

**СОЦІАЛЬНІ МЕРЕЖІ
ЯК ЧИННИК
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

*Огляд інтернет-ресурсів
(30.12–12.01)*

2014 № 1

Соціальні мережі як чинник інформаційної безпеки

Інформаційно-аналітичний бюлетень
Додаток до журналу «Україна: події, факти, коментарі»
Огляд інтернет-ресурсів
(30.12–12.01)
№ 1

Засновники:

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

Головний редактор

В. Горовий, д-р іст. наук, проф.

Редакційна колегія:

Т. Касаткіна, Л. Чуприна

Заснований у 2011 році
Виходить двічі на місяць

© Національна бібліотека України
імені В. І. Вернадського, 2014

Київ 2014

ЗМІСТ

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ.....	4
СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА.....	10
БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ	13
СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ.....	21
Інформаційно-психологічний вплив мережевого спілкування на особистість.....	21
Маніпулятивні технології.....	26
Зарубіжні спецслужби і технології «соціального контролю»	30
Проблема захисту даних. DOS та вірусні атаки	35

РОЗВИТОК І ПЕРСПЕКТИВИ СОЦІАЛЬНИХ МЕРЕЖ

Количество и разнообразие социальных сетей постоянно растёт. В последнее время, как известно, показатели использования подростками крупнейшей в мире социальной сети Facebook падали. Очередное исследование лишь раз подтвердило эту тенденцию, а также выявило, что популярность Facebook среди раннего юношеского возраста минимальна.

Исследование Global Social Media Impact Study было проведено в восьми европейских странах среди людей 16–18 лет. Среди этой возрастной группы многие сделали выбор в пользу использования Instagram, Twitter, Snapchat и WhatsApp вместо Facebook. При этом главная причина ухода из Facebook – растущее число пользователей старшего возраста, то есть родителей.

Исследование также показало, что молодых людей мало беспокоит вопрос уровня сложности или недостаточной функциональности альтернативных служб. В то же время их мало беспокоит вопрос приватности и доступа к опубликованным данным сторонних людей или организаций. Выяснилось, что они обычно ведут частные беседы, делятся личными фотографиями и видеороликами через Skype или мобильные приложения вроде WhatsApp, а при публикациях на Facebook срабатывает психологическая цензура.

Глава команды исследователей из медицинского колледжа Лондонского университета Д. Миллер отмечает: «Популярность Facebook [у этой возрастной группы] не просто падает – по сути эта служба осталась давно в прошлом. Большинство опрошенных ощущают смущение только от того, что их могут ассоциировать с пользователями Facebook. Как когда-то родители беспокоились о присоединении их детей к Facebook, так дети теперь говорят, что их семья настаивает, чтобы они публиковали в Facebook обновления о своей жизни» (*Facebook совершенно не интересен пользователям в возрасте 16–18 лет // InternetUA (<http://internetua.com/Facebook-sovershenno-ne-interesen-polzovatelyam-v-vozraste-16-18-let>). – 2014. – 1.01).*

Почти половина американской интернет-аудитории старше 65 пользуется Facebook. Но самой «взрослой» соцсетью все равно является LinkedIn – в ней пользователей старше 50 больше, чем тем, кто младше 29, пишет Marketing Media Review (<http://mmr.ua/news/id/facebook-stareet-instagram-molodeet-37809/>).

Около 73 % американской интернет-аудитории старше 18 лет пользуется как минимум одной соцсетью. Около 42 % зарегистрированы на нескольких платформах, сообщается в исследовании центра Pew.

Первое место по популярности по-прежнему занимает Facebook. В нем зарегистрированы 71 % интернет-пользователей старше 18 лет. За год их количество возросло на 4 %.

За Facebook следует LinkedIn, в котором зарегистрировано 22 % пользователей. Третий по популярности – Pinterest, который с 2012 г. возрос на 6 % – в настоящее время им пользуется 21 %. В Twitter зарегистрированы 18 %, а в Instagram – 17 %.

Среди тех, кто пользуется только одной соцсетью, 84 % выбирают Facebook. Остальные 8 % зарегистрированы в LinkedIn, 4 % – в Pinterest и 2 % – в Instagram или Twitter.

У аудитории каждой соцсети есть свои особенности. В Pinterest в четыре раза больше пользователей-женщин, чем мужчин. LinkedIn особенно популярен среди взрослой аудитории с высшим образованием и достатком выше среднего. Это единственная соцсеть, в которой пользователей от 50 до 64 лет больше, чем тех, кому 18–24 года – 15 % и 24 % соответственно. У Twitter и Instagram аудитория значительно совпадает – этими сервисами пользуется в основном молодежь и городские жители.

Аудитория Facebook стареет – если в прошлом году им пользовались 35 % интернет-юзеров старше 65 лет, то теперь – 45 %. В Instagram, наоборот, растет количество молодых пользователей – если в 2012 г. 28 % интернет-аудитории до 29 лет были зарегистрированы в сервисе, то на сегодняшний день их уже 37 %.

Пользователи Facebook и Instagram – самые активные. 63 % Facebook-пользователей заходят в соцсеть ежедневно, среди них 40 % – несколько раз в день. Instagram ежедневно посещают 57 % пользователей, а больше одного раза за день – 35 % (*Facebook стареет, Instagram молодеет // Marketing Media Review (<http://mmr.ua/news/id/facebook-stareet-instagram-molodeet-37809/>). – 2014. – 3.01*).

Пользователи российской социальной сети «Одноклассники» получили возможность смотреть фильмы онлайн, сообщает bfm.ru со ссылкой на пресс-службу компании.

Сообщается, что в социальную сеть был интегрирован видеоканал с полнометражными фильмами. Его запуск приурочен к новогодним праздникам: компания надеется, что пользователи начнут смотреть фильмы онлайн с помощью «Одноклассников» во время отдыха. В настоящее время сообщение о нововведении прокомментировали уже более 3 тыс. человек, в основном они делятся своими планами относительно фильмов, которые намереваются посмотреть.

«Одноклассники» начали показывать бесплатное кино еще 12 декабря 2013 г. Однако изначально для просмотра были доступны различные сериалы, тогда как полнометражные фильмы смотреть было нельзя. Теперь компания существенно расширила ассортимент видеоконтента (*В «Одноклассниках» появился сервис просмотра фильмов онлайн // IT Expert (<http://itexpert.in.ua/rubrikator/item/33096-v-odnoklassnikakh-poyavilsya-servis->*

prosmotra-filmov-onlajn.html). – 2014. – 5.01).

Twitter вывел свой сервис коротких роликов на новый уровень: у Vine появилась полноценная веб-версия. Конечно, у ближайшего конкурента, Instagram, веб-интерфейс появился уже очень давно, но в любом случае это обновление будет удобно для Vine. В веб-версии есть весь привычный функционал – просмотр, комментарии и т. д. Также появилась новая функция – можно смотреть ролики в «ТВ-формате», то есть в полноэкранном режиме и без перерывов (*Vine обзавёлся веб-профилями // InternetUA (http://internetua.com/Vine-obzav-lsya-veb-profilyami). – 2014. – 5.01).*

В десятку украинских городов, в которых социальные сети пользуются наибольшей популярностью, вошли Киев, Одесса, Львов, Донецк, Днепропетровск, Симферополь, Тернополь, Луганск, Харьков и Севастополь.

Всего в социальных сетях зарегистрировано более 30 млн украинцев, лишь 8 % от всего населения страны ни разу не общались виртуально.

Наиболее популярной является социальная сеть «ВКонтакте» (20 млн). На втором месте – «Одноклассники» (6 млн), на третьем – Facebook (2 млн).

Среди пользователей «ВКонтакте» чуть больше мужчин, среди пользователей «Одноклассников» и «Facebook» – женщин.

Средний возраст пользователей «ВКонтакте» – 20–22 года, «Одноклассников» – 27–29, Facebook – 24–26 лет.

Только 8 % украинцев никогда не заходили в социальные сети.

Около 300 тыс. украинских блогов в настоящее время размещены в Twitter.

Больше аккаунтов зарегистрировано в Киеве, Одессе, Харькове, Львове и Днепропетровске. Ежедневно там появляется более 90 тыс. записей, средняя длина «твита» по-украински – 84 символа, по-русски – 72 (*Харьковчане вошли в ТОП-10 пользователей социальных сетей по Украине // Infa.kharkov.ua (http://infa.kharkov.ua/xarkovchane-voshli-v-top-10-polzovatelej-socialnyx-setej-po-ukraine/). – 2014. – 6.01).*

Главная задача социальной сети LinkedIn, с самого момента существования – дать работодателям и специалистам найти друг друга. Вот только в последнее время простое общение между сторонами в сети не дарит владельцам ресурса того прироста прибыли, на который рассчитывали. И приходится искать новые инструменты.

Мыслить нужно глобально – разработчики LinkedIn пытаются создать уникальный алгоритм, позволяющий компаниям найти именно такого

сотрудника, который нужен. Причем речь идет о целом наборе качеств, умений, навыков, психологических и физиологических элементов. Опять-таки – любой работник будет видеть, в какую сторону ему нужно расти.

Все резюме сотрудников в LinkedIn будут объединены в единую базу. В этой же базе будут учтены все «перемещения» рабочих, изменения профессиональных качеств и т. д. «Мы хотим создать совершенно новый алгоритм поиска сотрудников, – говорит Д. Шапиро, старший вице-президент по глобальным решениям LinkedIn. – Это будет как Google, только для поиска рабочих. Это будет самым большим проектом за все время нашего существования – поэтому я не берусь называть даже примерную дату релиза».

По словам Д. Шапиро, раньше, еще лет 20 назад поиск работников не был проблемой, не вызывал никаких трудностей. В настоящее время угадать и заполучить качественного специалиста невероятно трудно. Задачей LinkedIn и является обеспечить высокую вероятность «хорошего работника». А заодно и создать условия для здоровой конкуренции (*LinkedIn создаст сервис по подбору персонала // Uinny (<http://uinny.ru/index.php?id=1166>). – 2014. – 6.01*).

Сооснователь Twitter Б. Стоун представил мобильное приложение Jelly. Оно представляет собой сервис вопросов и ответов, действующий через социальные сети, говорится в блоге разработчиков.

Как сообщает IT Expert со ссылкой на портал Лента.ру, Jelly работает следующим образом: пользователь через программу для Android или iOS задает вопрос, а ответ на него дают его друзья по социальным сетям. Необходимо, чтобы у отвечающих тоже было установлено Jelly.

Если друзья не знают ответа, они в свою очередь могут спросить его у своих знакомых. Таким образом, ответ могут дать и те люди, которых нет в списке друзей у задавшего вопрос пользователя.

К вопросу можно прикладывать изображения – например, фото, снятые на смартфон. На снимке, в частности, может быть изображен предмет, о назначении которого спрашивает пользователь.

По мнению создателей Jelly, сервис отличается от традиционных поисковых систем тем, что находимые с его помощью ответы подкреплены практическим опытом реальных людей, включая друзей и знакомых.

Приложение Jelly распространяется бесплатно, но в России оно пока недоступно. Единственным языком, который поддерживает сервис в настоящее время, является английский.

Б. Стоун запустил Jelly совместно с программистом Б. Финкелем. Впервые он упомянул о сервисе в апреле 2013 г., но предназначение Jelly вплоть до запуска сохранялось в тайне.

Jelly отчасти схож с веб-сервисами вопросов и ответов – они есть, например, у Google и Mail.ru. С их помощью можно задавать вопросы, ответы на которые может дать любой пользователь. Лучший ответ выбирается

голосованием *(Сооснователь Twitter запустил сервис поиска ответов в соцсетях // IT Expert (<http://itexpert.in.ua/rubrikator/item/33151-soosnovatel-twitter-zapustil-servis-poiska-otvetov-v-sotssetyakh.html>). – 2014. – 8.01).*

Директор британского Центра по анализу соцмедиа Д. Бартлетт разобрался в преимуществах российской социальной сети «ВКонтакте», которые делают ее столь популярной на родине и в СНГ. Согласно его умозаключениям, успех соцсети основывается на пиратском контенте и функционале, который делает из нее удобный и бесплатный аналог сервиса знакомств. Facebook ни тем, ни другим похвастаться не может, поэтому его покидает молодежь.

«Пишу из Москвы. Пока никаких признаков Э. Сноудена не обнаружено, зато российский эквивалент Facebook – «ВКонтакте» – повсюду. Россияне – самые активные пользователи соцсетей в мире и проводят в них больше времени, чем жители других стран. «ВКонтакте» – это их выбор, в ней насчитывается примерно 50 млн уникальных пользователей, между тем как в Facebook – всего 10 млн. А на прошлой неделе сообщалось, что в Facebook не хватает тинэйджеров – она попросту больше «не крутая». «ВКонтакте» же, наоборот, преимущественно популярна среди юного населения», – пишет Д. Бартлетт.

«Почему? Вот вам простая теория. В отличие от Facebook, «ВКонтакте» предлагает две вещи, которые нужны молодым людям: поиск сексуальных партнеров и возможность посмотреть самые новые фильмы (пиратские копии). В Facebook этого нельзя.

Во «ВКонтакте» поиск реализован просто потрясающе – найти можно практически кого угодно, фильтруя пользователей по полу, статусу отношений и предпочтениям. Россияне, с которыми я общался, утверждают, что все это органично превратило сайт в бесплатный и всесторонний сервис знакомств, который одновременно является еще и социальной сетью. Я уверен, все в курсе того, что сервисы знакомств – очень прибыльный бизнес. Ссылки в социальных аккаунтах на хорошие приложения для свиданий невероятно популярны. Например, YouTube начинался как сайт знакомств, и во многом с того же стартовал и Facebook.

Сегодня – по ряду причин – в соцсети М. Цукерберга гораздо больше опций приватности, и многие этим пользуются, чтобы их сложнее было найти и связаться. В результате, за последние пару лет такие бесплатные «секстовые» приложения, как Tindr и Snapchat уже более или менее наполнили нишу. Огромное количество тинэйджеров сидят в них вместо Facebook.

«ВКонтакте» также позволяет пиратству проходить незамеченным. Это огромный каталог пиратских фильмов. По данным Ассоциации звукозаписывающих компаний Америки, «ВКонтакте» – один из самых пиратских сайтов в мире. Facebook же очень строг к пиратским материалам.

Однако это чрезвычайно популярное времяпрепровождение: в Северной Америке, Азии и Европе четверть всех интернет-пользователей загружают пиратский контент.

В скором времени «ВКонтакте» также может сделать шаг навстречу уважаемым организациям. Шаг в направлении подавления пиратства. В результате сайт, вероятно, потеряет некоторое количество юных пользователей. Но, как и Facebook, «ВКонтакте» начнет поднимать более широкую аудиторию – пользователей старше 30 лет, трендсеттеров и других – которая станет для соцсети более чем визитной карточкой» (*Британский эксперт по социальным медиа рассказал, чем «ВКонтакте» превосходит Facebook // InternetUA (<http://internetua.com/britanskii-ekspert-po-socialnim-media-rasskazal--csem--vkontakte--prevoshodit-Facebook>). – 2014. – 8.01).*

Исследователи южнокорейского института KAIST (Korea Advanced Institute of Science and Technology) разработали программу, которая позволяет выявлять и отсекают в соцсетях около 90 % «уток» – сообщений и слухов сенсационного характера, которые на самом деле являются ложными.

Как заявили представители этого известного корейского научного центра, успеха добилась группа исследователей во главе с профессором Чха Ми Ен. Специалисты в течение нескольких лет собирали и анализировали основные новостные темы и сообщения, которые появляются в сетях как Facebook и Twitter. Особое внимание обращалось на ту информацию, которая носила сенсационный характер, а затем было доказано, что она является ложной.

В результате были выявлены основные признаки ложных слухов. Например, если сенсационная, но правдивая информация на первых порах привлекает большое внимание, но затем практически полностью исчезает из информационного поля, то псевдосенсации имеют тенденцию регулярно появляться вновь и вновь, обрастая новыми деталями и подробностями. Кроме того, для «уток» характерно использование таких оборотов как «не знаю, правда или нет, но...», «неточно, но известно, что...», «мне кажется...» и т. д.

На основе полученной информации была создана специальная программа, которую можно активировать при пользовании соцсетями. Программа выявляет и отсекает не менее 90 % неверной информации и «уток», что существенно облегчает жизнь многим пользователям (*Корейцы создали программу для выявления ложных слухов в соцсетях // InternetUA (<http://internetua.com/koreici-sozdali-programmu-dlya-viyavleniya-lojnih-sluhovy-socsetyah>). – 2014. – 11.01).*

«ВКонтакте» вошла в топ-10 крупнейших в мире соцсетей
Ресурс «ВКонтакте» вошел в десятку крупнейших социальных сетей мира

по версии компании Adobe. Российская соцсеть разместилась на восьмом месте рейтинга с 228 млн зарегистрированных пользователей. Детище П. Дурова стало единственным интернет-сервисом из Европы, попавшим в топ.

Возглавляет рейтинг Facebook, количество пользователей которой превысило 1,4 млрд. Десятая часть аккаунтов соцсети М. Цукерберга приходится на США. Кроме того, Facebook активно пользуются в Бразилии, Индии, Индонезии, Мексике, Турции и Великобритании.

В качестве отдельной соцсети представители Adobe посчитали YouTube. Видеосервис с миллиардом пользователей разместился на втором месте. Далее следуют китайские ресурсы Qzone (623 млн) и Weibo (503 млн), передает «РИА Новости». В рейтинг также вошли Twitter, Google+, LinkedIn и Renren. Замыкает первую десятку Instagram (*«ВКонтакте» вошла в топ-10 крупнейших в мире соцсетей // InternetUA (<http://internetua.com/vkontakte-voshla-v-top-10-krupneishih-v-mire-socsetei>). – 2014. – 12.01*).

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИЯВ ФОРМУВАННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

Соцсеть «ВКонтакте» составила рейтинг самых обсуждаемых ее пользователями тем 2013 г., сообщает Digit.ru. Среди международных новостей самым популярным событием стал Евромайдан в Киеве, на втором месте – гражданская война в Сирии, на третьем – разоблачения Э. Сноудена. Среди российских – выборы мэра Москвы, дело «Кировлеса» и «антипиратский» закон.

Самыми обсуждаемыми массовыми мероприятиями года стали эстафета Олимпийского огня, Евровидение-2013 и авиационно-космический салон МАКС-2013.

Среди происшествий больше всего обсуждалось падение Челябинского метеорита, авиакатастрофа в Казани и убийство Е. Щербакова, которое спровоцировало беспорядки в Бирюлево.

Лидером спортивных обсуждений стали чемпионат мира по футболу, бой В. Кличко с А. Поветкиным и Универсиада-2013 в Казани. Из новостей науки пользователей «ВКонтакте» больше всего интересовал бозон Хиггса.

Самым популярным мемом стала пародия на видео Harlem Shake, самой обсуждаемой игрой – Grand Theft Auto V. Второе и третье места заняли, соответственно, игровые консоли PlayStation 4 и Xbox One.

Ранее подобный обзор опубликовала социальная сеть Facebook. Самыми популярной мировой темой оказалось назначение нового Папы Римского. На втором месте – обсуждение различных выборов, на третьем – рождение наследника британской короны, на четвертом – тайфун, на пятом – смерть М. Тэтчер, на шестом – видео Harlem Shake. Также пользователи Facebook активно обсуждали певицу М. Сайрус, теракт во время Бостонского марафона,

соревнования Tour de France и смерть Н. Манделы.

Администрация соцсети также подсчитала, что пользователи чаще всего добавляли в свой Timeline. На первом месте события личной жизни – начало отношений, помолвка, женитьба. На втором – путешествия, на третьем – переезд, на четвертом – расставание, на пятом – знакомство с другом. Также многие добавляли новых родственников, отмечали, что они завели питомца, потеряли близкого человека, сделали пирсинг или бросили какую-то вредную привычку (*Соцсеть «ВКонтакте» подвела итоги года // InternetUA (<http://internetua.com/socset-vkontakte-podvela-itogi-goda>). – 2013. – 31.12).*

Хмельничанам розповіли про мережу колективного захисту «Свої». Приєднатися до мережі можна, заповнивши анкету.

«В Україні почастишали випадки індивідуальних репресій. Загроза небезпеки зростає, тому і була обговорена ідея створення мережі колективного захисту під назвою “Свої”. Свій за свого, як брат за брата. Півтисячі людей уже зареєструвалися у мережі і уже готові допомагати один одному. Принцип такий, що ти допоможеш комусь, потім тобі допоможуть усі. Долучилися декілька громадських організацій, зокрема “Сила людей”, яка ініціювала цей проект, також Євромайдан SOS – основний майданчик правозахисників у Києві, які захищали в’язнів Банкової, а також громадська рада “Євромайдану”», – розповідає громадський активіст Євромайдану Р. Рохов.

Приєднатися до мережі колективного захисту можна через соціальні мережі. «Наразі основний комунікаційний ресурс мережі колективного захисту “Свої” – Facebook. Люди можуть зайти на сторінку мережі, перейти за посиланням і зареєструватися за допомогою інтерактивної анкети. Після реєстрації людина потрапляє у нашу базу, одразу стає суб’єктом захисту, а також одночасно зобов’язує себе, у разі необхідності, надавати допомогу іншим», – наголошує Р. Рохов (*Хмельничанам розповіли про мережу колективного захисту «Свої» // Народна газета «Є» (http://ye.ua/news/news_14753.html). – 2014. – 5.01).*

В Австралии ученые придумали, как обезопасить купальщиков от больших белых акул, которые часто появляются вблизи общественных пляжей. Теперь отдыхающие смогут узнать о приближении хищников, просто прочитав твиты, передает «Сегодня» со ссылкой на FedPost.

Согласно информации Sky News, австралийские ученые прикрепили датчики к 320 акулам с целью контролировать их передвижения. По словам авторов проекта, если рыба с датчиком находится в километре от пляжа, то на компьютер подается сигнал тревоги и в сервисе микроблогов Twitter появляется короткое предупреждающее сообщение.

В твите указываются размер, вид акулы и ее примерное местонахождение.

За последние два года в Западной Австралии жертвами акул стали шесть человек. Последнее нападение хищницы произошло в ноябре – она убила 35-летнего серфера К. Бойда. Государственные власти пытались обезопасить отдыхающих с помощью патрулирования пляжей вертолетами и катерами, но в последнее время произошел всплеск нападений, что побудило чиновников искать новые пути решения проблемы. Так, ранее правительство разрешило рыбакам убивать акул, которые находятся в трех метрах от береговой линии (***В Австралии с помощью Twitter будут спасать купальщиков от нападения акул // IT Expert (<http://itexpert.in.ua/rubrikator/item/33077-v-avstralii-s-pomoshchyu-tvittera-budut-spasat-kupalshchikov-ot-napadeniya-akul.html>). – 2014. – 3.01).***

Посол США в Москве М. Макфол пользуется соцсетями, чтобы донести свою позицию до общества, отмечает на страницах Foreign Policy журналистка А. Немцова. Так, в начале декабря он провел настоящий «марафон» – отвечал на вопросы российских пользователей Twitter.

А. Немцова признается: ей, как начинающему пользователю, Twitter было очень интересно наблюдать, как «профессионал» (так она называет М. Макфола) решает взаимоисключающие задачи: нужно было выдержать баланс между максимальной открытостью, которой требовала аудитория, и необходимостью дипломатического такта.

Дипломатия требует подбирать слова осмотрительно, но в Twitter свою мысль нужно уложить в 140 знаков максимум. М. Макфол пошутил: «Живьем я лучше», но отметил, что Twitter дает ему «огромные преимущества как послу, пытающемуся разъяснить нашу политику этой огромной стране».

Многие россияне просто потрясены возможностью прямого общения с Госдепартаментом США, говорится в статье.

По данным А. Немцовой, еще два года назад, до приезда в Россию, М. Макфол не знал, как выглядят твиты. Это тогдашний госсекретарь Х. Клинтон посоветовала ему вести диалог с обществом через социальные медиа. Теперь (по данным А. Немцовой, на декабрь) у М. Макфола более 57 тыс. фолловеров: вчетверо меньше, чем у К. Собчак, но почти в два с половиной раза больше, чем у А. Пушкина – одного из его основных оппонентов.

А. Немцова разъясняет: «Правда, российские пользователи Twitter – крохотное меньшинство в стране, где правительство контролирует все виды медиа с широчайшим охватом». Для большинства простых россиян основной источник информации – федеральные телеканалы. Крупные каналы, по словам источников, в последнее время не приглашают М. Макфола в эфир. Возможно, Кремль счел, что его открытая, обаятельная манера слишком эффективна,

считает автор. Впрочем, другие российские СМИ часто цитируют записи М. Макфола в соцсетях, а некоторые частные СМИ охотно берут у него интервью. Но социальные медиа оказались очень эффективным инструментом распространения его идей среди все более широкой аудитории.

Популярность М. Макфола особенно примечательна на фоне российско-американских трений, а также антиамериканского тона в крупных российских СМИ, отмечает А. Немцова.

М. Макфол особо подчеркнул, что общается с Россией не только через Twitter: он посещает мероприятия, встречается с чиновниками, а также при любом удобном случае проводит время с россиянами из самых разных социальных слоев.

М. Макфол с гордостью говорит: «Я выступал с двухчасовыми лекциями на русском языке. Интересно, делали ли это когда-нибудь другие дипломаты».

Правда, говорить на иностранном языке легче, чем писать на нем. Некоторые фолловеры охотно придираются к грамматическим ошибкам в Twitter М. Макфола. Посол совершенствуется – по вечерам он часто сидит со словарем, стараясь, чтобы его тексты для Twitter были написаны на безупречном русском.

«Подход М. Макфола к дипломатии раздражает некоторых российских дипломатов и кремлевских чиновников», – отмечает А. Немцова. С. Марков, работающий в правительственных структурах, заметил, что российская дипломатия находится «на другом краю спектра» – «мы заново изобретаем нашу экзотическую, империалистическую дипломатию с гораздо большей дисциплиной, поскольку нам нужно именно это». Однако С. Марков похвалил таланты М. Макфола и назвал его «трендсеттером»: «Теперь даже наш МИД следует его примеру, используя Twitter» (*Покорить сердца российских «просвещенных твиттерян» // Статус (http://statuspress.com.ua/international-news/pokorit-serdca-rossijskix-prosveshhennyx-tvitteryan.html). – 2014. – 7.01).*

БІЗНЕС І СОЦІАЛЬНІ МЕРЕЖІ

Не так давно социальная сеть Facebook, вслед за Twitter, реализовала возможность встраивания постов на сторонние сайты. Эта функция может быть очень полезна для маркетологов брендов, однако не все знают, для чего вообще ее можно использовать, пишет Marketing Media Review (<http://mmr.ua/news/id/dlja-chego-brendy-mogut-ispolzovat-vstraivaemye-posty-s-facebook-37784/>).

В материале собраны советы восьми известных западных предпринимателей, которые эффективно применяют этот инструмент.

1. Увеличение вовлеченности в Facebook.

Размещение постов из соцсети в блоге может положительно сказаться на

показателях вовлеченности страницы в Facebook. Поскольку встраиваемые посты интерактивны, то читатели блога могут делиться вашим контентом в своих блогах или, собственно, на своих страничках, кликнув на кнопку Share. Естественно, они могут и лайкнуть вашу страницу на Facebook прямо из поста в блоге. Так что, как ни посмотри, встраиваемые посты – это просто отличное средство, которым грех не воспользоваться.

Б. Фармило, Internet Marketing Agency

2. Продвижение вирусного контента.

В Twitter уже давно есть возможность встраивания постов где угодно в вебе, и вот теперь к этому пришел и Facebook. Это значит, что «жизнь» популярного контента станет еще длиннее, и он сам сможет выйти за границы социальной сети. Бренды могут получать хорошие результаты, размещая популярные посты из Facebook на своих сайтах и страницах для прессы и клиентов.

Д. Блох, Poshly Inc.

3. Кросс-промоушн.

С помощью встраиваемых постов можно одновременно увеличить и вовлеченность в самой соцсети и поднять трафик на сайт. Это средство интеграции поможет предпринимателям и маркетологам быстрее добиваться положительных результатов.

Э. Шрейдж, Money Crashers Personal Finance

4. Использование в игровых механиках.

При проведении промо-акции на сайте, для того, чтобы принять в ней участие, можно попросить пользователей «лайкать», комментировать или делиться на своих страницах вашим встроенным постом.

Э. Саладино, Just Bath Vanities

5. Поддержание образа бренда.

Вы можете использовать встраиваемые Facebook-посты для того, чтобы транслировать позицию бренда по разным вопросам и его философию не только в социальной сети, но и на сайте и в блоге. Текст, видео, картинки, хештеги – все это, вкупе с возможностью разместить пост на любой площадке, поможет увеличить охват контента, расширить и сильнее вовлечь аудиторию.

Л. Перкинс, Perks Consulting

6. Освежение веб-сайта.

Новый инструмент отлично подходит для трансляции сообщений из соцсети прямо на страницы вашего сайта или блога. Во встраиваемом посте отображается число лайков, которое он получил, что позволит вам понять реальное качество трафика с сайта и увеличить его – ведь лайк, шейр или комментарий являются отличными рекомендациями для тех пользователей Facebook, которые еще не знакомы с вашим брендом. Кроме того, встраивание постов из соцсети облегчит обновление контента на сайте – ведь нужно опубликовать контент только один раз, а использовать его можно сразу в нескольких местах.

Н. Смартт, Star Staffing

7. Увеличение охвата и объемов взаимодействий.

Facebook отлично подходит для распространения любой информации. С появлением возможности встраивания публикаций на сторонних сайтах, их охват значительно увеличился, что влечет за собой и большее взаимодействие с аудиторией. Теперь у брендов появилось больше возможностей для доставки своих сообщений людям.

Д. Ву, A Forever Recovery

8. Доставка контента из Facebook посетителям других площадок.

Встраиваемые посты крайне полезны тем брендам, у которых пока нет страницы на Facebook с большим количеством подписчиков, но зато имеются сайты или блоги со значительным трафиком. Гораздо проще показать им контент из Facebook, чем заставить этих людей подписаться на страницу компании в соцсети. В конечном итоге, это поможет добиться большей вовлеченности количества лайков, чем если бы вы просто публиковали контент в Facebook.

Э. МакГиерти, Globe Runner SEO (*Для чего бренды могут использовать встраиваемые посты с Facebook // Marketing Media Review (<http://mmr.ua/news/id/dlja-chego-brendy-mogut-ispolzovat-vstraivaemye-posty-s-facebook-37784/>). – 2013. – 30.12).*

Чтобы помочь компаниям составить их медиа-планы на 2014 г., Mashable собрал наиболее актуальные прогнозы экспертов по социальным медиа, пишет Marketing Media Review (<http://mmr.ua/news/id/top-3-trenda-socialnyh-media-v-2014-godu-37804/>):

1. Специалисты в социальных сетях: больше и лучше.

Согласно Business Insider в 2014 г. будет спрос на шесть специалистов в сфере социальных медиа: специалиста SEO, стратега в области соцмедиа, менеджера онлайн комьюнити, менеджера по маркетингу в соцсетях, координатора по маркетингу в соцсетях, и блогера или соцмедийного копирайтера.

2. За рамками Facebook: новые платформы.

Forbes составил свой список топ-7 трендов в социальных медиа, которые будут доминировать в 2014 г. MySpace вернется, Google+ станет ведущим фактором, и в сетях станет больше микровидео. Что это означает для брендов:

Так как MySpace находится все еще на ранней стадии, не следует бренду выстраивать всю социальную стратегию на этой платформе. Нужно просто присматривать за ней – как бренды будут использовать платформу в этом году.

Google+ становится неотъемлемой частью великого плана Google в рамках SEO, социальных сигналов, предоставляя более персонализированный поиск. Если у вас нет аккаунта в Google+, в этом году вы должны завести его.

Если вы еще не освоили видео Vine или Instagram, пришло время их

освоить. Если прогнозы подтвердятся, создание коротких видео станет таким же важным, как и создание сообщений в 140 символов. Чем раньше вы освоите этот тренд, тем лучше.

3. Маленькие моменты, большие тренды.

PR Daily выделила 10 моментов в социальных сетях в 2013 г., которые, по их мнению, являются предшественниками главных трендов в 2014 г., включая твит Oreo во время Super Bowl, запуск хэштегов Facebook и преобразование Pinterest. Что это означает для компаний?

Эксперты социальных медиа весь год говорили об огромном успехе твита Oreo в режиме реального времени во время Super Bowl. PR Daily прогнозирует, что как бренды платят за «продакт плейсмент», так компании будут заключать сделки с каналами, чтобы узнать сюжетную линию ТВ-программы заблаговременно, чтобы их контент был более актуальным.

PR Daily также предсказывает, что введение хэштегов Facebook означает, что бренды будут включать хэштеги в ТВ-ролики, печатную рекламу и радиоролики более часто, чтобы усилить кампании в социальных медиа.

Pinterest представил в этом году такие функции, как Place Pins, аналитику и Rich Pins, усилив ROI для брендов. Компаниям стоит ознакомиться с новыми функциями Pinterest (*Топ-3 тренда социальных медиа в 2014 году // Marketing Media Review (<http://mmr.ua/news/id/top-3-trenda-socialnyh-media-v-2014-godu-37804/>). – 2014. – 2.01*).

В начале этого месяца Facebook сообщил, что администраторы сообществ могут заметить небольшое снижение органического охвата своих постов из-за изменений в алгоритме Edge Rank. Однако многие западные маркетологи отмечают существенное падение охвата – вплоть до 44 %, и началось оно уже несколько месяцев назад, пишет Marketing Media Review (<http://mmr.ua/news/id/ohvat-brendovyh-facebook-stranic-upal-na-44-37798/>).

По словам Facebook, бренды могут компенсировать недостающий охват, покупая рекламу и используя платное продвижение постов. Но компании вряд ли заинтересованы в таком решении проблемы.

Западная компания Komfo проанализировала 5 тыс. брендовых Facebook-страниц в период август – ноябрь 2013 г. и отметила следующие изменения:

- уменьшение охвата постов на 42 %;
- увеличение вирусного распространения постов на 31 %;
- увеличение CTR на 28 %.

По словам А. Джоргенсон, менеджера по маркетингу Komfo, такие результаты означают, что бесплатные методы работы в Facebook уходят в прошлое. Как и другие каналы, Facebook начинает требовать все больше бюджетов.

Вместе с тем специалисты Komfo отмечают, что алгоритмы Facebook стали лучше в том, что касается показа публикаций правильным пользователям

– об этом свидетельствует увеличение вирусного распространения и CTR.

Аналитики Ignite Social Media также отмечают существенное уменьшение органического охвата постов в Facebook. Изучив 689 публикаций 21 крупного бренда, компания пришла к выводу, что на неделе, когда Facebook сделал заявление, охват упал в среднем на 44 %.

Если раньше, по словам соцсети, бренд мог охватить порядка 16 % своей аудитории, то теперь, по данным Ignite, этот показатель может упасть до 3 %.

Д. Тобин, исполнительный директор Ignite Social Media: «Компании инвестируют более 6 млрд дол. в Facebook. Как мне кажется, вряд ли такое изменение алгоритма обусловлено желанием “обделить” контент брендов. Не очень мудро так поступать – привлекательность Facebook для брендов заключается именно в миксе платных и бесплатных возможностей.

Facebook вправе изменять свой алгоритм, чтобы улучшить пользовательское взаимодействие с сайтом. Но эти изменения должны быть основаны на силе контента, а не на закрытых правилах и догадках, что каждый пользователь Facebook внезапно захотел увидеть больше новостных статей в своей ленте.

Мы передали данные нашего исследования Facebook и надеемся, что проблема будет исправлена. В последнее время Facebook очень часто вносил изменения в новостную ленту, и, наверняка, это просто случайные последствия этих поправок.

Однако все это происходит не в самое лучшее время – многие компании согласовывают стратегии и бюджеты на 2014 г., и изменения в алгоритмах Facebook могут усложнить данные процессы» (*Охват брендовых Facebook-страниц упал на 44 % // Marketing Media Review (<http://mmr.ua/news/id/ohvat-brendovyh-facebook-stranic-upal-na-44-37798/>). – 2014. – 2.01).*

The Next Web собрал в одном посте 10 статистических фактов о Twitter, которые дают пищу для размышлений, как добиться там успеха, пишет Marketing Media Review (<http://mmr.ua/news/id/10-sovetov-tem-komu-nuzhen-uspeh-v-tvittere-37824/>).

1. Вовлеченность для сообщений брендов в выходные на 17 % выше.

Невероятно, но факт: именно в выходные ваши твиты более востребованы аудиторией. При этом лишь 19 % корпоративных аккаунтов что-то пишут во время уикенда.

...Social media scientist Д. Зарелла провел ряд экспериментов, которые также позволили сделать вывод о том, что показатель CTR для твитов, отправленных в пятницу, субботу и воскресенье, значительно выше.

2. Показатели вовлеченности для твитов со ссылками на изображения в два раза выше, чем без них.

В этом плане аудитория сервиса микроблогов ничем не отличается от своих коллег из Facebook.

3. Твиты, содержащие менее 100 символов, вовлекают народ на 17 % лучше.

Еще одно сходство с Facebook – чем меньше букв, тем лучше в любой из двух соцсетей.

Если вы обязательно вставляете в твиты-ссылки, то исследование Д. Зареллы устанавливает для вас оптимальную планку в 120–130 символов на сообщение.

4. Самая быстрорастущая возрастная категория в Twitter – 55–64 года.

Если вы хотите нарастить аудиторию, самое время обратить внимание на новичков Twitter старшего поколения. Соцсети уже давно не только для подростков, пора признать этот факт.

5. Показатели вовлеченности твитов с хештегами в два раза лучше, чем без них.

И все же #не #надо #увлекаться #хештегами. Добавить 1–2 – это нормально, а вот твиты, содержащие три или больше слова с решеткой, уже показывают не такие хорошие результаты. Кроме того, необходимо стараться подбирать правильные хештеги, которые хорошо подходят к теме сообщения.

6. 66 % пользовательских твитов с упоминанием брендов отправлены с мобильных устройств.

Если вы решили поплотнее поработать с мобильной аудиторией, то, во-первых, в своих твитах старайтесь давать ссылки на сайты, оптимизированные для мобильных устройств, во-вторых упоминания юзернеймов других пользователей в комбинации с хештегами также помогут мобильной аудитории – мало кому хочется заморачиваться с поиском в приложении или браузере со смартфона.

7. Вероятность того, что пользователи Twitter, которые в основном заходят в соцсеть с мобильного, находятся при этом в пути на 181 % выше.

При отправке твитов всегда нужно думать о своей аудитории: где сейчас эти люди и чем они занимаются? Например, с утра есть большая вероятность, что они еще в дороге на работу – скучают в маршрутках, метро и электричках – отличное время, чтобы предложить им что-то интересное.

8. Вероятность того, что пользователи, которые больше других «ретвитят», напишут прямое сообщение, на 122 % выше.

Обитателей Twitter, которые любят «ретвитить» больше других, англоязычные эксперты называют «усилителями» (amplifiers) контента. Как выясняется, эта категория пользователей также ничего не имеет против отправки прямых сообщений. Еще один факт – 90 % из них «твитят» о ТВ-шоу.

Это свидетельствует о том, что такие люди рассматривают Twitter как средство общения с близкими (отсюда и отправка прямых сообщений) и рассказов о своих привычках и увлечениях, таких как просмотр ТВ-программ.

9. Если попросить «ретвитнуть» сообщение, то шансы на это повышаются в 12 раз. А если прямо написать retweet – аж в 23 раза.

10. Твиты со ссылками ретвитят на 86 % чаще.

Пользователи Twitter любят не только картинки, но и ссылки. Однако если первые больше влияют на вовлеченность, то ссылки повышают число «ретвитов». Так что если перед вами стоит задача увеличения охвата, лучше сосредоточиться на ссылках (*10 советов тем, кому нужен успех в Twitter // Marketing Media Review (http://mmr.ua/news/id/10-sovetov-tem-komu-nuzhen-uspeh-v-tvittere-37824/). – 2014. – 8.01).*

Недавно проведенное исследование показало, что страничка соискателя работы в социальных сетях может подсказать менеджеру по персоналу, кто станет хорошим сотрудником, а кого лучше не нанимать. Однако, согласно результатам последних исследований, прежний вывод был поспешным, сообщает newsoboz.org. со ссылкой на russian.rt.com.

Учёные из трёх университетов США, а также одна консалтинговая фирма подвергли испытанию профессионалов в области подбора персонала. Целью тестов было выяснить, способны ли они определить, станет ли тот или иной человек хорошим работником по его странице в соцсетях, пишет The Raw Story.

Результаты исследования оказались противоположными результатам другого исследования, которое в 2012 г. провёл Д. Клюмер из Университета Северного Иллинойса. Итогом его работы стал вывод о пользе профайлов соискателей рабочего места в Facebook: на его основе, якобы, наниматель может составить впечатление о кандидате и решить, подходит ли он.

Тем не менее, результаты последнего исследования говорят об обратном: не существует никакой статистической корреляции между впечатлением менеджера по персоналу и тем, как новый сотрудник будет работать на новом месте.

Более того, исследование показало, что наниматель часто относится предвзято к кандидатам, у которых на странице в Facebook были указаны «традиционно не белые имена», а также к тем, кто «очевидно не белый».

«Итоговые результаты исследования дают возможность предположить, что организациям нужно быть очень осторожными, используя информацию со страниц социальных сетей при приёме людей на работу», – заявляют авторы исследования (*Facebook не поможет работодателю выбрать трудолюбивого сотрудника // NewsOboz (http://newsoboz.org/obshchestvo/facebook-ne-pomozhet-rabotodatellyu-vybrat-trudolyubivogo-sotrudnika-08012014083000). – 2014. – 8.01).*

Социальная сеть Facebook покупает Little Eye Labs, индийского разработчика инструментов для анализа производительности и мониторинга Android-приложений. Финансовые условия сделки не разглашаются.

На сайте Little Eye Labs говорится, что компания перестала поставлять

свои разработки для новых клиентов и работает над бесплатной версией инструмента, которая будет доступна для нынешних клиентов до 30 июня.

Little Eye Labs базируется в Бангалоре, однако после реализации сделки с Facebook вся команда разработчиков переедет в Менло-Парк (Калифорния), чтобы работать в штаб-квартире социальной сети.

В блоге индийских разработчиков сказано, что там они получают доступ к наилучшей инфраструктуре и смогут улучшить ранее начатые проекты.

Напомним, Little Eye Labs выпустил первую версию своего приложения в апреле 2013 г., а компания была основана в 2012 г. В настоящее время многие Android-разработчики применяют их инструменты для анализа, оптимизации и мониторинга работы созданного софта.

В Facebook не предоставляют дополнительных комментариев относительно сделки с Little Eye Labs (*Facebook покупает индийский стартап* // *Подробности.UA* (<http://podrobnosti.ua/internet/2014/01/08/951936.html>). – 2014. – 8.01).

Социальная сеть Facebook откажется от использования так называемых «рекламных новостей» (Sponsored stories). Об этом говорится в опубликованном компанией плане технических изменений на 2014 г.

Sponsored stories перестанут отображаться в соцсети начиная с 9 апреля. Все купленные ранее в этом блоке рекламные размещения автоматически переведут в другие форматы. Принцип «социального контекста», лежащий в основе механизма работы «рекламных новостей», планируется сохранить и распространить на всю рекламу в социальной сети.

Блок Sponsored stories появился в Facebook в январе 2012 г. Платные посты из этого блока встраиваются в новостные ленты пользователей, исходя из анализа «социального контекста» – рекламный блок пользователь видит только тогда, когда кто-то из его друзей нажал лайк на странице заказавшего размещение рекламодателя. При этом такой пост сопровождается фотографией и именем нажавшего лайк друга, а также подписью о том, что ему нравится та или иная страница.

Sponsored stories часто подвергались критике. Facebook обвиняли в незаконном использовании персональных данных (имен и фотографий) в рекламных целях (*Facebook откажется от блока «рекламных новостей»* // *Лента.Ру* (<http://lenta.ru/news/2014/01/10/sunset/>). – 2014. – 10.01).

СОЦІАЛЬНІ МЕРЕЖІ І ПРОБЛЕМИ СУСПІЛЬНОЇ БЕЗПЕКИ

Інформаційно-психологічний вплив мережевого спілкування на особистість

Психологія лайків і шейрів

Що спонукає користувачів Facebook натискати ці кнопки? Психологи дійшли висновку, що активність у соціальних мережах пов'язана з двома типами мислення: повільним і швидким.

Чому ми натискаємо кнопки like та share у Facebook? Які новини стають популярними в соціальних мережах? Як редактор соціальних медіа має подавати матеріали, аби якомога більше читачів стали активними передплатниками сторінки?

Nieman Journalism Lab опублікував результати дослідження, що встановлює зв'язок між типами мислення й активністю користувача у Facebook. Дослідження провела С. Сонг, журналіст і науковець із Центру Knight-Mozilla. Вона вивчала психологічні мотивації активності в соцмережах на прикладі сторінки The Boston Globe. «Моя мета – допомогти “нюзрумам” краще просувати свої матеріали в соцмережах і привертати більше уваги», – пише вона. MediaSapiens публікує найвагоміші результати дослідження.

Спочатку основні теорії та дані, які справедливі для середовища соціальних мереж:

– два типи мислення людини – швидке та повільне – привертають різні типи уваги;

– процес, коли ми ділимося матеріалом у соцмережі, пов'язаний з емоціями; нашим власним уявленням про себе та самопрезентацією; стосунками з іншими людьми.

Дослідження базувалося на трьох ключових показниках Facebook Insights: охоплення (reach), включені користувачі (engaged users), взаємодія з дописом (talking about this). Охоплення – це кількість унікальних користувачів, які побачили конкретний допис; включені користувачі – це ті, які клікнули на посилання; нарешті останній показник – це кількість користувачів, які лайкнули, прокоментували, поділилися, відповіли на запитання, підписалися на подію. Ці показники демонструють поведінку користувача, відмінність пасивного читання від активної взаємодії.

Великі картинки та гарячі новини

Велика ілюстрація до тексту призводить до збільшення трафіку порівняно з дописом без картинки або з мініатюрою зображення. Цей взаємозв'язок стосується всіх трьох показників Facebook. Вислів «ГАРЯЧА НОВИНА» позитивно впливає на охоплення аудиторії, але не має впливу на включеність користувачів чи обговорення новини. Працюють й інші вислови: «ДИВІТЬСЯ

НАЖИВО», «ГОЛОВНА НОВИНА ДНЯ», «ВРАЖАЮЧЕ ФОТО» та ін.

Якщо ви працелюбний журналіст, то можете засмутитися, що такі примітивні способи, як великі фото чи подібні вислови, приваблюють читачів. Але хороша новина в тому, що ці примітивні трюки не потребують витрат, вони дешеві. Крім того, щоб підвищити включеність користувачів, саме складні методи є кращим вибором, про це йтиметься нижче.

Типи мислення

Щоби зрозуміти, як ми реагуємо на прості та складні подразники (текст, зображення, пазл), корисно почитати книжку Д. Канемана «Мислення. Швидко й повільно» (2011 р.). У ній виділено два типи людського мислення: система 1 (швидко), система 2 (повільно).

Система 1 – неусвідомлена увага. Система 1 пов'язана з тими навиками чи рефlekсами, які важливі для виживання. Вони спрацьовують швидко та автоматично. Наприклад, коли ми відсмикуємо пальці від вогню. Або коли чуємо гучний звук і повертаємо голову – це та увага, якої ми не можемо «вимкнути». Коли бачимо приклад $1+1 = _$, то теж, не замислюючись, можемо дописати результат.

Система 2 – усвідомлена увага. Це набуті навички, наприклад іноземна мова, математика. Система 2 повільна й потребує більших зусиль. Вона спрацьовує, коли треба дописати результат у такому прикладі $23 \times 67 = _$. Ця увага не завжди вмикається, ось чому ми вразливі до маркетингових і рекламних технологій. Крім того, увага відсутня, коли ми втомлені, голодні чи не в гуморі.

Розподіл праці та правило найменшого зусилля

Більшість часу в нас увімкнена система 1. Вона оцінює середовище, і якщо потрібно сконцентруватися на чомусь, звертається до системи 2. Крім того, система 2 вмикається, коли є якісь труднощі, конфлікт, тиск. Та оскільки лінь – це наша природа, і ми схильні накопичувати енергію для можливих майбутніх зусиль, то більшість часу перебуваємо в системі 1.

Тепер подумайте, як ми використовуємо соціальні мережі: ми переглядаємо повідомлення досить швидко. Хоча іноді беремо участь в онлайн-обговореннях, більшість часу ми прокручуємо екран, почувавшись при цьому відпочилими і навіть задоволеними. Іншими словами, ми звертаємося до соціальних мереж, щоб добре провести час, а не долати якісь перешкоди.

Добре проведення часу в соцмережах є тим, що Д. Канеман називає «когнітивною простотою». Немає загроз, екстремальних новин, немає потреби перемикаєти увагу та мобілізувати зусилля.

Зрозумілий і просто написаний текст підходить до когнітивної простоти і тим догоджає системі 1. Подивіться на ці приклади:

«Адольф Гітлер народився у 1892 році».

«Адольф Гітлер народився у 1887 році».

Експеримент демонструє, що більшість людей повірять першому твердженню, бо воно виділене жирним шрифтом і впадає в очі (насправді

А. Гітлер народився у 1889 р.).

Якщо ми спроектуємо цю психологічну закономірність на соціальні мережі, то зрозуміємо, що «ГАРЯЧІ НОВИНИ» відіграють таку саму роль і привертають більше уваги, це неусвідомлений процес. Оскільки у соцмережах ми не можемо змінювати розміру, кольору й шрифту тексту, то великі літери – це єдине, що залишається для привертання уваги.

Як і великі літери, великі зображення – це така ж цукерка для системи 1, водночас вони привертають увагу користувачів.

Ще один спосіб догодити системі 1 – максимально читабельний текст. Кількість складів у слові негативно корелює з усіма показниками Facebook (тобто чим довші слова, тим менше охоплення, включеність і взаємодія). Тому редактори соцмереж мають розуміти, що читач частіше перебуває у системі 1, і текст має підходити для швидкого читання.

Складніші тексти й коментарі

На відміну від когнітивної простоти, когнітивне напруження має протилежні причини та наслідки. Керуючись системою 2, люди стають більш уважними, роблять менше помилок, але водночас є менш креативними і витрачають багато зусиль.

Як у соціальних мережах досягти когнітивного напруження, щоб «включити» читачів? Один зі шляхів – це складніші тексти, тобто речення з більшою кількістю слів і більшою кількістю складів у слові. Щоб виміряти складність текстів у Facebook, ми застосували індекс Флеша-Кінсайда. Він вираховується за допомогою середньої кількості складів у слові та кількості слів у реченні.

І тут гарна новина для журналістів. Складніші дописи мають більше коментарів (зауважте, не лайків чи шейрів)! Це пояснюється саме швидким і повільним мисленням. Коли текст здається складним, деякі користувачі соцмереж лишають його і переглядають інші повідомлення. А ті, хто вирішив прочитати складне повідомлення, включають повільне мислення, і воно дає змогу їм зрозуміти повідомлення краще та сформулювати думку. Отже, чим складніший текст, тим більше коментарів до нього.

Крім психології, тут ще впливають й інші фактори. Загальна складність тексту може означати важливість допису, тому складніші тексти отримують більше переглядів та кліків. Складні повідомлення довші, а довші повідомлення відображаються у більших блоках тексту. Складніші й довші дописи забирають більше часу для перегляду і потребують більш уваги.

Напруження + полегшення = обговорення

Загальне співвідношення для трьох показників Facebook таке: чим більше охоплення, тим більша включеність, чим більша включеність, тим більше лайків, шейрів, коментарів. Тобто це лінійний взаємозв'язок. Тим не менше, іноді ми помічаємо відхилення від цієї моделі. Чому одні історії спонукають до більшої активності, ніж інші?

Щоб кількісно це виміряти, дехто застосовує показник, який називається

«рівень обговорення». Це співвідношення між тими користувачами, які взаємодіють із дописом (talking about this – лайки, шейри, коментарі) та охопленням (кількістю, які побачили пост).

...З огляду на те, які матеріали мають найбільший показник обговорення, можна зробити такі висновки.

Найбільше балів у красивих і приємних постів, у тому числі слайд-шоу. Більше обговорюють ті повідомлення, які фіксують проблему, але й пишуть про рішення, наприклад:

- не змогли завершити марафон, але їх запросили знову;
- природний катаклізм, але діти врятовані;
- жертви теракту, але їм надали медичну допомогу.

Менший показник – у тих дописів, які пов'язані з мистецтвом (музика, фільми, книжки) або сфокусовані на фактичній інформації (рахунок спорту, бізнес-угоди).

Такі результати можна пояснити швидким і повільним мисленням. Дописи з красивими картинками (лебеді та лілії) приваблюють систему 1 і спонукають до взаємодії. Але інші історії не містять красивих картинок. Замість цього вони повідомляють про проблему, а потім пропонують вирішення. Цю модель я називаю «напруження – полегшення».

Два шляхи – одна ціль

Підсумовуючи, можна сказати, що є різні способи привернути увагу в соцмережах. Красиві картинки, прості тексти й великі літери приваблюють систему 1, тобто неусвідомлену увагу. Щоб привернути усвідомлену та осмислену увагу, ми можемо використати щось несподіване або складну мову, метод «напруження – полегшення». Обидва підходи допоможуть залучити більше уваги й трафіку через соцмережі.

Дехто може сказати, що ці підходи не щирі. Тим не менше, осуд залежить від цілі. Якщо наша ціль щира – досягнути більшої аудиторії та збільшити суспільний вплив від нашого ЗМІ, використання цих технологій виправдане й доцільне. Тут можна процитувати Д. Канемана: «Це все дуже гарні поради, але ми не повинні захоплюватися. Якісний папір, яскраві кольори, римована чи проста мова особливо не допоможуть, якщо ваше повідомлення очевидно позбавлене змісту, або суперечить фактам, які аудиторія знає як правдиві. Психологи, які займаються експериментами, не думають, що люди дурні чи дуже легковажні. Але що точно думають психологи – більшість нашого життя минає під враженнями від системи 1» (*Дорон М. Психологія «лайків» та «шейрів» // Телекритика (<http://osvita.mediasapiens.ua/material/26405>). – 2014. – 2.01).*

Пожилые пациенты часто жалуются на ослабление памяти и внимания. Возможно, скоро вместо медикаментов врачи будут выписывать рецепты немного другого содержания, чем обычно. Это могут быть советы подобного

вида: завести страницу на Facebook или найти определенную информацию в Интернете.

В чем же секрет целебного действия всемирной паутины на мозг? И как электронные страницы способны избавить от недугов старости, связанных с плохим кровообращением мозга?

Целебная сила Интернета для пожилых людей

Исследовательская группа провела опыт на пожилых пациентах после 70 лет, которые не являлись активными пользователями Интернета. Специалистами была найдена взаимосвязь между работой на известных интернет-ресурсах и улучшением когнитивных способностей пациентов. Было отмечено, что именно работа в социальных сетях, а не в онлайн-дневниках давала высокие результаты улучшения работы мозга. Поразительно, но те, кто был вынужден в ходе эксперимента постоянно пользоваться социальным аккаунтом и производить определенные действия на интернет-страницах, на 25 % улучшили свои показатели в когнитивной сфере.

Эксперимент проводился в сравнении с контрольной группой и был повторен не единожды. Это дает основания для однозначных выводов: работа в социальных сетях и знакомство с Интернетом пожилым людям просто необходимы. Они позволяют избежать ослабления познавательных способностей и улучшить показатели запоминания, восприятия информации. Онлайн-общение может также стать психологическим мотиватором и усилителем социальных взаимодействий для таких пациентов. По некоторым предположением, именно социальная интеграция, возможность общаться и получать поддержку, необходимость проявлять активность – залог длительной работоспособности мозга и тела в пожилом возрасте. Ученые рассматривают социальные сети, как вариант игровых программ для пожилых, которыми они могут пользоваться в любое удобное время. И если обычные скучные игры могут приесться, то о странице в социальной сети такого не скажешь. Она дает не только изобилие информации, но и такое необходимое для престарелых людей общение.

Онлайн поддержка мозга

Другое исследование доказало, что не только Facebook, «ВКонтакте» или «Одноклассники» способны улучшать работу мозга. Поиск информации в Интернете также усиливает активность определенных зон мозга. Это, скорее только, связано с мультитазачностью Интернета. Для поиска информации существует необходимость задействовать зрение, внимание, способность к анализу, память, а также воспроизвести полученную информацию. Такая тренировка мозга не может пройти бесследно. У подопытных наблюдаются значительные улучшения показателей. Во многих случаях Интернет может стать прекрасной альтернативой таблеток. Положительным является и то, что каждый может сделать свой вклад в здоровье родителей, бабушек и дедушек. Для этого стоит запастись терпением и помочь близкому человеку научиться пользоваться Интернетом, завести ему страничку в Facebook или в другой

соціальної мережі (*Соціальні мережі ефективні проти старечого слабощу // Сводка.net (http://svodka.net/mir/mir/1106435). – 2014. – 9.01).*

Маніпулятивні технології

Російська соціальна мережа «Однокласники» заблокувала посилання на інтернет-видає «Українська правда». При розміщенні посилання на будь-який матеріал УП з'являлось системне повідомлення про заборону, повідомляє Watcher.

Однак пізніше користувачі «Однокласників» змогли опублікувати новини з «Української правди».

«Однокласники» – популярна соціальна мережа в Україні. Денна аудиторія «Однокласників» в Україні становить 3–4 мільйон користувачів, відзначає ресурс.

«Однокласники» належать російському холдингу Mail.Ru Group, до якого також належить сайт Mail.ru, 40 % соціальної мережі «ВКонтакте» і ряд інших активів (*«Однокласники» вже не блокують посилання на «Українську правду» // Інформаційне агентство «ПІК – Південна інформаційна Компанія» (http://pik.ua/news/url/odnoklassniki_uzhe_ne_blokirujut_ssyli_na_ukrainskuju_pravdu). – 2013. – 30.12).*

Чи можуть бути небезпечні соціальні мережі?

З моменту появи соціальних мереж їх популярність зростає з кожним днем. І вона настільки висока, що практично кожен користувач мережі Інтернет зареєстрований в тій чи іншій соціальній мережі. Усі ми знаємо про плюси цього вірусоподібного сегмента мережі, але чи замислюємося ми про його мінуси?

У деяких соціальних мережах зареєстровано просто колосальна кількість користувачів. Як відомо, ще здавна масове згуртування людей завжди приваблювало любителів наживи й обману довірливих громадян. У цій статті розповідається про справжню небезпеку і шкоду, яку завдають нам соціальні мережі. Перша небезпека пов'язана не тільки з соціальними мережами, але і з Інтернетом у цілому. Мова піде про мобільних шахраїв.

Види шахрайства

Якщо ви активний користувач мережі Інтернет, то нерідко помічали, що деякі сайти пропонують виконати якусь послугу тільки після відправки смс-повідомлення. Наприклад, для того щоб скачати фільм, книгу, гру тощо, треба відправити смс-повідомлення. Крім того, останнім часом вся банерна та контекстна реклама рясніє оголошеннями такого роду: «Надішліть смс-повідомлення з номером людини, і ви дізнаєтеся всю інформацію про нього, яка міститься в єдиній закритій базі». Або ось ще: «Ви можете дізнатися все

листування, відправивши нам повідомлення з номером людини» ... і так далі. Ще бувають випадки, коли ви пройшли якийсь тест, але для того, щоб дізнатися його результати, необхідно відправити смс-повідомлення. Це все різні випадки одного виду шахрайства. Який же зв'язок цього виду шахрайства з соціальними мережами? А зв'язок дуже простий, бо вся реклама на ці шкідливі сайти поширюється через соціальні мережі. Як правило, реальна вартість відправленого смс-повідомлення набагато перевищує заявлену сайтом. Якщо ви вже попалися на вудку мобільним шахраям, тобто відправили смс-повідомлення, ви можете звернутися із заявою до вашого стільникового оператора. У заяві варто докладно описати проблему, що склалася. Нерідко вдається повернути гроші назад.

Залежність

Друга небезпека пов'язана із залежністю від цих мереж. Сучасні віртуальні мережі містять деякі платні послуги. Наприклад, одна з відомих мереж представляє можливість посилати повідомлення за допомогою звичайних смс: коли на ваш акаунт приходять повідомлення, ви отримуєте оповіщення на мобільний телефон і можете відповідати на нього смс-повідомленням. Природно, сильно залежна людина прагне використовувати соціальні мережі в повному обсязі, без будь-яких обмежень, і, як правило, платить за подібні сумнівні послуги. Крім того, у багато соціальні мережі інтегровані онлайн-ігри, для гри в які потрібні реальні гроші.

Метою наступного виду шахрайства є заволодіння вашою сторінкою в соціальній мережі. Заволодівши сторінкою, шахрай може дізнатися докладну інформацію про вас, ваші контакти, інформацію про ваших знайомих, друзів, також він може вести шахрайську діяльність з вашої сторінки. Схема цього шахрайства дуже проста. По суті, таке шахрайство можна віднести до виду хакерської атаки, яка називається фішингом. Вона полягає в тому, що хакер підсовує вам, замість справжньої сторінки, де ви вводите логін і пароль, щоб зайти в соціальну мережу, підроблену сторінку, і тим самим ви самі передаєте шахраєві дані від вашої сторінки. Підробка відбувається таким способом: на призначену для користувача пошту приходять повідомлення з пропозицією дружби в соціальній мережі, завантажити музику, відео, ігри тощо. Повідомлення містить замасковане посилання, яка веде до копії сторінки деякої соціальної мережі. У цілях безпеки радимо вам ніколи не переходити за подібними посиланнями і вводити адресу сторінки в адресний рядок.

Довіра

Інший вид шахрайства заснований на довірі. Уявіть таку ситуацію. Вам приходять повідомлення від знайомого з проханням позичити електронних грошей, скачати якийсь контент або перейти по якомусь посиланню. Сидячи по інший бік екрану, ви не можете точно знати, хто відправив вам повідомлення – друг чи шахрай, який заволодів його сторінкою, і, як правило, ви, не замислюючись про це, виконуєте прохання. Відгородити себе від цього шахрайства дуже просто, треба лише зв'язатися з тим, хто відправив

повідомлення з проханням, зв'язатися по іншому каналу зв'язку (наприклад, зателефонувати) і запитати підтвердження прохання. Тут перераховано лише найпопулярніші види шахрайства за допомогою соціальних мереж. Однак пам'ятайте, кожен день вигадуються все нові більш витончені шахрайські схеми. Будьте обережні. Як це не банально, але ваша безпека у ваших руках ***(Чим можуть бути небезпечні соціальні мережі? // InternetUA (http://internetua.com/cim-mojut-buti-nebezpechn--soc-ahn--merezj). – 2014. – 3.01).***

Объявления о поиске активистов для участия в автопробеге в поддержку Президента Украины В. Януковича распространяются в соцсетях, – пишет «Украинская правда» со ссылкой на журналиста Н. Седлецкую.

«Похоже, Партия регионов запускает очередной “оригинальный” ответ на действия Евромайдана. В соцсетях нанимают водителей со своими авто на автопробеги с 8 января и в течение 20 дней. Объявления от тех же “супервайзеров”, которые приводили людей на митинги ПР в Мариинский парк», – отметила она.

В объявлениях указано, что оплата водителям гарантируется на уровне 200–250 грн, пассажирам в автомобилях будут платить 80–100 грн за 6 часов «работы».

По словам Н. Седлецкой, один из «супервайзеров» подтвердил, что ездить по Киеву нужно в поддержку Януковича.

Ранее активисты Евромайдана провели серию автопробегов, которые завершились пикетами особняков влиятельных «регионалов» ***(Партия регионов в соцсетях собирает свой проплаченный «анти-Автомайдан» // Четверта Влада (http://4vlada.net/partii-lidery/partiya-regionov-v-sotssetyakh-sobiraet-svoi-proplachennyi-anti-avtomaidan-smi). – 2014. – 8.01).***

Facebook-сторінка «Жить в Киеве» за неповні три доби свого існування набрала 15 тис. лайків. Приблизно стільки ж користувачів поширили несправжню новину про розіграш квартири у Києві, якої насправді не існує. Про це повідомляє онлайн-видання Aip.ua.

Уранці 6 січня на Facebook-сторінці «Жить в Киеве» опублікували повідомлення про акцію-розіграш. Людям пропонували поділитися новиною на своїй сторінці, підписатися на паблік «Жити в Києві» та взяти участь у лотереї. Люди нібито мали можливість виграти квартиру-студію площею 28 квадратних метрів у новобудові на Оболоні. Переможця обіцяли визначити 8 березня.

Водночас чимало Facebook-користувачів звернули увагу, що на сторінці не вказані жодні контактні дані організаторів акції. Немає також жодних юридичних подробиць, які зазвичай зазначають великі компанії у таких випадках. Журналіст Aip.ua Т. Ворона звертає увагу, що зображення квартири

можно легко знайти в Google на сайтах з планування та дизайну квартир. Фоновою світлиною сторінки «Жить в Києве» обраний знімок житлового комплексу в Алушті. На думку журналіста, це вказує на те, що конкурс несправжній, а сторінка – штучно розкручена.

Аналогічну сторінку під назвою «Жить в Москве» 6 січня створили Росії. Але там зображенням «акційної квартири» поділилося лише 138 користувачів.

На думку адміністраторів популярної спільноти «Типичный Киев», несправжні розіграші часто використовуються для популяризації нових сторінок. За однією із версій, згодом паблік «Жить в Києве» може використовуватися для поширення міських новин або ж просто стати клоном спільноти «Типичный Киев» **(Близько 15 тис. користувачів Facebook поширили фейкову новину про розіграш квартири у Києві // Osvita.Mediasapiens (<http://osvita.mediasapiens.ua/material/26545>). – 2014. – 8.01).**

LinkedIn подала в суд на неизвестных американских спамеров

Как сообщает Bloomberg, социальная сеть для поиска и установления деловых контактов LinkedIn утверждает, что неизвестные хакеры из США создали большое количество поддельных аккаунтов, с помощью которых собирали информацию о реальных пользователях сети.

В мае 2013 г. администрацией сайта была отмечена подозрительная активность на сайте. Было выявлено, что неизвестные злоумышленники создали тысячи страниц со стандартными настройками с помощью автоматизированных инструментов. Таким образом они нелегально собирали нужную для себя информацию о пользователях соцсети.

Подобные действия спровоцировали ряд нарушений, главными из которых являются нарушения правил сети и американских законов о компьютерной безопасности. Также истцы заявляют о незаконности сбора данных о пользователях без ведома администрации сайта.

Напомним, что это уже не первый подобный случай по нарушению прав соцсетей. В 2012 г. сеть Twitter судилась с компанией, которая собирала информацию о пользователях с целью рассылки спама **(LinkedIn подала в суд на неизвестных американских спамеров // InternetUA (<http://internetua.com/LinkedIn-podala-v-sud-na-neizvestnih-amerikanskih-spamero>). – 2014. – 12.01).**

Зарубіжні спецслужби і технології «соціального контролю»

Служба безпеки України починає викликати користувачів соціальних мереж, для надання пояснень щодо своїх коментарів у соціальних мережах. Про це повідомляє Twitter Євромайдану.

У прикріпленому документі йдеться про виклик для дачі пояснень в Управління СБУ в Запорізькій області за публікацію в мережі Facebook.

Нагадаємо, працівники силових відомств 9 грудня захопили офіс інтернет-телеканалу INTV, у якому розташоване інтернет-видання «Цензор.нет». Також «Беркут» влаштував погром в офісі газети «Вечірні вісті».

Формальною причиною до захоплення офісів згаданих видань стали нібито коментарі, у яких містились заклики до повалення влади *(СБУ почало викликати на допити через пости у Facebook // iPress.ua (http://ipress.ua/news/sbu_pochalo_vyklykaly_na_dopyty_cherez_posty_u_feysbutsi_37135.html). – 2013. – 29.12).*

Агентство національної безпеки США (АНБ) має доступ до комп'ютерів та інших електронних пристроїв для розміщення на них шпигунського програмного забезпечення. Для цього використовуються програмні «діри» і навіть перехоплення системи звітності Microsoft. Про це пише німецький журнал Der Spiegel з посиланням на внутрішні документи АНБ.

За даними видання, відділ АНБ вузькоспеціалізованих операцій Tailored Access Operations (TAO) має справу зі складними системами, які важко зламати. TAO відповідає за доступ до захищених мереж керівників держав з усього світу і співпрацює з ЦРУ і ФБР у рамках «делікатних завдань», проникаючи в міжконтинентальні оптоволоконні комунікації за допомогою особливих приладів, які агенти АНБ розміщують на підводних лініях.

TAO перехоплювала поставки електронного обладнання для введення у нього шпигунського програмного забезпечення, щоб отримати доступ до систем, де воно потім використовувалося.

Відповідно до звіту, АНБ розміщала такі лазівки на комп'ютерах, жорстких дисках, маршрутизаторах та інших пристроях таких компаній, як Cisco, Dell, Western Digital, Seagate, Maxtor, Samsung і Huawei.

Усі перераховані компанії на запит журналу Der Spiegel заявили, що не були інформовані про шпигунські системи у своєму обладнанні.

Журнал повідомляє про 50-сторінковий каталог інструментів і методів вартістю до 250 тис. дол., що називається ANT (Advanced/Access Network Technology), використовується для отримання доступу до пристроїв. Наприклад, «спеціальний» кабель для монітора вартістю 30 дол. дає змогу TAO бачити виведене зображення. А пристрій у вигляді звичайного USB-брелока

може приймати дані по замаскованому радіозв'язку, коштує понад 20 тис. дол. Спеціальна активна базова станція GSM, що видає себе за вишку стільникового оператора, коштує 40 тис. дол.

«Здається, що АНБ може підібрати зі свого інструментарію ключ майже до кожного замка. І не має значення, які стіни збудували компанії – схоже, фахівці АНБ уже обійшли їх», – коментує Der Spiegel.

Раніше повідомлялося, що шпигунськими програмами АНБ заражені 50 тис. комп'ютерних мереж у цілому світі і що вони управляються дистанційно тисячею хакерів (*Комп'ютери провідних фірм «заражені» шпигунськими програмами // Західна інформаційна корпорація (http://zik.ua/ua/news/2013/12/31/kompyutery_providnyh_firm_zarazheni_shpygunskymy_programamy__der_spiegel_450728). – 2013. – 31.12).*

Два пользователя социальной сети Facebook подали на нее в суд, обвинив в сканировании личной переписки. Об этом сообщает интернет-издание MediaPost.

Как утверждают истцы, соцсеть отслеживает, какие ссылки пользователи отправляют друг другу напрямую в личных сообщениях, проверяет их и затем передает эту информацию третьим лицам с корыстными целями. Таким образом, Facebook создает ложное впечатление о том, что личная переписка остается закрытой. В действительности, по мнению истцов, пересылаемые в личных сообщениях ссылки ничем не отличаются от публичных лайков или от перепоста на своей странице.

Иск в окружной суд Северной Калифорнии подали М. Кэмпбелл из Арканзаса и М. Харли из Орегона. Они обвинили Facebook в нарушении федеральных законов о слежке за гражданами и законов Калифорнии о защите частной жизни. Истцы надеются, что иск получит статус коллективного. Чего именно требуют от ответчика М. Кемпбелл и М. Харли, не сообщается.

Как напоминает MediaPost, информация о том, что Facebook сканирует личные сообщения, появилась еще в 2012 г. Тогда ряд пользователей заметили, что пересланные ссылки засчитываются как лайки и учитываются в общем количестве понравившихся страниц. Facebook тогда подтвердила, что счетчик «лайков» действительно учитывает пересылаемые друг другу ссылки, однако никакая личная информация при этом не разглашается.

В августе 2013 г. Facebook обязался в досудебном порядке выплатить 20 млн дол. в качестве компенсации за использование имен и фотографий пользователей в рекламных блоках Sponsored Stories («Рекламные новости»). Как сообщалось, компенсацию по коллективному иску должны были получить около 614 тыс. человек (*На Facebook подали в суд за сканирование личных сообщений // Лента.Ру (<http://lenta.ru/news/2014/01/03/sue/>). – 2014. – 3.01).*

Агентство национальной безопасности (АНБ) США пытается создать собственный квантовый компьютер, который смог бы взломать практически любую систему шифрования. Об этом пишет в пятницу, 3 января, газета The Washington Post со ссылкой на документы, обнародованные бывшим сотрудником ведомства Э. Сноуденом.

Проект является частью исследовательской программы «Внедрение в сложные цели», на осуществление которой выделено 79,7 млн дол. Большая часть работ проводится в Лаборатории физических наук в Колледж-Парке в штате Мэриленд.

О каких-либо существенных успехах АНБ в области квантовой физики неизвестно. Как заявили газете ученые, маловероятно, чтобы АНБ серьезно продвинулось на пути создания квантового компьютера и никто об этом не узнал. Судя по документам из архивов Э. Сноудена, работающие на спецслужбы физики подошли ненамного ближе к решению задачи, чем европейские ученые, и каких-либо прорывов в ближайшее время не ожидается.

Квантовый компьютер, поясняет The Washington Post, основан на идее о том, что объект может одновременно существовать во всех состояниях. В отличие от битов, которые используются в обычных компьютерах, квантовый компьютер основан на работе кубитов, которые случайно переходят в одно из своих состояний. Предполагается, что с определенными задачами квантовый компьютер справляется во много раз быстрее обычного, так как не выполняет операции последовательно одну за другой, а пропускает ненужные для решения шаги.

Если работоспособный квантовый компьютер будет создан, отмечает газета, он сможет взломать популярный сейчас метод шифрования RSA. Этот криптографический алгоритм основан на сложности факторизации больших целых чисел. Обычные компьютеры справиться с ней за разумное время не смогут.

«Применение квантовых технологий к алгоритмам шифрования серьезно повлияет на способность правительства США как защищать собственные коммуникации, так и перехватывать коммуникации зарубежных правительств», – цитирует газета предоставленные Э. Сноуденом документы.

Напомним, бывший сотрудник АНБ Э. Сноуден бежал в Россию и получил временное убежище. Он передает СМИ засекреченные документы, касающиеся работы американских спецслужб. Благодаря этим утечкам стало известно, в частности, что правительство США вело широкомасштабную слежку как за собственными гражданами, так и за иностранными лидерами (*Спецслужба США создает суперкомпьютер для взлома кодов // InternetUA (<http://internetua.com/specslujba-ssha-sozdaet-superkompuater-dlya-vzloma-kodov>). – 2014. – 3.01).*

Суд США по делам о надзоре за иностранными разведками разрешил спецслужбам продолжать массовый сбор информации о телефонных переговорах американских граждан. Об этом 3 января сообщает Associated Press со ссылкой на представителя Управления национальной разведки США.

Разрешение на продолжение программы прослушки телефонных разговоров было дано после запроса американских властей санкции на продолжение этой деятельности. Запрос был связан с окончанием срока полномочий, ранее предоставленным спецслужбам решением суда. Такие запросы на подтверждение санкций власти регулярно направляют суду с 2006 г., когда была запущена программа прослушки.

Разрешение на продолжение программы, предоставленное судом по делам о надзоре за иностранными разведками 3 января 2014 г., стало первым после того, как Федеральный окружной суд в Вашингтоне постановил прекратить сбор информации о телефонных переговорах американцев.

В тот же день, 3 января, как пишет Reuters, Министерство юстиции США подало в апелляционный суд США апелляцию на решение Федерального окружного суда о блокировке программы прослушки.

Ранее, 16 декабря, Федеральный окружной суд в Вашингтоне постановил прекратить сбор информации о телефонных переговорах, удовлетворив иск двух американцев к правительству и Агентству национальной безопасности США (АНБ). Суд решил, что программа сбора информации о телефонных переговорах противоречит четвертой поправке к Конституции США, защищающей граждан США от необоснованных обысков. Исполнение судебного решения было отложено до рассмотрения апелляции со стороны правительства: судья постановил, что дело затрагивает интересы национальной безопасности, а также касается не рассматривавшихся ранее конституционных вопросов.

Как пишет Reuters, в том же месяце законность сбора информации о телефонных переговорах рассматривал окружной судья в Манхэттене, который признал программу прослушки законной на том основании, что она направлена на борьбу с терроризмом. Как отмечает агентство, противоречащие друг другу судебные решения указывают на необходимость рассмотрения дела Верховным судом США (*Спецслужбы США получили разрешение на продолжение программы прослушки // InternetUA (<http://internetua.com/specslujbi-ssha-polucsili-razreshenie-na-prodoljenie-programmi-proslushki>). – 2014. – 4.01*).

Ряд хакерских атак на сайты государственных учреждений, компаний и университетов Швеции, зафиксированных в прошлом году, был организован зарубежными спецслужбами. Об этом сообщает РИА Новости, ссылаясь на шведский новостной портал Local.

«Мы можем подтвердить, что инциденты, связанные с хакерскими атаками, которые происходили в прошлом году, были организованы иностранными спецслужбами», – заявил официальный представитель Радиокommunikационной службы шведской обороны (FRA) Ф. Валлин, отметив, что эти атаки «угрожают конкурентоспособности Швеции как государства».

При этом спецслужбы какой страны стоят за нападениями хакеров, Ф. Валлин не уточнил.

По данным Local, речь идет о серии атак, связанных как с попытками взлома отдельных компьютеров, так и с попытками полномасштабного обрушения информационных систем. Жертвами этих атак, как правило, были руководители общественных организаций, крупных коммерческих предприятий и исследователи, работающие в оборонной промышленности. «Они (хакеры) выбирали человека и пытались внедрить в его компьютер вредоносный код, чтобы осуществлять мониторинг и хищение информации», – прокомментировал действия хакеров один из IT-специалистов, знакомый с ситуацией.

Напомним, ранее сообщалось, что Радиокommunikационная служба шведской обороны (FRA) активно помогала американскому Агентству национальной безопасности (АНБ) собирать информацию о российских политиках. Об это свидетельствуют секретные документы, обнародованные экс-сотрудником ЦРУ Э. Сноуденом (*Швеция уличила спецслужбы извне в организации хакерских атак // InternetUA (<http://internetua.com/shveciya-ulicsila-specslujbi-izvne-v-organizacii-hakerskih-atak>). – 2014. – 9.01*).

Авторитетное издание Der Spiegel утверждает, что популярнейшая в мире операционная система позволяет спецслужбам, включая Агентство национальной безопасности, получать доступ к компьютеру любого пользователя.

В частности, направляя в адрес Microsoft отчеты об ошибках операционной системы Windows, пользователи могут неосознанно указывать спецслужбам самый легкий путь к получению доступа к каждому отдельно взятому компьютеру с учетом его «слабых мест».

Совсем недавно эксперты в области безопасности также заявили о том, что сотрудники спецслужб могут использовать в целях шпионажа смартфоны линейки iPhone, однако руководство корпорации Apple поспешило заявить, что производителю не известно о случаях получения экспертами АНБ доступа к смартфонам отдельных пользователей или о существовании соответствующей возможности (*«Windows» позволяет шпионить за пользователями // InternetUA (<http://internetua.com/Windows--pozvolyaet-shpionit-zapolzovateljami>). – 2014. – 12.01*).

Проблема захисту даних. DOS та вірусні атаки

Хакерське угруповання «Сирійська електронна армія» (SEA) атакувало облікові записи компанії Skype в соцмережах. Про це повідомляє сайт TechCrunch.

Хакери зламали сторінки Skype у Facebook та Twitter, а також офіційний блог компанії. На зламаних сторінках зловмисники розмістили повідомлення, у яких закликали користувачів не використовувати поштові сервіси Outlook та Hotmail, які належать Microsoft. Хакери стверджували, що в цій компанії проглядають акаунти користувачів та продають інформацію урядам.

Через деякий час Skype вирішили проблему, повідомлення хакерів видалили та попросили вибачення за спричинені незручності. У компанії також заявили, що дані користувачів через атаку не постраждали.

SEA вперше заявили про своє існування у 2011 р., коли розпочалася громадянська війна у Сирії, – зазначає Lenta.ru. Тоді хакери зламали сайт Гарвардського університету та розмістили на ньому інформацію про підтримку президента Сирії Б. Асада. Пізніше угруповання атакувало Twitter-акаунти Б. Обами, газети The Financial Times, телеканалу Al Jazeera, агентств Associated Press та Agence France-Press, сайти The New York Times, CNN та The Washington Post (*Сирійські хакери зламали облікові записи Skype у соціальних мережах // Телекритика (<http://osvita.mediasapiens.ua/material/26407>). – 2014. – 2.01).*

Социальные сети в жизни среднестатистического современного жителя Украины, да и других стран, занимают определенное и далеко не последнее место. Очень часто, включая утром компьютер, пользователь одновременно открывает окна с почтой и с избранными социальными сетями.

Помнится, как в период своего «расцвета», лет восемь назад, всеми известные «Одноклассники» прославились не столько восстановлением старых связей между бывшими учащимися, сколько распространением вирусного программного обеспечения. Причем трояны были далеко не самыми страшными в этих посланиях.

...Однако «Одноклассники» потом приняли целый ряд мер, в связи с которыми рассылка спама и прочего информационно-вирусного хлама стала почти невозможной. Да и популярность эта социальная сеть начала стремительно терять. На смену «Одноклассникам» пришли два монстра, покоровшие почти тотально все постсоветское пространство.

«ВКонтакте» и Facebook стали чуть ли не главным источником не только общения между старыми товарищами, но и информационной площадкой для медийных ресурсов, начиная от новостных, заканчивая развлекательными.

Распространители вирусов, моментально почувствовав новое

направление, ринулись на новое поприще. Facebook оказался самым популярным сетевым ресурсом, где возможно подхватить вирусную программу.

Уже более недели по вышеупомянутой сети идет рассылка через «друзей» программного обеспечения, которое не только делает вас обладателем отвратительного видео, но и превращает ваш компьютер в почтальона «писем счастья». Иными словами посредством вашего аккаунта и вашего компьютера вредители рассылают по социальной сети вирус.

Такие эпизоды наглядно доказывают тот факт, что никогда не знаешь кто на самом деле сидит по ту сторону монитора, то ли закадычный друг, то ли злоумышленник. Помните! Используя меры предосторожности при работе в Интернете, вы помогаете не только своему компьютеру, но и сотням других (*Facebook распространяет через аккаунты друзей опасный вирус // InternetUA (http://internetua.com/Facebook-rasprostranyaet-cserez-akkaunti-druzei-opasnii-virus). – 2014. – 4.01).*

Антивирусная компания Symantec обратила внимание, что в последние несколько недель в сети участились случаи DDoS-атак с использованием Network Time Protocol.

Network Time Protocol (NTP) – сетевой протокол для синхронизации внутренних часов компьютера, использует для своей работы UDP и представляет собой один из старейших протоколов Интернета. Работает на порту 123.

Атака через «отражение» предусматривает, что злоумышленник посылает относительно небольшой запрос к промежуточному узлу, который отвечает относительно большим ответом в адрес указанного хоста. Раньше атаки подобного типа осуществлялись через DNS-резолверы, которые установлены у каждого интернет-провайдера. Обычно DNS-резолверы сконфигурированы так, чтобы обрабатывать только запросы своих собственных пользователей, но существует большое количество компаний, которые неправильно их сконфигурировали, так что резолверы принимают запросы от любого пользователя Интернета. Злоумышленники направляют к открытым DNS-резолверам поток DNS-запросов с IP-адресом жертвы, а резолвер отвечает на указанный адрес. Чтобы максимально усилить трафик, злоумышленники составляют запросы, которые требуют максимально объемного ответа: например, запрос списка всех DNS-записей в определенной зоне.

Атака через серверы NTP происходит схожим образом, но с использованием команды monlist. Она высылает в ответ список 600 хостов, которые последними подключались к серверу. Это даже эффективнее, чем DNS-резолверы: маленький запрос может перенаправить на жертву мегабайты трафика.

Для защиты своего NTP-сервера от подобной атаки нужно установить

NTP версии 4.2.7, в которой полностью удалена поддержка команды monlist (*DDoS-атаки через Network Time Protocol // InternetUA (http://internetua.com/DDoS-ataki-cserez-Network-Time-Protocol). – 2014. – 3.01).*

Специалисты по безопасности компаний Trend Micro и ESET сообщают об обнаружении новой версии Cryptolocker, которая блокирует доступ к файлам и для восстановления доступа к компьютеру требует от пользователя выкуп. Эта модификация зловреда ведет себя как червь и распространяется через USB-диски.

Cryptolocker 2.0 (вариант Crilock.A) квалифицирован как Filecoder.D и Filecoder.E, вредонос часто встречается на файлообменниках под видом обновления для Microsoft Office и Adobe Photoshop. Программа имеет целый ряд отличий от предыдущей версии Cryptolocker: во-первых, она блокирует доступ не только к документам, но и к файлам мультимедиа; во-вторых, вместо AES использует алгоритм шифрования 3DES; в-третьих, имеет новую архитектуру управления, с алгоритмом генерации домена (domain generation algorithm, DGA) вместо жестко прописанных URL. И главное – в этой версии вредоноса реализована старая техника инфицирования съемных дисков. Новая версия также дополнена функциями запуска компонентов DDoS-атак, кражи кошельков Bitcoin и инструментами поиска Bitcoin. Полный перечень различий Cryptolocker и Crilock.A/Cryptolocker 2.0 опубликован на веб-сайте ESET (*Вредонос Cryptolocker 2.0 может распространяться через USB // InternetUA (http://internetua.com/vredonos-Cryptolocker-2-0-mojet-rasprostranyatsya-cserez-USB). – 2014. – 7.01).*

Специалисты компании Malware Must Die установили предположительного автора новой вредоносной программы PrisonLocker/PowerLocker, которая станет достойным наследником известного трояна-вымогателя CryptoLocker, заразившего около 250 тыс. компьютеров в Америке и Западной Европе с сентября по декабрь 2013 г.

CryptoLocker шифрует документы на жестком диске – и дает жертве несколько дней на то, чтобы собрать деньги и перечислить их на указанный кошелек. В этом случае они обещают выдать ключ для расшифровки документов.

Стоимость выкупа изначально составляла 2 BTC, но по мере роста курса биткоина снижалась до 1 BTC, 0,5 BTC и, в конце концов, 0,3 BTC.

Новая программа PrisonLocker/PowerLocker будет обращаться с пользователями более жестко, если верить функционалу, который описывает ее автор. По его словам, программа будет шифровать не только документы, но также видеофайлы, фотографии и другие файлы на компьютере пользователя

(кроме .exe, .dll, .sys, других системных файлов) с помощью шифра BlowFish. Уникальный ключ для каждого ПК защищен шифрованием RSA-2048 (одна пара ключей RSA на каждый компьютер).

Владелец командного сервера сможет переустанавливать или удалять таймер с каждого ПК и снимать шифрование с файлов после получения корректного платежного кода.

Клиентская часть PrisonLocker/PowerLocker, по описанию, сможет определять виртуальное окружение VM, песочницы или дебаггера, что затруднит анализ зловреда антивирусными компаниями. Программа отключает клавиши Windows и Escape на клавиатуре, чтобы избежать неправильных действий пользователя в процессе шифрования и после него. Она также убивает процессы taskmgr.exe, regedit.exe, cmd.exe, explorer.exe и msconfig.exe. Проверка и удаление этих процессов осуществляется каждые несколько миллисекунд (*Обнаружен троян, который опаснее чем «вымогатель» CryptoLocker // InternetUA (<http://internetua.com/obnarujen-troyan--kotorii-opasnee-csem--vimogatel--CryptoLocker>). – 2014. – 8.01).*

Французский регулятор цифрового рынка CNIL оштрафовал интернет-компанию Google на 150 тыс. евро (чуть более 200 тыс. дол.) за нарушение правил работы с пользовательской информацией. CNIL 8 января заявило, что новая политика безопасности Google в области работы с пользовательскими данными недостаточно точно поясняет, как компания использует полученные сведения от пользователей, не занимается ли интернет-компания сканированием личной email-переписки и не поясняет, как долго компания хранит полученные данные. При этом в CNIL говорят, что интернет-гигант поступил довольно хитро, реализовав единую политику данных, которая распространяется на все его сервисы, что еще больше запутывает ситуацию.

Напомним, что ранее власти Европейского Союза также заявляли, что политики Google в области работы с данными не полностью соответствуют нормам ЕС и его законодательству. В самой Google пытаются утверждать, что их новая политика работы с данными проще и удобнее для пользователей, а кроме того позволяет создавать более удобные для пользователей сервисы.

В CNIL говорят, что накануне штрафа они неоднократно предупреждали компанию о возможном штрафе, но компания ничего не изменила. При этом регулятор подчеркивает, что выплата штрафа со стороны интернет-компания не дает ей индульгенцию в отношении данных пользователей и регулятор все равно будет оказывать давление на Google.

В Google говорят, что им известно о вынесении штрафа, но пока компания не знакома с вердиктом и после того, как юристы изучат итоговое постановление, Google определится с дальнейшими шагами (*Google оштрафована во Франции на 150 000 евро // InternetUA (<http://internetua.com/Google-oshtrafovana-vo-francii-na-150-000-evro>). – 2014. – 9.01).*

Масштабная атака на все крупнейшие игровые сайты и серверы стала возможна благодаря тому, что хакеры использовали NTP-протокол. Ранее данная техника осуществления DDoS-атак никогда не использовалась.

Хакеры DERP, недавно атаковавшие сервера игр League of Legends, EA.com и нескольких других крупных игровых проектов, воспользовались никогда не применявшейся ранее техникой нападения, которая позволила значительно увеличить количество обрабатываемых веб-ресурсом данных.

Вместо применения привычных попыток генерирования большого количества «мусорного» трафика, злоумышленники из DERP Trolling отправили, как оказалось, небольшой запрос к серверам синхронизации времени, использующим NTP-протокол.

Во время атаки хакеры изменяли свои запросы таким образом, чтобы они выглядели так, словно они пришли от одного из игровых сайтов. Благодаря этому, хакеры добились неожиданных результатов: после отправки запроса в 8 байт «жертва» получает ответ в 468 байт.

Ранее о данной технике ничего не было слышно по причине её непопулярности. Подобных инцидентов настолько мало, что их просто не включают ни в один доклад о безопасности. Вероятно, теперь новая техника встанет на вооружение и остальных хакеров (*Группировка DERP использовала новый принцип DDoS-атаки через NTP-протоколы // InternetUA (<http://internetua.com/gruppirovka-DERP-ispolzovala-novii-princip-DDoS-ataki-cserez-NTP-protokoli>). – 2014. – 11.01*).

Как сообщила компания Symantec, занимающаяся вопросами безопасности, на прошлой неделе пользователи Великобритании столкнулись с масштабной кампанией по загрузке вредоносного ПО. Для того чтобы заставить их загрузить вирус, определяемый как Trojan.Shylock, злоумышленники использовали социальную инженерию.

Для начала они заманивали жертв на сайты, где якобы можно бесплатно смотреть фильмы. Далее появлялось поддельное уведомление о необходимости установить ручную «критическое обновление» браузера, направляющее пользователя на поддельную веб-страницу Chrome, Firefox или Internet Explorer (в зависимости от браузера жертвы). При помощи JavaScript злоумышленники заставляли жертв оставаться на сайте, поскольку, чтобы закрыть браузер, им приходилось 100 раз кликнуть на опцию Yes/No.

Отметим, что хостинг сайта является украинским. Ресурс использует двойную гибридную установку веб-сервера Apache и Nginx, По словам экспертов из Symantec, поддельная веб-страница Internet Explorer больше не функционирует (*Злоумышленники распространяли троян под видом обновлений браузера // InternetUA (<http://internetua.com/zloumishlenniki>*

rasprostranyali-troyan-pod-vidom-obnovlenii-brauzera). – 2014. – 11.01).

Cisco Systems провела анализ недавней хакерской атаки, проведенной при помощи рекламной сети Yahoo. В рамках кампании группа мошенников размещала вредоносные объявления в сети Yahoo, переходы по которым приводили к заражению компьютеров вредоносными программами. Анализ Cisco показал, что корнями данная атака уходит на Украину и там же, скорее всего, находятся ее организаторы.

5 января Yahoo заявила, что атака была ориентирована на пользователей из Европы, а вредоносные рекламные объявления размещались с 31 декабря по 4 января. В Cisco рассказали, что жертвы вредоносных сайтов перенаправлялись на ресурсы, которые прежде уже были использованы для атак и были связаны с украинскими хакерскими группировками. Д. Шульц, специалист по ИТ-безопасности Cisco Systems, говорит, что все множество доменных адресов, задействованных в данной атаке, было размещено в одном и том же блоке IP-адресов, принадлежащих одному и тому же провайдеру (клиенту).

По данным расследования Cisco, всего в атаке были задействованы 393 IP-адреса из одного блока. Также в компании говорят, что имена вредоносных доменов всегда начинались с серии цифр в поддоменах и заканчивались случайными словами в домене второго уровня, причем зачастую слова представляли собой бессмысленные наборы букв. Большая часть доменов на сегодня уже не отвечает, но некоторые работают и по сей день.

Организаторы атак чаще всего использовали компьютеры своих жертв в рамках партнерской программы Paid-to-Promote.net, которая используется для разных целей, но чаще всего для нагона трафика с целью обмана рекламодателей. В Cisco говорят, что большая часть мошеннических доменов была зарегистрирована одним днем – 28 ноября 2013 г. Некоторые из доменов хостились в Канаде, другие – в Украине.

Известно, что в рамках вредоносной кампании хакеры заражали компьютеры вредоносными кодами Zeus, Andromeda, Dorkbot/Ngrboot, а также рекламными системами нагона кликов Tinba и Necrus.

По данным мониторинга Fox-IT, вредоносный ролик показывался примерно 27 тыс. раз в час, а основная зрительская аудитория организаторов кампании находилась в Румынии, Франции и Великобритании. В Yahoo также сообщили, что кампания была ориентирована только на Европу, причем только на Windows-пользователей, тогда как Mac-аудитория, а также пользователи мобильных устройств были в безопасности (***Организаторы хакерской атаки в рекламной сети Yahoo находятся в Украине // InternetUA (<http://internetua.com/organizatori-hakerskoi-ataki-v-reklamnoi-seti-Yahoo-nahodyatsya-v-ukraine>). – 2014. – 11.01).***

Декабрь 2013 г. отметился накаленной вирусной обстановкой

Исследования компании «Доктор Веб» показали, что наиболее распространёнными среди вирусных программ стали рекламные троянцы. Также были выявлены троянские динамические библиотеки, которые позволяют выполнять перехват различных функций браузеров. Специалисты компании «Доктор Веб» составили список 20 наиболее используемых вирусных программ.

Также было отмечено значительное расширение бот-сети. Например, в одной из обнаруженных «Доктор Веб» подсетей было зарегистрировано около 20 тыс. инфицированных компьютеров, что превышает ноябрьские показатели на 5 тыс.

Вирусную базу пополнил новый троянец, который является надстройкой к браузерам и должен обеспечивать безопасность при просмотре сайтов в Интернете, на самом же деле он выполняет абсолютно противоположные функции с помощью загруженных файлов сценария.

Второй сценарий предлагает пользователю фальшивые всплывающие окна социальной сети «ВКонтакте» и заменяет рекламные модули сети своими собственными.

Прошедший год был удачным также для распространителей вредоносных программ с целью заполучения криптовалюты Bitcoin и ее аналога Litecoin. Помимо этого, одним из знаменательных событий декабря стало обнаружение в каталоге Google Play троянского приложения, которое совершало кражу истории переписки из официального клиента всемирно популярного сервиса *(Декабрь 2013 года отметился накаленной вирусной обстановкой // InternetUA (<http://internetua.com/dekabr-2013-goda-otmetilsya-nakalennoi-virusnoi-obstanovkoi>). – 2014. – 12.01).*