

Об'єктом дослідження став величезний обсяг персональних даних, які можуть бути використані різними комп'ютерними програмами. За результатами дослідження можна дізнатись найнесподіванішу особисту інформацію про користувачів: починаючи з того, яка у вас сексуальна орієнтація, чи вживаєте ви наркотики, аж до можливості оприлюднення факту розлучення ваших батьків.

«Точність, з якою алгоритми визначили сексуальну орієнтацію у чоловіків, становить 88 %, расу – 95 %, а релігійну приналежність і політичні погляди – 80 %. Тип особистості й емоційну стабільність також вдалося передбачити з точністю до 62–75 %», – ідеться в повідомленні Financial Times.

Автори роботи кажуть, що для дослідження вони використовували тільки Facebook. Офіційні представники найпопулярнішої соцмережі світу результати дослідження не коментують. «Ми застосовували дуже прості і загальні методи. Маркетингові компанії можуть піти набагато далі і підключити великі ресурси», – говорить один з організаторів проекту М. Косинські.

Зазначимо, що отримання особистої інформації віднедавна є джерелом значних прибутків. Наприклад, британська компанія Wonga, яка займається онлайн-кредитуванням, приймає рішення щодо видачі кредиту протягом декількох секунд, ґрунтуючись на величезній інформації про кандидата, у тому числі його профілі у Facebook (*Facebook може розповісти найнесподіванішу інформацію про користувачів // iPress.ua (http://ipress.ua/news/facebook_mozhe_rozpovisty_naynespodivanishu_informat_siyu_pro_korystuvachiv_16914.html). – 2013. – 12.03*).

Маніпулятивні технології

Кандидата в депутаты сняли с выборов из-за социальных сетей. По заявлению суда, он использовал в агитации символику Facebook и «ВКонтакте».

«Краснодар, 9 марта – АиФ-Кубань». Кандидата в депутаты городской думы от партии «Справедливая Россия» Г. Уфимцева не стал регистрировать Ленинский районный суд Краснодара.

По мнению суда, Г. Уфимцев использовал в агитации интеллектуальную собственность социальных сетей – он указывал в информационном бюллетени адреса своих страниц в социальных сетях в Facebook, «ВКонтакте» и Twitter.

В региональном отделении «Справедливой России» считают, что пользователи социальных сетей имеют право использовать логотипы сайтов. Г. Уфимцев собирается обжаловать решение в вышестоящей инстанции. Он заявил, что это «политическая расправа», так как по одному кругу с ним баллотируется сын председателя краевой избирательной комиссии, сообщает портал Южного федерального округа (*Кандидата в депутаты сняли с*

выборов из-за социальных сетей // Webkrasnodar.ru (http://news.webkrasnodar.ru/polit/4528137/). – 2013. – 9.03).

В Кировоградской области милиционеры допрашивали активистов ВО «Свобода» из-за записей в социальных сетях с призывом снести памятник Ленину. Об этом MyTime сообщили в пресс-службе политсилы.

По словам председателя Кировоградской областной ВО «Свобода» А. Ромащенко, накануне выходных заместитель начальника Александрийского горотдела (Кировоградская область) и начальник криминальной милиции решили пообщаться с членами Александрийской городской организации ВО «Свобода». Как выяснилось, целью встречи стала «профилактическая беседа» по поводу идеи сноса памятника Ленину в городе.

Милицейский руководитель заявил, что местные «свободовцы» выступают в социальных сетях с призывом к разрушению памятника Ленину, что является нарушением законодательства. На что представитель ВО «Свобода» апеллировал, что такие действия милиционера являются недопустимыми из-за права свободного волеизъявления мыслей гражданами Украины, которое гарантирует Конституция Украины.

«Подобная практика граничит со здравым смыслом. Складывается такое впечатление, будто правоохранные органы уже преодолели преступность, коррупцию и решили заняться мониторингом социальных сетей», – отметил глава ВО «Свобода» в Кировоградской области (***Милиционеры допрашивали свободовцев из-за записей в соцсетях // MyTime (http://mytime.net.ua/news/2013/03/2013-03-04-73.htm). – 2013. – 4.03).***

Роль соцсетей в поиске и проверке сотрудников.

Социальные сети создавались не для проверки сотрудников, но сегодня не секрет, что, кроме основного предназначения, их используют для рекламы продукции, увеличения продаж, раскрутки своего бренда и многого другого. Worknew.info рассказывает, какую можно получить пользу от социальных сетей в процессе поиска и проверки сотрудников.

В Украине наибольшей популярностью пользуются V Kontakte.ru (аудитория – в основном молодежная – школьники, студенты), Facebook.com (характеризуется более взрослой и «состоявшейся» аудиторией), Odnoklassniki.ru (аудитория в основном взрослая).

Для рекрутеров социальные сети могут быть полезны в двух направлениях: поиск интересных кандидатов и проверка информации о уже имеющихся кандидатах (часто может быть полезно узнать о интересах найденного специалиста, его круге общения и т. д.). Источником полезной информацией является также список групп, в которых зарегистрирован ваш

кандидат и его активность в этих группах. Но есть и определенные сложности, которые возникают при сборе информации в соцсетях: 1. Закрытые группы. К счастью там, как правило, не отказывают в принятии в группу новых подписчиков. 2. Аккаунты, которые доступны только для друзей. Для того чтобы просмотреть профиль надо стать другом, то есть получить подтверждение от пользователя, что удастся далеко не всегда. Хотя при желании просмотреть такие аккаунты можно, зная структуру ссылок в социальных сетях и id человека.

Полезным источником информации для рекрутера может стать анализ того, какие приложения использует конкретный человек, а также и их количество. В Facebook есть функционал, который транслирует всю активности человека в Интернете, так что здесь можно быстро получить все необходимые сведения. В социальных сетях можно сделать еще одно важное наблюдение, а именно: проявляет ли там активность кандидат в рабочее время и, соответственно, будет ли он вместо исполнения своих прямых обязанностей проводить время в Интернете.

Кроме общих социальных сетей, существуют еще социальные бизнес-сети. Они придуманы для ведения деловых споров, поиска новых профессиональных контактов, а также поиска работы и сотрудников, то есть напрямую могут быть полезны рекрутеру. Наиболее популярны на сегодня такие социальные сети: LinkedIn.com – сеть для поиска и установления новых деловых контактов, Moikrug.ru – это один из сервисов Яндекса, который в принципе аналогичен LinkedIn, существуют и другие менее распространенные бизнес-сети. Здесь можно быстрее и лучше раскрыть именно профессиональные качества кандидата. Профиль в бизнес-сетях похож на то, что кандидат пишет в резюме, опция рекомендации позволяет советовать специалистов, можно также сделать запрос на отзывы о конкретном человеке. Часто имеет смысл изучить события, в которых принимает участие кандидат (к счастью закрытых аккаунтов в таких сетях не существует).

Кроме социальных сетей, иногда стоит изучить блоги: livejournal.com, blogspot.com, blog.ru, liveinternet.ru и микроблоги Twitter, chikchirik. В них человек часто более раскрепощен, здесь больше «живых» сообщений. Помните, что блоги индексируются поисковиками, это обязательно облегчит поиск интересующей информации.

Как правило, социальные сети помогают узнать о человеке намного больше, чем резюме и классические собеседования, поскольку многие пользователи абсолютно беспечно относятся к безопасности их личной информации. Но к сожалению, на сегодня социальные сети часто недооценивают в мире бизнеса, а рекрутеры зачастую жалеют времени на получение ценной информации о кандидатах. Хотя если в ближайшее время к нам не придет волна опасений людей насчет этичности использования их личных данных и информации другими пользователями, ожидается существенный рост интереса рекрутеров, специалистов в области персонала,

а также служб безопасности предприятий к социальным сетям (*Роль соцсетей в поиске и проверке сотрудников // Украинский Бизнес Ресурс (http://ubr.ua/labor-market/ukrainian-labor-market/rol-socsetei-v-poiske-i-proverke-sotrudnikov-213176). – 2013. – 7.03).*

По статистике, почти 50 % украинских детей размещают в соцсетях свои адреса и телефоны и не догадываются, что виртуальное общение может быть опасным.

14-летняя львовянка Аня боится выходить на улицу. Телефон поставила в режим «без звука». Каждый день в мобильном появляются все новые непринятые звонки, а во дворе ее дома то и дело мелькает высокая фигура в затертом синем пуховике. Аня знает, что мужчину в пуховике зовут Игорь, ему 35 лет и он так же, как она, очень любит смотреть мультфильм «Винкс». Еще что он очень одинок и ищет друга, пишет стихи и работает компьютерщиком. Всю эту информацию она почерпнула из соцсети. Аня – типичный подросток, и посещение своей странички в Интернете для нее такой же привычный ритуал, как и чистка зубов. Благодаря онлайн-активности у нее 74 виртуальных друга. Игорь был 75-м. Правда, общалась она с ним всего неделю. Потом надоело. Только вот Игорь думал иначе. Он продолжал писать. Потом стал звонить, и вот сейчас караулит ее у дома. Поначалу Аня удивлялась: откуда он знает? Вскоре поняла и удалила со своей странички телефоны и адреса. Однако Игорь продолжает ходить, звонить и травить в сети, отправляя непристойности. В отличие от множества «электронных» друзей, в реальной жизни подруг у Ани просто нет, даже пожаловаться некому. А обратиться к родителям она никогда бы не решилась – отец бы точно взял ремень и выпорол. Все, на что она надеется, что Игорь, наконец, перестанет ее преследовать и исчезнет из ее виртуальной и реальной жизни.

ФОТО. 12-летняя киевлянка Маша боится идти в школу. Как только она переступает порог класса, все начинают глупо хихикать, показывать пальцами и обзывать секс-бомбой. Дело в том, что фото с ее оголенным телом уже несколько месяцев «гуляет» в соцсетях. И это не фотошоп, а реальная фотография, которую Маша сама сделала с помощью мобильного телефона и отослала своему уже бывшему парню в ММС. «Чтобы ты понял, что потерял», – подписала девочка свое сообщение. Таким образом она «отомстила» ему за то, что он ее бросил. Только Маша не знала, что через несколько дней «сердобольный» парень выложит ее фото на своей страничке в Интернете. Даже подпись сохранил, чтобы соблюсти авторские права!

С этого дня учеба в школе стала для Маши пыткой. С ней никто не хочет сидеть за одной партой. Когда она выходит к доске, ее начинают травить и отпускать колкости. Маша возражать не может, иначе фотография появится на столе в учительской. По крайней мере, так ее запугивают

одноклассницы. Кроме всего прочего, школьницу волнует что будет с родителями, когда они увидят это фото!

ШАНТАЖ. 10-летний харьковчанин Миша боится ложиться спать. «Мне очень страшно», – объясняет он маме и просто плачет. Мальчик не может сказать родителям, что боится своего нового интернет-«друга» под вымышленным именем Макколей Калкин. Каждый день на его страничку приходят сообщения с очередными угрозами расправы, нецензурной бранью и требованием встречи. «Иначе я расскажу твоим родителям, какой ты плохой мальчик», – пишет Макколей. Ребенок пытался удалять сообщения, но злостный Калкин преследует его, рассылая гадости не только ему, но и его друзьям.

КИБЕРОХОТНИКИ. Все эти истории – увы, реальность. С такими проблемами дети все чаще обращаются на Национальную детскую горячую линию, работающую в Центре «Ла СтрадаУкраина», плачут и просят о помощи. «То, с чем столкнулись ребята, называется кибербуллинг, – говорит директор департамента консультативной поддержки национальных горячих линий центра И. Мидловец. – В это понятие входит размещение угроз в сети Интернет, рассылка сплетен, компрометирующих фотографий. Так кибернасилы держат свою жертву – ребенка – под контролем. Могут шантажировать и даже довести до самоубийства. Киберохотники (грумеры), как правило, хорошо разбираются в детской психологии, умеют быстро войти в доверие и умело манипулировать. Грумеры выбирают ребенка, который чувствует себя покинутым или ненужным, и становятся их “другом”. Как это было в случае с львовянкой Аней, которую теперь ее друг просто преследует, и в случае с Мишей, которого травит некий Макколей». Юрист центра В. Мудрик, также консультирующая на линии, добавляет: «Чаще всего грумеры “дружат”, пока не добьются своего (как правило, сексуального контакта), после чего теряют интерес к своей жертве. Родители должны как можно быстрее сообщить о грумере в правоохранительные органы. Кибербуллинг как минимум подпадает под статью о хулиганстве, за что предусмотрена криминальная ответственность (а это может быть до трех лет лишения свободы)».

ТРАВЛЯ. «Наиболее распространенный вариант кибербуллинга – это травля детьми друг друга, – разъясняет И. Мидловец. – Мы все помним фильм “Чучело”, где героиню травили одноклассники. То же происходит и сегодня, только онлайн. В отличие от фильма, в Интернете нельзя сказать: “Прости нас, Чучело!” – и все забудется. Однажды выложенная в Интернете фотография, даже при ее дальнейшем удалении, не исчезает, она сохраняется на сервере и может “всплыть” в любой момент. Вариант перейти в другую школу или переехать в другой город – не срабатывает. Потому что первое, что делают школьники, когда к ним в класс приходит новый человек, – “пробивают” его по всем соцсетям. И все начинается сначала».

ЧТО ДЕЛАТЬ? «Жертвам кибербуллинга в первую очередь необходима поддержка и понимание родителей, – уверена психолог детской

горячей линии А. Кривуляк. – Потому мамам и папам нужно постараться максимально сохранять спокойствие. Если родители в панике, ребенок еще больше чувствует себя виноватым в том, что он не оправдал надежд родителей. Будет полезен визит к квалифицированному психологу. Если ребенок эмоционально не готов посещать школу, следует дать ему возможность побыть дома столько, сколько посоветует психолог. Главное – всячески показать ребенку, что вы его любите и не сердитесь за проступок, ведь ему и так очень тяжело. Если травля происходила в среде одноклассников, не стоит устраивать большой скандал. Лучше подойти к классному руководителю и школьному психологу. Очень эффективным бывает приглашение в класс детского психолога, который бы провел тренинги или игры, разъясняющие ситуацию. Чтобы дети сами поняли, что они поступают неправильно».

ФАКТЫ. По статистике, 44 % пользователей с 11 до 17 лет размещают в соцстраничках свои адреса и телефоны. 60 % детей с 15 до 17 лет попадали в рискованные ситуации (ходили на встречи с виртуальными знакомыми). 50 % детей вообще не догадываются, что Интернет может быть опасен, и не знают элементарных правил безопасности онлайн-общения.

Родителям: пять правил безопасности поведения в Интернете, которые нужно объяснить каждому ребенку.

1. Не разглашать домашний адрес, телефон, номер школы, место работы родителей.

2. Стараться общаться в Интернете только с теми, кого знаешь в реальной жизни.

3. Виртуальные люди не всегда пишут правду о себе. Если ребенок решит встретиться с таким другом, надо предупредить родителей и встречаться только в людных местах.

4. Не размещать в Интернете откровенные фотографии.

5. Не отвечать на письма или просьбы, которые вызывают чувство стыда или дискомфорта.

Национальная детская горячая линия: 0-800-500-225 (*Белюсова А. Как уберечь ребенка от опасностей в Интернете // Сегодня (<http://www.segodnya.ua/ukraine/Kak-uberech-rebenka-ot-opasnostey-v-internete.html>). – 2013. – 15.03).*

«Кликтивизм», или Почему провалилась «Революция через социальные сети».

Не так давно в Беларуси возник интерес к тому, чтобы превратить социальные сети в протестную среду, а виртуальную активность – в реальную политическую борьбу. Опыт «Революции через социальную сеть» был удачным только отчасти. Почему?

Не так давно в Беларуси возник интерес к тому, чтобы превратить социальные сети в протестную среду, а виртуальную активность – в

реальную политическую борьбу. Опыт «Революции через социальную сеть» был удачным только отчасти. Имевшие место в Беларуси эксперименты с организацией протестной активности в социальных сетях можно рассматривать в контексте развернувшейся некоторое время назад критики роли в обществе социальных медиа и «кликтивизма».

Социальные сети: «слабые связи» и «низкие риски»

Общественная активность в период «Арабской весны», протестных и революционных выступлений, начавшихся в 2010 г., привела к тому, что все начали обсуждать роль в этих событиях социальных сетей и медиа. Журналист «Нью-Йоркера» М. Гладуэлл критически отнесся к происходящему, сравнивая протестное движение против расовой сегрегации в США в период 1960-х годов с тем, что происходит сегодня, в цифровую эпоху.

По мнению М. Гладуэлла, удачный опыт активизма в «доцифровую эпоху» связан с тем типом отношений, который существовал между людьми, занимавшими активную позицию – все они хорошо знали друг друга и были способны объединиться не только ради идеи, но и благодаря этим связям. Но платформы социальных медиа сегодня строятся иначе, вокруг «слабых связей».

Facebook и Twitter, например, – это скорее инструменты для коммуникации с людьми, с которыми вряд ли можно поддерживать отношения другими способами.

«Слабые связи», доминирующие в сети, могут быть в определенном смысле эффективными, но только не в том случае, когда речь идет о «высокорискованной активности». При помощи социальных сетей можно организовать сбор средств, найти подходящего донора, но очень трудно совершить революцию.

Социальные сети, вопреки распространенному мнению, способствуют не повышению мотивации для участия в «праведном деле», а скорее развитию «соучастия» и даже снижению мотивации: люди, не имеющие мотивации для реального самопожертвования, заменяют ее отсутствием онлайн-активностью.

Кроме того, существует еще одна важная особенность социальных сетей и онлайн-протестов – социальные сети принципиально неиерархичны, связи между людьми в группе свободны, в то время как наиболее успешный опыт протеста связан с наличием централизованной структуры и конкретных лидеров, как это и было в 1960-е в США, в эпоху Мартина Лютера Кинга. Свободная структура движений в социальных сетях делает их уязвимыми извне и изнутри, хотя и создается модель гибких, мобильных социальных связей.

Новая реальность «кликтивизма»

В 2011 г. в оксфордском словаре появилось новое слово – кликтивизм. Сам термин обозначает «использование социальных медиа и других интернет-методов для продвижения какого-либо дела, процесса». Конечно, в

это понятие не включена вся интернет-активность, но «кликтивизм» стали использовать для анализа ряда случаев, включая феномен организованных протестов во время «Арабской весны», подписание онлайн-петиций, организацию бойкотов политиков и т. д.

«Кликтивизм» не сводится только к онлайн-поддержке инициатив, но включает и другие способы связанной с этим активности. Появление «кликтивизма» совпало с развитием социальных медиа и ростом их влияния в мире, чем и воспользовались многочисленные НГО для того, чтобы влиять на общественную ситуацию.

Левое движение, протесты и рынок

В 2010 г. в газете «Гардиан» появляется статья, автор которой попытался разобраться с тем, как возникновение «кликтивизма» могло повлиять на содержание и практику работы «традиционных» активистов. С его точки зрения, новые практики онлайн-активности не избежали того, что он называет «маркетизацией»: для организации протестов и массового привлечения участников стали использоваться «рыночные» способы и «маркетинговые» ходы, которые выхолащивают суть протестного движения.

Так возникает угроза превращения «дигитального/цифрового» активизма в «кликтивизм» в негативном смысле.

Одновременно возникает важный вопрос: не делает ли такая активность невозможной «освободительные» революции, хотя бы потому, что вся деятельность протекает онлайн?

По сути, «кликтивизм» стал разрушать левую протестную активность, поскольку в нее вносилась идеология рынка, когда организация социальных движений начинает приравниваться к организации кампаний по продаже туалетной бумаги.

Появление онлайн-кампаний и организаций массового толка часто препятствует тому, чтобы различные сообщества могли напрямую представлять свои идентичности и требования, которые таким образом «колонируются» «кликтивистами», а организации, которые действительно могли бы говорить от имени сообществ, выводятся из игры. Радикальные требования становятся невозможными, а количество собранных подписей превращается фактически в единственный критерий эффективности кампаний. И это достижение оформляется подобно витрине в универмаге «Уолмарт» – не активизм, а сплошной маркетинговый обман.

Цифровой, технократический подход к организации онлайн-активности нивелирует идею социальных перемен и не имеет никакого отношения к природе «социальных разрывов». В результате подмены политической критики «рекламой» распространяются политический цинизм и политическая пассивность. Если говорить об индивидуальном участии, то «кликтивизм» скорее мешает появлению людей с сильными позициями, да и количество активистов на самом деле не является очень большим, несмотря на размах онлайн-петиций и кампаний.

Белорусский случай сетевых протестов

В Беларуси реальные попытки организации протестного движения при помощи социальных сетей относятся к 2011 г. (если не брать во внимание сетевую кампанию, стихийно возникшую после разгона митинга на площади 19 декабря 2010 г., когда при помощи Интернета шел активный обмен информацией и сбор помощи задержанным). Летом 2011 г. появился феномен «молчаливых протестов», организованных при помощи социальных сетей. История «Революции через социальную сеть» уже подробно описана в Википедии, но вот анализ роли социальных медиа и социальных сетей в тех событиях до сих пор не завершен.

Начать стоит со статистики, хотя ее цифры различаются в различных источниках и могут интерпретироваться различным образом. Но в любом случае статистика свидетельствует о том, что со второй половины 2000-х в Беларуси наблюдаются две тенденции.

Первая тенденция – значительный рост пользователей Интернета. В 2011 г. насчитывается, по данным Белстата, более 6,8 млн «пользователей и абонентов сети Интернет». Хотя, по данным Gemius Belarus, к пользователям Интернета относятся чуть более 4,5 млн человек и уровень проникновения Интернета оценивается в 56 % населения.

Вторая тенденция – значительный рост пользователей социальных медиа и сетей (в 2011 г. пользователей сети «ВКонтакте» насчитывалось более 2 млн, пользователей «Одноклассников» – более 1 млн человек, пользователей LiveJournal – более 600 тыс. человек, размер аудитории Facebook – более 1 млн человек и т. д.). Также важны некоторые особенности этой аудитории: люди могут иметь несколько аккаунтов в разных социальных сетях; в Минске и Минской области пользователей Интернета больше, чем в регионах.

Эти цифры выводят Беларусь на вполне «европейский» уровень проникновения Интернета, но при этом важно обращать внимание на то, как именно работают социальные медиа и сети, учитывая специфику белорусского общества – слабые структуры гражданского общества и установившийся политический режим.

Тезис о слабости гражданского общества обозначает ситуацию, в которой нельзя говорить о том, что различные группы белорусского общества сегодня могут артикулировать свои интересы и представлять их в разного рода структурах и организациях.

Общество в Беларуси плохо структурировано, и это отражается в Интернете: история «Революции через социальную сеть» показывает, что появившиеся в ходе протестов онлайн-сообщества ориентированы на несколько общих идей, но эти идеи могут и не соотноситься с интересами других социальных групп белорусского общества.

Об уровне репрезентации общественных настроений говорит и содержание более чем 1300 тем для обсуждения в группе «Революция через социальную сеть» (более 46 тыс. участников) в сети «ВКонтакте»:

наибольшее количество комментариев (22 270 сообщений) собрала тема «Игра – займемся сексом! Решаем демографические проблемы:»). В то время как тема, например, отношений с Россией собрала 1457 комментариев, а опрос на тему: «Беларусь и иммигранты» собрал 4188 сообщений. И все эти сообщения, конечно, часто далеки от взвешенной и информированной позиции. Даже учитывая специфику аудитории сети «ВКонтакте» можно задать вопрос о том, насколько эффективны подобные онлайн-сообщества в контексте политической борьбы и действительного обсуждения проблем.

Открытым остается вопрос и о том, к каким группам белорусского общества относятся те люди, которые принимали активное участие в событиях 2011 г., насколько они были активны, не ограничено ли участие в протестах определенными социальными рамками (принадлежностью, например, к спорной группе белорусского «среднего класса»), были ли они все интернет-пользователями и т. д.

Революционное одиночество в сети

Конечно, белорусские власти пытаются контролировать то, что происходит в сети, в том числе и занимаясь «работой» с модераторами социальных сетей и цензурой. Однако проблема состоит и в том, что за пределами виртуальных сетей практически отсутствуют структуры гражданского общества, которые бы регулярно и в массовом порядке контактировали с обычными гражданами и социальными группами, а уж потом это становилось бы «видимым» в социальных сетях и медиа. У нас всё наоборот – в сетях конструируется определенный образ общества, который потом ему и сообщается или провозглашается верным.

Проведенное М. Недвецким для «Палітычнай сферы» в 2010 г. исследование веб-активности депутатов на выборах в Минске показало ее низкий уровень, отсутствие навыков использования Интернета в политической борьбе.

Кроме того, согласно цифрам, приведенным в презентации А. Мецик, на ноябрь 2011 г. только очень небольшое количество пользователей социальных медиа в Беларуси (от 1 до 4 %) регулярно пользуются социальными медиа при поиске ответа на интересующие их вопросы, пусть даже бытового характера. Хотя, как отмечают эксперты, экономический кризис подстегнул интерес к социальным медиа в 2011 г. – жители Беларуси стали чаще обращаться за экономической информацией, находящейся в сети.

Поместив белорусскую ситуацию в международный контекст, можно отметить, что распространяющаяся там сегодня критика «кликтивизма» актуальна и для Беларуси в том смысле, что у нас политическая активность онлайн явно страдает собственной маркетизацией – когда привычные лозунги борьбы подаются в новой и привлекательной веб-форме, не наполняясь, однако, существенным и важным содержанием.

Для нас также актуальны и рассуждения о том, что онлайн-активность часто бывает всего лишь безопасным способом выражения собственной позиции и признаком отсутствия мотивации иного толка.

Революционно настроенные одиночки обмениваются твитами и линками, но из этого получается не революция, а психотерапия.

Можно также предположить, что социальные сети и медиа в Беларуси являются своего рода «квазипубличной сферой» – в них хоть и отражаются определенные общественные настроения, но при этом трудно определить степень влияния дискуссий в социальных медиа на общество в целом, как и невозможно утверждать, что мы имеем дело со всем спектром общественных настроений. И это заставляет относиться с осторожностью к мечте о «Фейсбук-революции» в Беларуси (*Браточкин А. «Кликтивизм», или Почему провалилась «Революция через социальные сети» // http://n-europe.eu/article/2013/03/13/kliktivizm_ili_pochemu_provalilas_revoljutsiya_cherez_sotsialnye_seti). – 2013. – 12.03).*

Зарубіжні спецслужби і технології «соціального контролю»

При помощи Skype власти Китая проводят слежку за пользователями. Как сообщило издание Businessweek, аспирант Университета Нью-Мексико Д. Нокел провел исследования китайской версии Skype от Microsoft, в результате чего обнаружил, что Skype для китайских пользователей поставляется со встроенным клавиатурным шпионом, проверяющим вводимые тексты на предмет запрещенных слов и отправляющим полученные данные в государственные спецслужбы.

Отметим, что пользователи из Поднебесной пользуются особым дистрибутивом ПО. Так, в Китае запросы Skype переадресовываются к местной интернет-компания TOM Online, которая распространяет китайскую версию мессенджера – TOM-Skype.

В ходе исследования Д. Нокел обнаружил тысячи терминов, отслеживаемых государственными органами, которые относятся к таким запрещенным темам, как порнография и наркотики, а также к политической сфере, в частности «международная амнистия», «тяньаньмэнь» (термин, относящийся к протестным акциям и революции), «Репортеры без границ», BBC News и пр.

Исследователь сообщил, что база запрещённых в Китае ключевых слов постоянно обновляется. Несмотря на то что эти данные зашифрованы, Д. Нокелу удалось выделить конечные последовательности символов, отвечающие за отдельное словосочетание, при помощи последовательного деления файла базы надвое и наблюдения за сетевой активностью при его вводе.

Согласно полученным в результате исследования данным, в настоящее время органы власти Китая фиксируют не только переписку внутри страны, но отслеживают также сообщения, отправляемые пользователям за границей.

По словам Д. Нокела, результаты его исследования демонстрируют конфликт между пропагандой Microsoft неприкосновенности личной жизни

человека и ролью компании в надзоре и мониторинге. «Я хотел бы получить от них (Microsoft) отчет, где бы раскрывалась социальная политика компании и подтверждался тот факт, что TOM-Skype используется для проведения надзора», – заявил исследователь (*При помощи Skype власти Китая проводят слежку за пользователями // ООО «Центр информационной безопасности»* (<http://www.bezpeka.com/ru/news/2013/03/12/skype-hijacked-in-china.html>)). – 2013. – 12.03).

Власть собирается контролировать Интернет.

Специалисты МВД разработали законопроект, который позволит противодействовать киберпреступности и уголовно наказывать за DDoS-атаки, которые направлены на интернет-сайты госорганов. Отдельным пунктом идет статья, которая предусматривает наказание за пропаганду жестокости и насилия в сети, которая теперь будет восприниматься как угроза национальной безопасности, передает newsoboz.org со ссылкой на uapress.info

Нардеп С. Гриневецкий, который является членом Комитета по вопросам национальной безопасности, считает целесообразным ужесточение наказаний за подобные правонарушения. А вот юрист О. Мальский считает, что увеличение статуса таких правонарушений даст дополнительные возможности правоохранительным органам. Ведь теперь под предлогом угрозы нацбезопасности силовики смогут получать доступ к документам и компьютерам предприятий.

«Расширение компетенций в этом вопросе даст органам больше возможностей при проверке предприятий. Например, это позволит проводить выемку документов под предлогом угрозы нацбезопасности», – пояснил О. Мальский.

А вот в самом МВД отказываются давать комментарии по поводу предлагаемого законопроекта. В частности, начальник управления по борьбе с киберпреступностью МВД Украины М. Литвинов сослался лишь на пояснительную записку к документу, где говорится о создании правовой основы для дальнейшей разработки законов и подзаконных актов для защиты интересов граждан и государства в киберпространстве.

Следует отметить, что уголовная ответственность за преступления в Интернете существует и сегодня, но противодействие киберпреступникам со стороны МВД неэффективное. Достаточно вспомнить успешные DDoS-атаки на веб-порталы госорганов, которые были проведены в отместку за закрытие файлообменника ex.ua и принятия закона о языковой политике.

Эксперты и блогеры считают, что МВД делает очередную попытку в ограничении гражданских свобод в стране под видом борьбы с порнографией, культом жестокости. Кроме того, некомпетентность людей, которые были авторами законопроекта, привела к тому, что предложенный

законопроект оказался явно недоработанным. В конечном счете, принятие такого закона может привести к появлению проблем у провайдеров.

Вряд ли сама инициатива МВД направлена именно на то, чтобы противодействовать киберпреступности, поскольку главная проблема для властей в том, что Интернет, в отличие от телевидения и прессы, им не подконтролен. И пользователи глобальной сети имеют возможность активно критиковать власть, правительство, а также получать информацию о причастности чиновников к коррупции. Поэтому нынешний режим попросту хочет получить возможность пресекать деятельность любого неудобного для него сайта под прикрытием угрозы национальной безопасности (*Власть собирается контролировать Интернет // NewsOboz (http://newsoboz.org/obshchestvo/vlast-sobiraetsya-kontrolirovat-internet-12032013115900). – 2013. – 12.03).*

Google согласились выплатить 7 млн дол. штрафа за сбор личных данных людей без их разрешения в рамках работы своего сервиса Street View (NovostiUA.net (<http://novostiua.net/techniks/32953-google-postradal-na-7-mln-dollarov-iz-za-prilozheniya-street-view.html>)).

В 38 штатах США интернет-гигант согласился уничтожить сообщения электронной почты, пароли и веб-истории. Эти данные были собраны с домашних беспроводных сетей, так как Street View собирало информацию в период между 2008 и 2010 г.

Google заявили, что они очень рады тому, что проблема решена. «Мы прилагаем все усилия, чтобы получить право на неприкосновенность частной жизни в Google. Но в данном случае мы не учли всех правил, поэтому мы быстро реорганизовали наши системы для решения вопроса», – говорится в заявлении фирмы.

«Руководители проекта никогда не хотели получать данные и тем более использовать их – даже ознакомительно. Мы рады, что работали с генеральным прокурором штата Коннектикут Д. Джепсеном и другими адвокатами государственных служб над тем, чтобы достичь этого соглашения».

«Потребители имеют право на защиту своей жизненно важной личной и финансовой информации от неправильного и нежелательного использования корпорациями, такими как Google», – заявил генеральный прокурор Нью-Йорка Э. Шнейдерман.

«Это было урегулированием вопросов о неприкосновенности частной жизни и защите прав граждан, чья информация была собрана без их разрешения» (*Google пострадал на 7 млн дол. из-за приложения Street View // NovostiUA (http://novostiua.net/techniks/32953-google-postradal-na-7-mln-dollarov-iz-za-prilozheniya-street-view.html). – 2013. – 13.03).*

Американская полиция по горячим следам поймала вора, который, недолго думая, опубликовал сделанные украденным телефоном фото на странице в Facebook.

Вор напал на девушку на улице г. Бронкс и убежал с ее телефоном. Полиция пыталась проследить за грабителем, но безуспешно. Вскоре, однако, пострадавшая увидела фото курящего марихуану вора и тут же рассказала об этом полиции.

Полицейские утверждают, что этот случай не первый и вор из Бронкса только пополнит уже существующий список глупых воров, которые сами станут жертвой украденного телефона.

Не так давно в Калифорнии арестовали женщину, которая украла iPad. Полиция обнаружила след преступницы только тогда, когда ее дети опубликовали фотографии матери в социальных сетях владельца гаджета.

Напоминаем, полиция во многих странах давно сделала вывод, что чем больше в руках у граждан становится дорогих смартфонов, тем чаще этих людей грабят. В Нью-Йорке же полиция жалуется, что устройства Apple портят им всю статистику преступности в городе, которая постоянно снижалась последние 20 лет.

Как сообщил представитель нью-йоркской полиции, в прошедшем году число «изъятий» преступниками у людей гаджетов Apple возросло на 40 %. Статистика могла быть еще хуже, если бы полиция не направила своих сотрудников магазины Apple Store. Там полиция помогает покупателям настраивать телефоны так, чтобы их можно было отследить в случае кражи (***Facebook снова помог полиции поймать преступника // InternetUA (<http://internetua.com/Facebook-snova-pomog-policii-poimat-prestupnika>). – 2013. – 13.03***).

Российские спецслужбы научились прослушивать разговоры, которые ведутся с помощью сервиса интернет-телефонии Skype, пишет газета «Ведомости» 14 марта со ссылкой на специалистов по информационной безопасности.

Так, по словам И. Сачкова, гендиректора компании Group-IB, занимающейся расследованием киберпреступлений, спецслужбы «уже пару лет» могут прослушивать разговоры, которые ведутся по Skype, а также определять местонахождение пользователя. И. Сачков добавил, что по этой причине сотрудникам его компании запрещено вести деловые разговоры по Skype.

Как рассказал М. Эмм, исполнительный директор компании Peak Systems (сервис-провайдер в области платежных систем), компания Microsoft, которая купила Skype в мае 2011 г., снабдила сервис технологией законного прослушивания. Любого абонента, по словам М. Эммы, можно

переключить на особый режим, в котором ключи шифрования генерируются не на устройстве пользователя, а на сервере.

Тот, кто имеет доступ к серверу, может, соответственно, прослушать разговор пользователя или прочитать его переписку. Как пояснил М. Эмм, такую услугу Microsoft предоставляет спецслужбам многих стран, а не только России.

Также газета, ссылаясь на неназванных специалистов по информационной безопасности, пишет, что российские спецслужбы не всегда получают доступ к разговорам Skype по решению суда. Часто доступ обеспечивается просто по запросу (*Российские спецслужбы научились прослушивать Skype // InternetUA (<http://internetua.com/rossiiskie-specslujbi-naucsilis-proslushivat-Skype>). – 2013. – 14.03*).

Сервис интернет-телефонии Skype опроверг информацию о том, что осуществляемые через него звонки прослушиваются российскими спецслужбами.

Как сообщает ИТАР-ТАСС со ссылкой на представителей работающего с Microsoft коммуникационного агентства, у компании действительно есть соглашение со спецслужбами о предоставлении исходного кода ПО. Без раскрытия кода невозможно использование программы в российских органах государственной власти.

Однако предоставление кодов не означает, что государственные организации могут читать сообщения или получать доступ к данным частных пользователей, отметил собеседник ИТАР-ТАСС. Зная алгоритм шифрования, но не имея ключа, невозможно перехватить сообщение. Спикер подчеркнул, что ключ создается на стороне пользователя (*Skype опроверг сообщения о прослушке спецслужбами // InternetUA (<http://internetua.com/Skype-oproverg-soobsxeniya-o-proslushke-specslujbami>). – 2013. – 14.03*).

Проблема захисту даних. DOS та вірусні атаки

По информации Reuters, хакеры атаковали некоторые из крупнейших новостных сайтов Чехии, полностью выведя из строя или проведя дефейс некоторых наиболее посещаемых чешских информационных ресурсов. 5 марта три крупнейших чешских новостных ресурса – ihmed.cz, idnes.cz и novinky.cz – одновременно, но независимо друг от друга сообщили о хакерских атаках и перебоях в работе сайтов.

На данный момент нет информации о том, кто мог бы стоять за атаками и что могло спровоцировать нападения. В отношении всех трех сайтов на данный момент предпринимаются скоординированные DDoS-атаки.

В прошлом месяце в Чехии стало известно о такой организации, как Комитет по защите журналистов, который заявил, что намерен атаковать ряд крупных чешских изданий, которые, якобы, цензурировали оригинальные статьи журналистов в угоду корпоративной политике и защите интересов собственников. Однако на данный момент нет никаких фактов о связи сегодняшних атак и заявлений, сделанных в феврале (**Неизвестные хакеры атаковали крупнейшие новостные сайты Чехии // ООО «Центр информационной безопасности»** (<http://www.bezpeka.com/ru/news/2013/03/05/checkh-sites-attacked.html>). – 2013. – 5.03).

Ведущие интернет-компании договорились сообща бороться с СМС-мошенничеством. Об этом изданию Lenta.ru рассказали в компании «Яндекс».

Как отметили в компании, в последнее время участились случаи мошенничества с СМС-подписками использованием названий «Яндекса» и других известных интернет-ресурсов. Вместе с «Яндексом» в проекте участвуют Google, Group-IB, Mail.Ru Group, «ВКонтакте», «Доктор Веб», «Лаборатория Касперского». Программа получила неформальное название «Операция Мухобойка».

Компании договорились об обмене данными об обнаруженных угрозах. Предполагается, что это поможет антивирусным компаниям оперативно блокировать мошеннические веб-страницы, а интернет-компаниям – предупреждать пользователей об опасности при попытке перехода на такие ресурсы.

Кроме того, участники программы договорились передавать обнаруженные короткие номера, с которых рассылаются недобросовестные сообщения, сотовым операторам. Интернет-компании надеются, что операторы будут блокировать такие номера (**Яндекс и Google объединились против СМС мошенников // Forenet.info** (http://forenet.info/news/news.php?subaction=showfull&id=1362559017&archive=&start_from=&ucat=4&). – 2013. – 6.03).

Согласно новому отчету компании Senzic, существующие уязвимости в веб-приложениях являются серьезной проблемой, поскольку они присутствуют почти в 99 % продуктов.

Исследователи спрогнозировали, каким уязвимостям наиболее всего будут подвержены жертвы в текущем году.

«Обеспечение необходимого уровня безопасности в современных компаниях должно быть решено более реалистично, – отмечает технический директор Senzic С. Парсель. – В текущем году увеличилось количество угроз, с которыми сталкиваются корпорации из-за существующих

уязвимостей, однако большинство компаний не в полной мере защищают себя от подобной опасности. И эта тенденция ухудшается».

Отчет экспертов Cenzic также включает в себя результаты исследования угроз безопасности мобильных устройств.

Согласно исследованию, 57 % всех уязвимостей в мобильных устройствах составляют ошибки в проверке входных данных (21 %), ошибки управления сессией (11 %), а также бреши раскрытия важных данных (25 %) **(99 % web-приложений содержат уязвимости // ООО «Центр информационной безопасности»** (<http://www.bezpeka.com/ru/news/2013/03/07/Cenzic-Application-Vulnerability-Trends-Report.html>). – 2013. – 7.03).

Киберпреступность по-запорожски: новые схемы и уловки злодеев.

Киберпреступность стала одним из распространенных экономических преступлений в Украине. Мошенники идут в ногу со временем и постоянно придумывают новые способы отъема денег у людей. О том, какая ситуация сложилась в Запорожской области и как уберечь себя, 11 марта 2013 г. на брифинге рассказал заместитель начальника управления по борьбе с киберпреступностью ГУМВД Украины в Запорожской области И. Ворона.

Мошенников, которые работают с банковскими карточками, называют кардерами. Они постоянно изобретают различные пути для получения финансовой или личной информации о людях, чтобы дальше воровать денежные средства.

«Так называемые “кардеры” используют специальные приборы: скиммеры, накладки. Скиммер – это устройство для считывания информации с платежной карточки, – говорит И. Ворона. – Он устанавливается на картоприемник на самом банкомате. Накладки устанавливаются на клавиатуру банкомата. В дальнейшем мошенники получают благодаря этим приборам всю информацию, включая пароль. Информация с помощью приборов передается им на мобильный телефон или электронную почту».

Иногда мошенникам достаточно подержать в руках банковскую карточку, чтобы сфотографировать или переписать номер счета и CV-код – четырехзначный код, который находится на обратной стороне карты. В дальнейшем это дает возможность осуществить списание средств при расчете в интернет-магазине.

По словам И. Вороны, мошенники также действуют по такой схеме: в Интернете находят объявления о необходимости предоставления материальной помощи на лечение. Там, как правило, указываются банковские реквизиты, адрес, телефон. Мошенники связываются с жертвой и сообщают, что намерены перечислить материальную помощь. Правда, для этого просят указать пароль, который будет послан банком в смс-сообщении на телефон жертвы. Жертва соглашается, называет пароль и мошенники спокойно снимают денежные средства без самой карты.

Самым популярным видом мошенничества является обман в интернет-магазинах, на аукционах. Продавцы требуют, чтобы покупатель перевел на счет предоплату, только после этого он сможет получить свой товар. Естественно, никакого товара никто в дальнейшем не получает.

Схемы мошенничества в Запорожье: как не попасться «на крючок»

Управлением также принимаются меры по очистке сети Интернет от противоправного контента, а именно: распространения программного обеспечения, аудиовизуальных произведений, продукции, которая размещается с нарушением авторских смежных прав, также продукции порнографического характера, лекарственных препаратов и т. д.

Для примера, в текущем году было выявлено три факта реализации через Интернет холодного оружия: это клинки, ножи времен ВОВ. Открыты уголовные дела в отношении этих лиц по статье 263 УКУ.

«В течение двух месяцев 2013 г. в сфере использования электронно-вычислительных машин по инициативе подразделения УБК в Единый реестр досудебных расследований внесено 39 информации, по которым начато досудебное расследование. Из них по ст. 190 (мошенничество) – 14, ст. 301 (сбыт и распространение порнографических предметов) – 3 факта, ст. 203 ч. 2. (занятие игорным бизнесом) – 4, ст. 361 (несанкционированное вмешательство в работу электронно-вычислительных машин) – 6, ст. 231 (незаконный сбор с целью использования ведомостей, что составляют коммерческую или банковскую тайну) – 1, ст. 176 (нарушение авторского права и смежных прав) – 6, ст. 263 (сбыт холодного оружия) – 3, – сообщил И. Ворона. – 12 лицам сообщено о подозрении в совершении преступлений. На рассмотрение в суд направлено 6 обвинительных актов».

Также в феврале прошлого года в суд было направлено уголовное дело в отношении ОПГ, в состав которой входили жители Запорожской области – молодые люди, которые имеют образование в сфере IT-технологий. Они похищали чужую информацию и занимались воровством денежных средств. Сумма убытков от деятельности этой ОПГ составила 100 тыс. грн. Судом были рассмотрены материалы уголовного дела и признаки ОПГ подтверждены.

«В ноябре 2012 г. сотрудники УБК разоблачили группу лиц, которые на протяжении апреля–ноября 2012 г. осуществляли преступную деятельность, направленную на завладение денежными средствами жителей разных регионов Украины путем обмана и злоупотреблением доверием, – говорит И. Ворона. – Они действовали по такой схеме: один из фигурантов размещал объявления на сайте Auto.gia о продаже транспортных средств по заниженным ценам. Во время телефонного разговора злодей настаивал на перечислении задатка. Это средства в сумме от 800 грн до 4 тыс. грн. После этого перечисленные деньги обналачивались через банковские учреждения и, конечно, жертвы не получали автомобиль. По указанному факту возбуждено

уголовное дело по ч. 3 ст. 190 УК. Сумма убытков составила свыше 100 тыс. грн».

Как уберечь себя?

В первую очередь необходимо внимательно относиться к безопасности во время пользования электронными сервисами и не размещать персональную информацию в свободном доступе. Не сообщать информацию о платежной карточке через сеть Интернет, не сообщать пин-коды, пароли, срок действия платежной карточки, кредиты, лимиты, персональные данные и др.

Также И. Ворона советует для оплаты товаров через Интернет завести отдельную карточку, где будет установлен предельный лимит, чтобы она использовалась только для приобретения товаров на сайтах. Также необходимо использовать страницы только известных и проверенных интернет-магазинов. Перед покупкой желательно почитать отзывы на форумах. Следует устанавливать на компьютеры современное антивирусное обеспечение и регулярно осуществлять его обновление (*Киберпреступность по-запорожски: новые схемы и уловки злодеев // Репортер Запорожья (<http://reporter-ua.com/2013/03/11/kiberprestupnost-po-zaporozhski-novye-skhemy-i-ulovki-zlodeev>). – 2013. – 11.03*).

Украина вошла в пятерку стран-источников кибератак.

Ведущий немецкий оператор связи Deutsche Telekom визуализировал карту стран-источников кибератак, на которой Украина оказалась на четвертом месте после России, Тайваня и Германии.

Об этом сообщает специализированное интернет-издание AIN.UA.

«За последний месяц с украинских серверов было совершено 566 531 атак», – говорится в сообщении.

В Deutsche Telekom подчеркивают, что число интернет-угроз постоянно растет – ежедневно обнаруживают около 200 тыс. новых образцов вредоносных. Только в ловушках Deutsche Telekom собираются записи о 450 тыс. атак в день (*Украина вошла в 5-ку стран-источников кибератак // Эксперт-центр (<http://expert.org.ua/statias/?st=2&id=105273>). – 2013. – 11.03*).

78 % скачанного из Интернета пиратского ПО содержит шпионские программы.

Каждый третий пользователь компьютера, который загружает нелицензионное программное обеспечение, надеясь сэкономить, рискует установить вредоносную программу. К такому выводу пришла международная компания IDC в ходе исследования «Опасный мир контрафактного и пиратского программного обеспечения».

В результате таких заражений пользователи потратят 1,5 млрд часов и 22 млрд дол. для выявления, ремонта и восстановления систем (в лабораториях восстановления данных) после воздействия вредоносных программ. А предприятиям борьба с вредным воздействием, вызванным кибератакой, будет стоить 114 млрд дол. Отчет IDC опубликован в День безопасности (Play it safe) – это глобальная инициатива Microsoft, призвана привлечь внимание к проблеме серьезных рисков для домашних пользователей и бизнеса через использование нелегального программного обеспечения.

В глобальном исследовании проанализированы 270 сайтов и peer-to-peer (P2P) сетей, 108 загрузок программного обеспечения и 155 компакт-дисков или DVD-дисков, а также опрошены 2077 потребителей и 258 системных администраторов и руководителей в Бразилии, Китае, Германии, Индии, Мексике, Польше, России, Таиланде, Великобритании и Соединенных Штатах.

Исследователи обнаружили, что 45 % контрафактного программного обеспечения было скачано из Интернета, и 78 % этого ПО содержало различные типы шпионских программ, в то время как 36 % – трояны и рекламные программы.

«Киберпреступники взламывают код и “вшивают” в него вредоносные программы, – рассказывает Д. Финн, помощник генерального советника в Центре киберпреступности Microsoft. – Некоторые злоумышленники записывают каждое нажатие клавиш человеком, что позволяет похищать персональную и финансовую информацию жертв или дистанционно включать микрофон и видекамеры зараженного компьютера, что дает возможность наблюдать за событиями в комнате или зале совещаний. Лучший способ обезопасить себя и свое имущество от угроз вредоносного ПО – выбирать подлинное программное обеспечение при покупке компьютера».

«Результаты исследования еще раз подтверждают, что пользователи и бизнес подвергаются опасности, используя контрафактное программное обеспечение, – отметил Д. Ганц, директор по исследованиям IDC. – Некоторые выбирают пиратские программы в целях экономии, однако использование нелегальным, уязвимым к вирусам ПО, подвергает угрозе, в том числе и финансовой, как предприятия, так и обычных пользователей».

Среди главных выводов исследования можно выделить следующие:

- 64 % респондентов, которые использовали нелегальное ПО, сталкивались проблемами безопасности;
- В 45 % случаях нелегальные программы тормозили работу компьютера, поэтому их приходилось удалять;
- 48 % респондентов признали, что, используя пиратское ПО, больше волновались из-за риска потери информации;
- 29 % пользователей больше всего боялись потери личных данных.

Заражение нелицензионного ПО вредоносными программами стало новым способом для киберпреступников получения выгоды от пользователей, незнакомых с потенциальными рисками.

Исследование IDC также обнаружило частые случаи установки ПО пользователями на свои рабочие компьютеры, что является еще одним способом проникновения вредоносных программ в корпоративную экосистему. 38 % системных администраторов подтверждают такую проблему, а 57 % офисных работников признают, что скачивают программы для личного пользования на работе. В то же время респонденты отметили, что лишь 30 % установленного ПО не было зараженным. 65 % системных администраторов согласны, что самостоятельная установка ПО работниками повышает риски безопасности предприятия. Таким образом, загрузки приложений сотрудниками может быть слабым звеном в обеспечении защищенности корпоративной сети.

«Сегодня большинство IT-специалистов считают киберугрозы наиболее опасными для бизнеса после нестабильной экономической ситуации, – комментирует А. Урденко, Директор департамента исследований компьютерной техники, программных продуктов и телекоммуникационных систем АБ “Традиции профессионалов”. – Эксплойты – это наиболее распространенный способ проникновения вредоносного кода на компьютер пользователей. В результате чего можно потерять конфиденциальную информацию, частные и финансовые данные, а также нанести вред ПК. Использование нелицензионного ПО только увеличивает шансы заражения компьютера вредоносными программами, поскольку оно является неофициальным, вовремя не обновляется и может заранее содержать вредоносный код».

Узнать больше о вредоносных программах и проверить свой компьютер пользователи могут на сайте www.microsoft.com/security; если будут найдены вирусы, ресурс предложит их удалить. Пользователям, которые покупают новый компьютер, рекомендуется обращаться к надежному продавцу с хорошей репутацией, чтобы убедиться, что они покупают лицензионное программное обеспечение Microsoft (78 % *скачанного из Интернета пиратского ПО содержит шпионские программы // ООО «Центр информационной безопасности» (<http://www.bezpeka.com/ru/news/2013/03/11/78-pc-of-pirated-software-infected.html>). – 2013. – 11.03).*

Хакеры взломали Chrome, Firefox, IE 10 и Java на конкурсе Pwn2Own.

В рамках конкурса Pwn2Own участники использовали ранее неизвестные уязвимости в Chrome, Firefox, IE 10, Windows 8 и Java. Атаки удалось осуществить посредством обработки в браузере специально созданной веб-страницы, открытие которой завершилось получением

полного контроля над системой. Хакеры проводили взломы самых последних и стабильных версий браузеров и операционных систем Windows 7, 8 и Mac OS X Mountain Lion.

Подробности об обнаруженных уязвимостях будут опубликованы после того, как производители выпустят устранения для них.

Призовой фонд конкурса Pwn2Own в этом году был значительно увеличен. В частности, вознаграждение за взлом Chrome составляет 100 тыс. дол., за взлом IE – 75 тыс. дол., за взлом Firefox – 60 тыс. дол., за взлом Safari – 65 тыс. дол.

Известно, что взлом Windows 8 осуществлялся на планшете Surface Pro посредством эксплуатации двух уязвимостей нулевого дня в IE 10, а также новой техники выхода за пределы песочницы.

Участники конкурса признались, что в этом году на поиск уязвимостей и написание эксплоитов было потрачено несколько месяцев (*Хакеры взломали Chrome, Firefox, IE 10 и Java на конкурсе Pwn2Own // ООО «Центр информационной безопасности»* (<http://www.bezpeka.com/ru/news/2013/03/11/Pwn2Own.html>). – 2013. – 11.03).

Анонимный хакер опубликовал в сети финансовые данные около десятка американских знаменитостей и политических деятелей, среди которых экс-госсекретарь США Х. Клинтон, американский вице-президент Д. Байден, светские львицы К. Кардашьян и П. Хилтон, а также супружеская пара Jay-Z и Бейонси. Об этом сообщает Times Live со ссылкой на американские таблоиды.

По данным издания, ФБР и полиция Лос-Анджелеса расследуют хакерскую атаку, в результате которой в Интернет были выложены номера социального страхования, информация о выплатах по ипотеке, банковских счетах и кредитах на автомобили, а также данные кредитных карт.

Среди жертв хакеров также оказались директор ФБР Р. Мюллер, генеральный прокурор Э. Холдер, начальник полиции Лос-Анджелеса Ч. Бек, а также актеры Э. Катчер и М. Гибсон (*Хакер выложил в сеть финансовые данные американских знаменитостей и политиков // Версии.com* (<http://www.versii.com.ua/news/274831/>). – 2013. – 13.03).

Обнаружена новая вирусная программа, перехватывающая входящие SMS-сообщения при пользовании мобильными устройствами под управлением ОС Android.

Независимый эксперт по компьютерной безопасности Б. Кребс нашел на одном из интернет-форумов выставленную на продажу программу, пересылающую тексты входящих SMS организаторам вирусной атаки, «сливая» конфиденциальную информацию пользователя – например, данные для интернет-банкинга.

Часть банковских учреждений во многих странах используют двухуровневую аутентификацию – клиенту для подтверждения платежа нужно вводить не только пароль, но еще и особый SMS-код.

Вирус Perkele (название программы переводится как финское нецензурное ругательство) действует совместно с другой вредоносной программой, которая устанавливает вирус и подменяет инструкции на платежной веб-странице – в результате пользователя просят установить на телефон «специальную защищенную программу для Android», под видом которой и скрывается Perkele.

Анализируя данные за прошлый год, эксперты по антивирусной безопасности сходятся во мнении: лидером по количеству атак остаётся ОС Android. Учитывая возможности мобильных Android-устройств и увеличение числа их пользователей, многие специалисты прогнозируют дальнейший рост популярности данной ОС у киберпреступников.

Финский антивирусный вендор F-Secure на днях опубликовал отчет, согласно которому в 2012 г. открытая операционная система Android показала стремительный рост не только по популярности, но и по количеству выпускаемого вредоносного ПО. В 2012 г. Android стала целью для 79 % выпускаемого вредоносного программного обеспечения. Годом ранее этот показатель составлял 65 %.

Только в IV квартале на долю Android пришлось 96 абсолютно новых вирусных семейств, а с учетом вариантов вредоносных кодов, количество новых угроз идет на сотни. F-Secure отмечает, что в последнем квартале 2012 г. самыми популярными Android-вредоносами стали разнообразные коды, выполняющие те или иные операции с SMS-сообщениями и премиальными SMS-номерами. Из 96 новых семейств 21 было ориентировано на тайную отправку коротких сообщений на короткие номера.

Также набирают популярность среди вирусописателей и сравнительно новые SMS-вредоносы, которые сами создают короткие сообщения и используют методы социальной инженерии, чтобы ввести пользователей в заблуждение и тем или иным способом вынудить его совершить платеж на счет мошенников. Также достаточно популярными являются вредоносные коды, ворующие мобильные банковские реквизиты и передающие их в фоновом режиме мошенникам.

Чтобы как-то снизить опасность, F-Secure рекомендует пользователям регулярно обновлять свои Android-устройства, а также регулярно обновлять антивирусное ПО и сканировать систему на предмет наличия вредоносных кодов в смартфоне (*Новый Android-вредонос Perkele перехватывает короткие сообщения // ООО «Центр информационной безопасности» (<http://www.bezpeka.com/ru/news/2013/03/13/Perkele.html>). – 2013. – 13.03).*

В 2013 г. Независимая ассоциация банков Украины продолжит работу в сфере повышения финансовой грамотности населения. Об этом,

как передает корреспондент ForUm'a, заявил руководитель проекта НАБУ «Финансовая грамотность» Р. Кобец.

«Прежде всего, мы запустим общедоступные веб-ресурсы. Так, уже создан портал “Антикибер”, на котором представлено единство интересов представителей банковского сообщества и клиентов, которые не хотят, чтобы в Украине развивалось мошенничество в сфере банковских услуг», – сказал он.

Продолжением этой деятельности, по его словам, станет создание интернет-ресурса «Финансовая грамотность».

«На этом ресурсе мы хотим разместить информацию, учитывая возрастной показатель пользователей (от детей до пенсионеров). На портале будет не только информация о банковских ресурсах, но и базовые знания о них: об управлении семейным бюджетом, как делать большие покупки, как не влезать в долги и т. д.», – сказал он.

Помимо этого, по словам Р. Кобца, в нынешнем году стартует проект, в рамках которого в 20 городах Украины будут проведены комплексные мероприятия по повышению финансовой грамотности.

«Эти мероприятия рассчитаны на разные категории граждан: для детей, молодёжи, населения старшего возраста. Мы надеемся, что это поспособствует возвращению доверия к деятельности финансовых учреждений», – подчеркнул руководитель проекта.

Он также добавил, что, в соответствии с этим проектом, значительное внимание будет уделено работе с журналистами и банками.

Р. Кобец отметил, что финграмотность следует рассматривать как часть соцработы и в перспективе стоило бы перенимать опыт других стран, где работают соцработники с категориями граждан групп риска (*НАБУ создаст веб-ресурсы для повышения финграмотности среди населения // ForUm (<http://www.for-ua.com/economics/2013/03/13/152938.html>). – 2013. – 13.03*).

Киберпреступники заводят в соцсетях странички от имени известных брендов.

До Украины добралось новое мошенничество – аферисты создают в социальных сетях фальшивые страницы именитых компаний, предлагая всем, кто отметит ее кнопкой like дорогие подарки. Таким образом, мошенники недобросовестно увеличивают количество подписчиков.

Суть мошенничества заключается в следующем – в популярной социальной сети, типа Facebook заводят страницу известного бренда или компании. На ней размещается «официальное уведомление» о «конкурсе». Каждый человек, который подпишется на страницу и поставит ей like получает шанс выиграть дорогостоящие товары от указанного бренда, сообщает Waffles At Noon. В частности, разыгрываются дорогие наушники от Beats Electronics и iPad Mini от Apple. Само время розыгрыша призов отстоит от текущей даты примерно на месяц.

Пример фальшивой страницы – товар не может быть продан, поскольку нарушена целостность упаковки

Чтобы избежать подозрений пользователей в том, что бренды предлагают слишком уж дорогие подарки, мошенники уточняют, что все разыгрываемые наушники не могут быть проданы из-за нарушения целостности упаковки.

Представители вышеупомянутых компаний уже обратились с официальным запросом к руководству соцсети Facebook с сообщением о том, что они не проводят никаких конкурсов и розыгрышей. Кроме того, корпорации уже разослали соответствующие уведомления другим крупнейшим социальным сетям.

Эксперты уже высказали предположение, что данные страницы являются частью какой-то крупной мошеннической схемы по недобросовестному увеличению подписчиков на странице. Возможно, после набора подписчиков страница будет продана и переименована (*Киберпреступники заводят в соцсетях странички от имени известных брендов // InternetUA (<http://internetua.com/kiberprestupniki-zavodyat-v-socsetyah-stranicski-ot-imeni-izvestnih-brendov>). – 2013. – 14.03*).

Ботнет Andromeda возвращается. Следы присутствия ботсети были обнаружены в одной из спам-рассылок.

Как сообщают исследователи компании Trend Micro, в одной из последних обнаруженных спам-рассылок присутствуют следы ботнета Andromeda.

По словам экспертов, спам-сообщения содержат вредоносные вложения, либо ссылки на скомпрометированные веб-сайты, загружающие на компьютер жертвы набор эксплоитов Blackhole (ВНЕК).

Следует напомнить, что ботнет Andromeda обнаружен еще в 2011 г., может включать в себя несколько различных модулей, среди которых кейлогеры, руткиты, а также прокси-модули SOCKS4.

Как и обычный бэкдор, вирус может загружать и исполнять на компьютере жертвы различные файлы, а также обновлять себя или удалять в случае необходимости.

Исследователи отмечают, что различные версии приложений, используемых ботсетью Andromeda, хакеры продают в сети Интернет за 300–500 дол., а наибольшее количество инфицированных компьютеров было обнаружено в Австралии, Турции и Германии.

По данным экспертов, на этот раз Andromeda распространяется при помощи съемных носителей. Вместо простого распространения своих копий, вирус разделяет компоненты файлов, усложняя анализ и обнаружение.

Последний обнаруженный исследователями образец вируса обладает способностью открывать и прослушивать TCP-порт 8000 и запускать командную строку (cmd.exe). После подключения к удаленной системе,

злоумышленник может выполнить произвольные команды и получить полный доступ к инфицированному компьютеру.

Помимо этого, Andromeda может использовать собственные API, которые внедряются в обычные процессы. Подобная техника ранее была замечена в поведении вирусов DUQU и KULUOZ (*Ботнет Andromeda возвращается // InternetUA (<http://internetua.com/botnet-Andromeda-vozvrashaetsya>). – 2013. – 15.03*).

В последнее время хакеры чаще атакуют мобильные устройства.

Эксперты подготовили отчет о вредоносной активности, в котором указали на появление новых приемов в проведении атак на мобильные устройства.

Исследователи антивирусной компании McAfee подготовили отчет о тенденциях распространения мобильных угроз в 2013 г.

По данным экспертов, в последнее время увеличилось количество вредоносных программ, в том числе фишинговых сообщений, мошеннических схем, инструментов тайпсквоттинга и «попутных загрузок».

Исследователи установили, что за последние три квартала количество атак на мобильные платформы, при проведении которых злоумышленники используют легальные ресурсы, увеличилось более чем в три раза. Так, на 75 % увеличилось количество атак, проведенных с использованием приложений, размещенных в Google Play, почти 25 % опасных приложений содержат также подозрительный URL-адрес, а 40 % вирусов атакуют систему сразу в нескольких направлениях.

Так, используя опасные приложения, хакеры похищают важные конфиденциальные данные жертв, адреса электронной почты, а сопоставляя полученную информацию с данными о местоположении владельца скомпрометированного гаджета, могут составить полный портрет жертвы.

Кроме того, злоумышленники активно осуществляют спам-рассылки, в результате чего жертвы, сами того не подозревая, могут подписаться на платные сервисы, сделать устройства частью ботнета или предоставить хакеру полный дистанционный доступ.

Популярными среди киберпреступников в отчетном периоде остаются загрузки и руткиты, которые используются для рассылки SMS-сообщений от имени жертвы на платные номера, размещения кликфродов, рассылки нежелательных сообщений, кражи данных и попытки банковских махинаций.

Эксперты также сообщают, что злоумышленники активно применяют тайпсквоттинг – рассчитывая воспользоваться опечатками или орфографическими ошибками жертв при вводе URL-адресов популярных сайтов и известных брендов.

Помимо этого, исследователи отмечают увеличение количества «попутных загрузок», в результате которых вредоносный код загружается автоматически без ведома жертвы вместе с легитимным приложением. В

случае запуска пользователем этого приложения, киберпреступник получает удаленный доступ к мобильному устройству (*В последнее время хакеры чаще атакуют мобильные устройства // InternetUA (http://internetua.com/v-poslednee-vremya-hakeri-csasxe-atakuuat-mobilnie-ustroistva). – 2013. – 15.03).*

Разгадана тайна вируса, поразившего Apple.

Исследователям в области компьютерной безопасности удалось идентифицировать новый вирус для Mac, который недавно поразил компьютеры сотрудников Apple, Facebook и Twitter, а также множества других компаний. Троян называется Pintsized, и он настолько силен, что способен обойти систему защиты Gatekeeper в OS X.

Компания Intego, занимающаяся разработкой антивирусов для Mac, сообщает, что троян маскируется на зараженных машинах под Linux-приложение для печати под названием cupsd. Специалистам еще предстоит выяснить, каким образом вредоносное ПО обходит защиту Gatekeeper.

После проникновения на компьютер Pintsized создает оболочку, с помощью которой злоумышленники могут получать доступ к компьютерам пользователей с удаленного сервера. Троян использует модифицированную версию утилиты OpenSSH для шифрования трафика, что позволяет ему перемещаться по сетям незамеченным.

Одним из доменных имен, к которому привязан такой сервис, являлся corp-aapl.com. Сервер привлек внимание сотрудников отдела безопасности Facebook, после того как они поняли, что внутренняя сеть компании была атакована вирусом. Когда специалисты получили контроль над сервером, они выяснили, что злоумышленники уже успели атаковать с него компьютеры сотрудников Apple, Twitter и Microsoft, воспользовавшись тем же самым паттерном.

На текущий момент пока имеется мало информации о том, где и как можно подцепить эту заразу и, следовательно, как от нее уберечься. Однако известно, что троян загружался на компьютеры пользователей после посещения некоторых сайтов, посвященных разработке для iOS и Android. В частности, речь идет о сайте iphonedevsdev.com, про который стало доподлинно известно, что он заражен. Примечательно, что трояном этот сайт заражал не все компьютеры, а только некоторые (*Разгадана тайна вируса, поразившего Apple // InternetUA (http://internetua.com/razgadana-taina-virusa--porazivshego-Apple). – 2013. – 15.03).*

В iOS обнаружена серьезная уязвимость.

Apple всегда стремилась позиционировать свои девайсы, как «наиболее безопасные» в сравнении с устройствами, работающими под управлением Android. Как оказалось, это не совсем так.

Специалистам по безопасности из израильской компании Skycure Security удалось найти весьма серьезную уязвимость в iOS, информация о которой была опубликована в их блоге.

«Специалисты из Skycure Security продемонстрировали способ использования профилей iOS для обхода защиты Apple от вредоносных программ», – сообщает CNET.

Напомним, что устройства с iOS защищены за счет наличия так называемой «песочницы», которая позволяет ограничить права приложений. Однако в операционной системе также присутствует возможность установки дополнительных профилей, используемых некоторыми разработчиками и операторами для настройки VPN и других сервисов. Именно при помощи таких профилей злоумышленники могут получить доступ к данным пользователей, а также сделать идевайсы уязвимыми для атак через Wi-Fi.

Специалисты из Skycure Security рекомендуют пользователям устанавливать сертификаты лишь от проверенных разработчиков (***В iOS обнаружена серьезная уязвимость // InternetUA (<http://internetua.com/v-ios-obnarujena-serezhnaya-uyazvimost>). – 2013. – 15.03***).

КНДР обвинил США в кибератаках.

Центральное телеграфное агентство Кореи (ЦТАК), государственное информагентство КНДР, обвинило США в хакерских атаках на корейские интернет-ресурсы. Об этом 15 марта 2013 г. сообщает ИТАР-ТАСС.

В заявлении ЦТАК говорится, что США и ее союзники пытаются «изолировать и задушить» КНДР. Агентство обращает внимание, что кибератаки начались во время военных учений в Южной Корее, в которых принимают участие американские военные.

ЦТАК подчеркивает, что КНДР не будет наблюдать за тем, как «враждебные силы расширяют масштабы кибератак на государственные интернет-ресурсы страны» и предпримет необходимые ответные меры. В чем они будут заключаться, не уточняется.

Из-за кибератак 13 марта в КНДР перестала работать система выхода в Интернет. Из-за этого пострадал ряд местных и иностранных компаний и СМИ, включая ИТАР-ТАСС и авиакомпанию Air Koryo, запустившую онлайн-продажу билетов в октябре 2012 г.

Кибератаки помешали и туристам, находящимся в Северной Корее, выходить в Интернет через мобильные устройства. Возможность подключаться к сети с помощью 3g-сети появилась у иностранцев в марте 2013 г. Местные жители практически не имеют возможности выхода в Интернет, но, как отмечает ТАСС, в Корее действует собственная сеть, призванная стать эквивалентом глобальной сети.

Учения в Южной Корее начались 1 марта. Руководство КНДР выступило против них и отменило перемирие с соседом, заключенное после Корейской войны 1950–1953 гг. Впрочем, Пхеньян ранее неоднократно

разрывал пакт о ненападении. Мирное соглашение между двумя государствами так и не было подписано (*КНДР обвинил США в кибератаках // InternetUA (<http://internetua.com/kndr-obvinil-ssha-v-kiberatakah>).* – 2013. – 15.03).

Trend Micro: бойтесь не китайских хакеров, а русских.

Технический директор антивирусной компании Trend Micro Р. Генес говорит, что опасения бизнеса в связи с участвовавшими атаками, спонсируемыми государствами, в реальности блекнут с масштабами хищений, совершаемых хакерами из России и стран СНГ. По его словам, подавляющему большинству частных пользователей и компаний малого и среднего бизнеса не следует опасаться так называемых «госхакеров», а вот хакеров из России и стран СНГ стоит.

«Когда я вижу большую шумиху вокруг отчетов, наподобие тех, что был недавно опубликован компанией Mandiant, обличающий китайских хакеров, то в большинстве случаев соглашаюсь, что китайцы действительно занимаются корпоративным шпионажем. Но вы думаете, что американцы не занимаются? Или русские?» – говорит Р. Генес. «Лично меня больше тревожит активность русских хакеров. Они занимаются киберпреступностью очень давно, задолго до того, как китайцы сели за компьютеры. Этих опасных ребят частенько нанимают для совершения разных грабежей. Все наши последние данные однозначно говорят о том, что наиболее сложные атаки исходят из России».

Некоторое время назад компания Mandiant опубликовала статистический отчет, в котором говорилось, что несколько сложных АРТ-атак (Advanced Persistent Thread) ведут в китайскую армию. Отчет вызвал публичный обмен обвинениями между Вашингтоном и Пекином. Генес отметил, что в последнее время все больше специалистов по ИТ-безопасности начинают спекулировать термином АРТ.

«Я ненавижу термин АРТ. На прошлой неделе я был в RSA, и там все кому не лень твердили о том, что АРТ повсюду. Тот факт, что подобные атаки вызывают большой интерес, невозможно оспорить, но не следует преувеличивать масштабы подобных атак. Многие коды, изначально созданные для АРТ-атак, потерпели провал – Stuxnet, Red October и другие, все они были созданы для удара по конкретным целям, но распространились слишком широко и не выполнили своих задач. Код хорош тогда, когда вы его не видите», – полагает он.

СТО Trend Micro говорит, что многие киберпреступники используют модифицированные коды для атак, а их довольно легко детектировать. В то же время оригинальная платформа вредоноса зачастую создается в «русском подполье», а уже потом растекается по всему миру. Р. Генес говорит, что на сегодня практически все ИТ-специалисты согласны с тем, что от таргетированных атак невозможно полностью защититься. «Если кто-то на

протяжении нескольких лет пытается взлезть в вашу сеть, рано или поздно он это сделает и неважно будет ли это сделано по электронной почте, через USB-накопитель или как-то еще», – уверен специалист.

Еще одним моментом, вызывающим опасение топ-менеджера антивирусной компании, является растущая доступность очень мощных инфраструктурных решений для все возрастающего числа хакеров.

«Раньше клиенты платили нам за то, чтобы мы защитили их ресурсы от атак. Сейчас – чтобы мы помогли минимизировать ущерб от атак и найти следы атаковавших злоумышленников», – признает Р. Генес.

По его словам, еще одной животрепещущей проблемой для бизнеса является отсутствие единых норм и требований по ИТ-безопасности. Р. Генес говорит, что в настоящее время Евросоюз движется в этом направлении, но до завершения этого пути еще далеко (*Trend Micro: бойтесь не китайских хакеров, а русских // InternetUA (<http://internetua.com/Trend-Micro--boites-ne-kitaiskih-hakerov--a-russkih>). – 2013. – 15.03*).

Взлом TLS и SSL через уязвимость в шифре RC4.

На этой неделе в Сингапуре прошла криптографическая конференция Fast Software Encryption. Главным событием стало выступление Д. Бернштейна, профессора университета Иллинойса, который представил новую технику для вскрытия протоколов Transport Layer Security (TLS) и Secure Sockets Layer (SSL), если в них используется шифр RC4: слайды презентации (pdf).

Шифр RC4, созданный в 1987 г., до сих пор широко используется и считается одним из самых популярных и рекомендуемых шифров. Слабости RC4 давно и хорошо известны, но до практических реализаций атаки на TLS дело пока что не доходило, хотя AES и Triple DES уже скомпрометированы в атаках BEAST и Lucky 13. Теперь дошло дело до RC4, впервые опубликован реальный и доступный способ такой атаки.

RC4 (Rivest Cipher 4) – популярный потоковый шифр, созданный легендарным криптографом Р. Ривестом, широко применяется в SSL, TLS и алгоритме безопасности беспроводных сетей WEP. Алгоритм RC4, как и любой потоковый шифр, строится на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Длина ключа может составлять от 40 до 256 бит. Основные преимущества шифра – высокая скорость работы и переменный размер ключа.

Уязвимость RC4 связана с недостаточной случайностью потока битов, которым скремблируется сообщение. Прогоняя через него одно сообщение много раз, удалось выявить достаточное количество повторяющихся паттернов для восстановления исходного сообщения.

Для атаки нужно прогнать через шифр гигантский объем данных. В текущей реализации взлом TLS занимает до 32 часов, но злоумышленник может использовать различные способы для оптимизации процесса.

Например, это может быть баннер на сайте с большой посещаемостью или фрагмент кода, который добавляют каждому пользователю на уровне маршрутизатора (*Взлом TLS и SSL через уязвимость в шифре RC4 // InternetUA (<http://internetua.com/vzлом-TLS-i-SSL-cserez-uyazvимость-v-shifre-RC4>). – 2013. – 16.03*).

Троян FinFisher используется властями стран для шпионажа.

Эксперты обнаружили C&C-серверы вредоносного ПО в 25 странах.

Специалисты лаборатории Citizen Lab при Университете Торонто сообщили о троянском программном обеспечении FinFisher, используемом правительствами стран для шпионской деятельности. Эксперты заявили, что обнаружили C&C-серверы бэкдоров FinSpy в 25 странах, в том числе в Австралии, Канаде, Эстонии, Германии, Великобритании и США.

FinFisher – это ПО, разработанное Gamma International для совершения удаленного вторжения и наблюдения, и производится исключительно для правоохранительных органов и спецслужб Великобритании. Исследователи отметили, что на C&C-серверы FinFisher стекаются данные печатных изданий, сообщения в Skype, а также аудиозаписи, перехваченные вредоносным ПО с микрофонов компьютеров. В Мексике, Бангладеш, Малайзии, Сербии, Бахрейне и Вьетнаме FinFisher применялся в отношении политических оппонентов.

Исследователи заявили, что в настоящее время FinFisher применяется в Эфиопии. Так, в августе прошлого года эксперты обнаружили образцы вредоносного ПО FinSpy, использующего фотографии участников эфиопской оппозиционной группы Ginbot 7 в качестве приманки. ПО связывается с C&C-серверами FinSpy, расположенными в Эфиопии. Его можно обнаружить по следующему адресу государственной телекоммуникационной компании Эфиопии Ethio Telecom:

```
IP: 213.55.99.74
route: 213.55.99.0/24
descr: Ethio Telecom
origin: AS24757
mnt-by: ETC-MNT
member-of: rs-ethiotelecom
source: RIPE # Filtered
```

Вредоносная программа перемещает себя в JPG--изображение, а затем исполняется ничего не подозревающими пользователями. ПО загружается при помощи буткита SHA-256: ba21e452ee5ff3478f21b293a134b30ebf6b7f4ec03f8c8153202a740d7978b2 и использует драйвер .sys – SHA-256: 62bde3bac3782d36f9f2e56db097a4672e70463e11971fad5de060b191efb196

(Троян FinFisher используется властями стран для шпионажа //

InternetUA (http://internetua.com/troyan-FinFisher-ispolzuetiya-vlastyami-stran-dlya-shpionaja). – 2013. – 16.03).

АНБ США готовит команду противодействия на случай кибервойны. Спецагенты готовятся проводить масштабные операции по противодействию агрессии в киберпространстве.

По словам руководителя Агентства национальной безопасности США К. Александера, спецслужбы страны готовят специальные подразделения на случай возникновения угрозы кибервойны. Об этом глава ведомства рассказал представителям комитета Конгресса по делам вооружения в среду, 13 марта.

К. Александер отметил, что АНБ готовит группу специалистов, которые «будут защищать нацию в цифровом пространстве». Это будет агрессивная группа, которую власти смогут привлекать в случае возникновения угрозы масштабных кибератак. «Члены 13 команд готовятся проводить спецоперации в одиночку», – пояснил генерал.

По данным the New York Times, К. Александер рассказал о подготовке 27 групп спецагентов, которые будут «защищать американские сети в киберпространстве».

Чиновник не раскрыл детали проекта, однако отметил, что подготовка спецкадров является одним из приоритетных заданий АНБ. Кроме того, К. Александер заявил, что наиболее успешным оказался мониторинг входящего в США трафика, который позволяет предотвращать атаки на объекты критической инфраструктуры страны (**АНБ США готовит команду противодействия на случай кибервойны // InternetUA (http://internetua.com/anb-ssha-gotovit-komandu-protivodeistviya-na-slucsai-kibervoini). – 2013. – 16.03).**

В сети появились фальшивые обновления для браузеров с вредоносным ПО.

Русскоязычный сегмент сети захлестнула волна фальшивых обновлений браузеров. Под их видом киберпреступники устанавливают на компьютеры пользователей вредоносное программное обеспечение.

Многочисленные отзывы русскоязычного сегмента сети и данные сервиса Яндекс.Блоги указывают на то, что в Рунете активизировались мошенники, занимающиеся распространением вредоносного программного обеспечения под видом обновлений для популярных браузеров.

Распространение вредоносного софта ведется с помощью стилизованного оформления, схожего с официальными экранами обновления браузеров Internet Explorer, Firefox, Chrome, Safari и Opera. Для максимальной убедительности преступники имитируют реальный процесс инсталляции обновлений, вводя тем самым в заблуждение невнимательных интернет-

пользователей. Предупреждаем, что такое «обновление» на самом деле устанавливает на компьютер вредоносное программное обеспечение.

Специалисты по безопасности уже призвали пользователей повысить внимание и тестировать антивирусами любой контент, загружаемый из сети. В частности, эксперты по безопасности из Group-IB создали сайт, позволяющий протестировать любую страничку на предмет надежности.

В настоящее время «лечения» для фальшивых обновлений еще не найдено (***В сети появились фальшивые обновления для браузеров с вредоносным ПО // InternetUA (<http://internetua.com/v-seti-poyavilis-falshivie-obnovleniya-dlya-brauzerov-s-vredonosnim-po>). – 2013. – 17.03).***